# حسابرسی سیستم‌ها و فناوری اطلاعات

ناشر

انجمن علمی حسابرسی فناوری اطلاعات ایران



e-ISSN: 3115-8773

**به نام خدا**




نشریهٔ علمی

# حسابرسی سیستم‌ها و فناوری اطلاعات

سال دوم، شمارهٔ ۱، پیاپی ۳، بهار و تابستان ۱۴۰۵

نشریهٔ علمی

# حسابرسی سیستم‌ها و فناوری اطلاعات

دورهٔ ۲، شمارهٔ ۱، پیاپی ۳، بهار و تابستان ۱۴۰۵

**صاحب امتیاز**: انجمن علمی حسابرسی فناوری اطلاعات ایران

**مدیر مسئول**: علی رحمانی، استاد دانشگاه الزهرا

**سردبیر**: علی رحمانی، استاد دانشگاه الزهرا

دبیر تخصصی: آمنه خدیور، دانشیار دانشگاه الزهرا

**اعضای هیأت تحریریه:**

**علیرضا حسن‌زاده**، مدیریت فناوری اطلاعات، استاد دانشگاه تربیت مدرس

**رضا حصارزاده**، حسابداری، استاد دانشگاه فردوسی مشهد

**مهدی خدمتی**، حسابداری، دانشیار دانشگاه موناش استرالیا

**ذبیح‌اله رضایی**، حسابداری، استاد دانشگاه ممفیس امریکا

**سعید روحانی**، مدیریت فناوری اطلاعات، دانشیار دانشگاه تهران

**ندا عبدالوند**، مدیریت فناوری اطلاعات، دانشیار دانشگاه الزهرا

**رضا عزمی**، مهندسی برق و الکترونیک، دانشیار دانشگاه الزهرا

**محمدرضا کیوان‌پور**، مهندسی کامپیوتر، استاد دانشگاه الزهرا

**امیر مانیان**، مدیریت فناوری اطلاعات، استاد دانشگاه تهران

**جمال‌الدین نظری**، حسابداری، استاد دانشگاه سایمون فریزر کانادا

**حسن یزدی‌فر**، حسابداری، استاد دانشگاه دربی انگلستان

**ناشر**: انجمن علمی حسابرسی فناوری اطلاعات ایران

**دبیر تخصصی**: آمنه خدیور

**دبیر اجرایی**: مریم امیری‌خواه

**ویراستار**: آتنا خازن، بهزاد پرویزی

**صفحه‌آرا**: مریم امیری‌خواه

**ترتیب انتشار**: دوفصلنامه

**شاپا الکترونیکی**: ۸۷۷۳ - ۳۱۱۵

این نشریه دارای پروانه انتشار به شماره ثبت ۹۶۸۲۲ از وزارت فرهنگ و ارشاد اسلامی است.

نشانی: تهران، شهرک غرب، بلوار فرحزادی، بلوار نورانی، پ ۵۸.

۱۴۶۸۹۷۳۴۶۶

Email: journalofista@gmail.com

# راهنمای نویسندگان

مقاله‌های ارسال‌شده پس از داوری تخصصی و در صورت تأیید هیأت تحریریه به‌چاپ می‌رسد. از تمامی استادان و پژوهشگران گرامی که مقاله‌های خود را برای چاپ به این نشریه ارسال می‌کنند، تقاضا می‌شود، در تنظیم مقاله به موارد زیر توجه کنند.

## ۱. شکل مقاله

مقاله درمحیط نرم‌افزاری Word و در قالب ارائه‌شده در سایت نشریه تنظیم شود. برای متن فارسی قلم B Zar و برای متن انگلیسی قلم Times New Roman به کار برده شود. فاصله بین خطوط یک سانتی متر وتورفتگی ابتدای هر پاراگراف معادل ۰/۳ سانتی متر و ردیف شده (Justify) باشد. تا جایی که ممکن است، در متن مقاله از عکس استفاده نشود و در صورت استفاده، عکس با کیفیت بالا باشد.

## ۲. ساختار مقاله

**۲-۱. صفحهٔ جلد مقاله:** این صفحه باید شامل موارد زیر باشد:

- عنوان کامل مقاله؛
- نام نویسنده یا نویسندگان (نام نویسنده‌ای که عهده‌دار مکاتبات است، با علامت ستاره مشخص شود) ؛
- رتبهٔ علمی و نام مؤسسه یا دانشگاه یا محل اشتغال (به صورت فارسی و انگلیسی)، نشانی کامل نویسنده‌ای که عهده‌دار مکاتبات است، شامل: نشانی پستی، شمارهٔ تلفن، نمابر و نشانی پست الکترونیک (برای تمام نویسندگان) ؛
- در ذکر نام نویسنده‌ها از القاب و عناوین استفاده نشود و فقط رتبهٔ علمی و محل خدمت درج شود.

**۲-۲. صفحهٔ اول مقاله:** عنوان و چکیدهٔ مقاله به زبان فارسی. چکیده در یک پاراگراف با حداکثر ۲۵۰ واژه تنظیم شود. واژه‌های کلیدی (حداکثر پنج واژه) و کد طبقه‌بندی JEL نیز در انتهای چکیده درج شود. این کدگذاری برای طبقه‌بندی موضوعی در ادبیات اقتصادی طراحی شده است و جزئیاتِ نحوهٔ استفاده از آن در پایگاه اینترنتی:

< http://www. aeaweb. org/jel/guide/jel. php >قابل دسترسی است.

**۲-۳. صفحهٔ دوم تا انتهای مقاله:** این بخش باید در بردارندهٔ موارد زیر باشد:

- مقدمه (چند پاراگراف شامل بیان مسئله، مبانی نظری، هدف، اهمیت و ضرورت آن) ؛
- مروری بر پیشینهٔ (صرفا پژوهش‌های مرتبط وبه ترتیب زمانی یا موضوعی بررسی شود و نتیجه آن در پایان این بخش استخراج ماتریس نظریه و یا مدل مفهومی یا تحلیلی باشد که متغیرهای پژوهش را مستند می‌سازد و تدوین فرضیه‌های پژوهش؛
- روش پژوهش (شامل: روش پژوهش، ابزار گردآوری اطلاعات، فنون تجزیه و تحلیل و مدل آزمون فرضیه‌ها، تعریف متغیرهای مورد مطالعه و تعریف عملیاتی آن‌ها (می تواند در همان بخش مدل‌های آزمون فرضیه ارائه شود و در این صورت نیازی به تکرار ندارد)، جامعهٔ آماری، حجم نمونه و روش نمونه‌گیری) ؛
- یافته‌های پژوهش (شامل: ارائه یافته‌ها، مقایسهٔ آن با یافته‌های پژوهش‌های مذکور در پیشینه و تفسیر انطباق یا ناسازگاری یافته‌ها با پژوهش‌ها و نظریه‌ها) ؛
- نتیجه‌گیری (شامل: خلاصهٔ مسئله، ارائه خلاصهٔ نتایج و نتیجه‌گیری کلی و ارائه پیشنهادها بر مبنای نتایج (توصیه‌های سیاستی صرفا در تحقیقات کاربردی ضرورت دارد)، و در صورت لزوم پیشنهاد برای پژوهش‌های آتی با توجه به محدودیت‌های پژوهش یا چگونگی توسعهٔ پژوهش حاضر) ؛
- فهرست منابع.
- چکیده کوتاه انگلیسی (که باید ترجمه مفهوم و روانی از چکیده فارسی باشد).

## ۳. ارجاع‌های درون‌متنی

به منظور ارجاع‌ها در متن مقاله از روش APA (ای. پی. ای) استفاده می‌شود؛ به این ترتیب که:

- نام خانوادگی نویسنده همراه با سال انتشار آن در متن به صورت فارسی ارائه می‌شود و نیازی به ذکر معادل انگلیسی اسامی در پی نوشت نمی‌باشد. چنانچه تعداد نویسندگان بیش از یک نفر بود از ویرگول (،) و چنانچه تعداد منابع مورد استناد بیش از یک عدد بود از نقطه ویرگول (؛) به منظور جدا سازی استفاده شود.
- هر منبعی که در متن مقاله به آن اشاره می‌شود، باید اطلاعات کامل آن در فهرست منابع درج شود و به غیر از این منابع، منبع دیگری در فهرست منابع و ماخذ درج نشود.

در صورت نیازبه توضیحات لازم دربارهٔ اصطلاح‌ها و یا ذکر معادل‌های انگلیسی واژه‌های درون متنی (به غیر از اسامی نویسندگان)، از پی‌نوشت استفاده شود. در متن به هیچ عنوان نباید عبارات و اصطلاحات انگلیسی ارائه شود، مگر در مورد فرمول‌ها و معادله‌ها.

## ٤. فهرست منابع

برای تنظیم فهرست منابع، از روش ارجاع APA (ای. پی. ای) استفاده می‌شود؛ به این ترتیب که ابتدا منابع فارسی و پس از آن منابع انگلیسی، به ترتیب حروف الفبا و بر اساس نام خانوادگی نویسنده، به شرح زیر ذکر و شماره گذاری می‌شود:

**٤-١. کتاب:** نام خانوادگی، نام کامل نویسنده. (نقطه و یک فاصله) (سال انتشار). (نقطه و یک فاصله) نام کتاب با حروف ایتالیک، (ویرگول و یک فاصله) نام مترجم، (ویرگول و یک فاصله) محل انتشار (دو نقطه و یک فاصله) نام انتشارات. (نقطه)

**٤-٢. مقاله:** نام خانوادگی، نام کامل نویسنده. (نقطه و یک فاصله) (تاریخ انتشار). (نقطه و یک فاصله) عنوان مقاله. (نقطه و یک فاصله) نام نشریه با حروف ایتالیک، دوره (شماره) با حروف ایتالیک، (ویرگول و یک فاصله) شماره صفحه شروع – (خط فاصله) پایان مقاله. (نقطه)

**٤-٣. مقالات برخط:** نام خانوادگی، نام کامل نویسنده. (نقطه و یک فاصله) (تاریخ انتشار). (نقطه و یک فاصله) عنوان مقاله. (نقطه و یک فاصله) نام نشریه با حروف ایتالیک، دوره (شماره) با حروف ایتالیک، (ویرگول و یک فاصله) شماره صفحه شروع – (خط فاصله) پایان مقاله. (نقطه ویک فاصله) دریافت شده از (دو نقطه و یک فاصله) آدرس سایت

**٤-٣. گزارش‌ها و سایر منابع:** در این‌باره نیز اطلاعات کافی و کامل ارائه شود.

-در فهرست منابع چنانچه تعداد نویسندگان بیش از یک نفر بود، اسامی آن‌ها با استفاده از نقطه ویرگول (؛) جدا شود.

- فهرست منابع نیازمند شماره گذاری نمی‌باشد. چنانچه بیش از یک عنوان از یک یا چند نویسنده مورد استناد قرار گرفته باشد، علاوه بر رعایت ترتیب حروف الفبا، ترتیب سال انتشار نیزرعایت شود؛ به این صورت که کتاب یا مقاله‌ای که زودتر (قدیمی تر) انتشار یافته است، در فهرست زودتر درج می‌شود. به منظور جلوگیری از بروز اشتباه بین منابع مختلف درج شده در فهرست، شروع هر منبع بدون تورفتگی یا بیرون زدگی خواهد بود و چنانچه عبارت طولانی شد، ادامه با تو رفتگی (با استفاده از تکنیک Hanging) ۰/۵ سانتی متر می‌باشد.

_ منابع فارسی باید به انگلیسی نیز برگردانده شوند و عبارت (In Persian) در انتهای منبع درج شود.

## ٥. شکلها، جدول‌ها و فرمول‌ها

عنوان شکلها در زیر و عنوان جدول‌ها در بالای آن‌هادرج شود. بهتر است شکلها و جدول‌ها، در داخل متن و پس از جایی که به آنها اشاره شده، درج شوند. برای شماره‌گذاری از شمارهٔ ۱ (عددی

و داخل پرانتز، مانند جدول (۱)) تا... استفاده شود. داخل جدول‌ها باید به فارسی نوشته شود و درشرایط استفاده ممیز، از به‌کار بردن نقطه به‌جای ممیز خودداری گردد؛ در صورت ضرورت ضمن درج عنوان فارسی متغیرها، یک ستون می‌تواند به نمادهای مورد استفاده برای متغیر به زبان انگلیسی به گونه‌ای که در معادله‌ها و مدل‌ها استفاده شده اختصاص یابد. عناوین ستون‌ها در جدول‌ها، به صورت وسط چین بوده و سطر اول هر جدول که شامل عناوین ستون‌هاست با رنگ طوسی و درجه روشنی ۲ نمایش داده شود. برای اشاره به محتوای جدول‌ها و شکلها در متن، می‌بایست با استفاده از شماره آن‌ها، ارجاع مناسب صورت گیرد. فرمول‌ها نیز در جدول‌هایی دو ستونی به صورت خطوط نامرئی (No Border) ارائه و به صورت مدل (۱) (عددی و داخل پرانتز) تا... شماره گذاری شوند.

## ٦. پی نوشت‌ها

اصطلاحات انگلیسی و برخی توضیحات لازم در پی نوشت در همان صفحه ارائه شود. شماره گذاری پی نوشت‌ها با تکنیک راه اندازی مجدد در هر صفحه، در ورد درج شود.

# فهرست مقالات


**پذیرش و حمایت دانشگاهی از تلفیق درس تحلیل‌شناسی داده در حسابداری: مطالعه‌ای از منظر اعضای هیئت علمی** ۱-۲۸
علی رحمانی، سمیرا پرماه و زهرا موسوی

**حاکمیت فناوری از مسیر مدل رتبه‌بندی نوین برای کنترل‌های امنیت فناوری اطلاعات COBIT** ۲۹-۶۰
سعید روحانی و محمد نیکبخت

**ارائه چارچوب مفهومی اکتشافی حکمرانی الگوریتمیک در نظارت هوشمند حسابرسی و توسعه کارآفرینی داده‌محور با رویکرد دلفی فازی** ۶۱-۹۶
بیژن رضایی، آرش خادمی و رسول محمدی

**بازتعریف نظارت بیمه‌ای در عصر دیجیتال: چارچوبی مفهومی برای استقرار نظارت هوشمند** ۹۷-۱۲۶
آمنه خدیور، لیلی نیاکان و ناصر بافکر شارک

**تحول دیجیتال در عملکرد حسابرسی داخلی: بررسی کیفی ادبیات** ۱۲۷-۱۵۸
ندا رسولی و پارسا بهمن‌آبادی

**گشودن جعبه سیاه: چارچوبی برای اطمینان‌بخشی حسابرسان از توضیح‌پذیری تصمیمات هوش مصنوعی در حاکمیت ریسک فناوری اطلاعات** ۱۵۹-۱۸۶
فرزاد ایوانی و دنیا کاظمی

**رابطه حاکمیت شرکتی و ویژگی‌های هیئت‌مدیره با ریسک فناوری اطلاعات و امنیت سایبری: شواهدی از شرکت‌های تولیدی پذیرفته‌شده در بورس اوراق بهادار تهران** ۱۸۷-۲۳۲
مریم قاسمیان سقی و عقیل فرهنگیان

**تبیین هم‌افزایی هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط: یک مرور نظام‌مند تفسیری** ۲۳۳-۲۶۳
سعید علی‌پور و مرتضی اسدی

**طراحی و اعتبارسنجی چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک: رویکردی آمیخته در حاکمیت فناوری اطلاعات** ۲۶۴-۳۰۲
امیرحسین کافی، محمدعلی سلطانشاهی، مجتبی رئیس صفری و امیرمحمد کافی

**فناوری‌های دیجیتال نوظهور در صنعت حسابرسی: چالش‌ها و فرصت‌های جدید** ۳۰۳-۳۳۲
کاوه پرندین، کاوه قادری و آوان جمشیدی

**فرصت‌ها و چالش‌های هوش مصنوعی در ارتقاء کیفیت گزارشگری مالی: مرور نظام‌مند مطالعات موجود** ۳۳۳-۳۷۰
غلامحسین میکائیلو و محمود نصیری

**حاکمیت شرکتی پلتفرمی در عصر دیجیتال: چارچوب مفهومی یکپارچه برای سازمان‌های هوشمند** ۳۷۱-۳۹۸
معصومه کاظمی، قدرت‌اله برزگر و دانیال حسن‌زاده

Journal of
Information System and Technology Auditing

**Research Paper**

# Academic Acceptance and Support for Integrating Data Analytics into Accounting Education: A Faculty Perspective Study [1]

**Ali Rahmani[2*], Samira Parmah[3] and Zahra Mousavi[4]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 1-28

Received: 2025.06.19
Revised: 2025.07.29
Accepted: 2025.09.02

## Abstract

With the expansion of modern technologies and the growing role of data in financial decision-making, equipping accounting students with data analytics skills has become a key requirement in updated curricula. This study aims to identify and analyze the perspectives of accounting faculty members at Iranian universities regarding the necessity, approach, and challenges of incorporating a "Data Analytics" course into the accounting curriculum. This research is applied in nature and follows a descriptive-survey method. The statistical population includes accounting faculty members at universities across the country during the 2024–2025 academic year, selected through purposive sampling. Data were collected using a researcher-designed questionnaire based on a literature review and previous studies, and were analyzed using descriptive and interpretive methods. Findings indicate that faculty members have low awareness and proficiency in the field of data analytics; translated and practice-based resources are prioritized for teaching; and major implementation challenges include a shortage of specialized instructors, weak technical infrastructure, and lack of institutional policy-making. Furthermore, the master's level and offering the course either as a standalone subject or integrated with information systems were identified as the most suitable formats. Effective implementation of this course requires a holistic approach involving faculty development, infrastructure improvement, and curriculum restructuring.

**Keywords**: Accounting Education, Curriculum Design, Data Analytics, Data-Driven Learning, Faculty Perceptions.

**JEL classification:** *M41, I23, C88, O33.*

---

[1] https://doi.org/10.22034/JISTA.2025.530859.1055
[1] Selected Paper of the 2nd Conference on Computer Auditing and data Analytics
[2] Professor, Department of Accounting, Faculty of Social Sciences and Economics, Alzahra University, Tehran, Iran. (Corresponding Author). (rahmani@alzahra.ac.ir).
[3] Department of Accounting, Faculty of Social and Economic Sciences, Alzahra University, Tehran, Iran. (parmahsamira@gmail.com).
[4] Department of Accounting, Faculty of Social and Economic Sciences, Alzahra University, Tehran, Iran. (z.mousavi88@gmail.com).

## 1. INTRODUCTION

In recent years, the accounting profession has undergone significant transformations due to rapid technological advancements, particularly in data analytics, big data, artificial intelligence, and automation. These changes have dramatically shifted the expectations for accounting graduates, who are now required to possess not only traditional accounting knowledge but also a set of data-driven analytical skills that enable them to interpret, visualize, and draw insights from complex datasets. In response, global professional organizations such as the American Institute of Certified Public Accountants (AICPA), the Association to Advance Collegiate Schools of Business (AACSB), and CPA Evolution have emphasized the integration of data analytics into accounting education (AICPA & NASBA, 2021; AACSB, 2018).

Many leading universities in developed countries have revised their accounting curricula to incorporate data analytics, statistical modeling, and information systems as core components. However, in developing contexts such as Iran, the process of curriculum reform has been slower and more fragmented. One of the key barriers identified is the lack of faculty readiness and institutional support for implementing such interdisciplinary and technology-oriented courses.

Given this backdrop, the present study seeks to investigate the perspectives of accounting faculty members at Iranian universities regarding the necessity, structure, and challenges associated with integrating a dedicated course on “Data Analytics in Accounting” into the academic curriculum. The study is motivated by the assumption that faculty support plays a crucial role in shaping curriculum decisions and ensuring successful educational innovation. By analyzing faculty attitudes, capabilities, and perceived institutional constraints, this research aims to inform future policy-making and curriculum design in higher accounting education in Iran.

## 2. MATERIALS AND METHODS

This research adopts an applied purpose and employs a descriptive-survey methodology. The target population includes accounting faculty members from public universities, Islamic Azad University, and Payame Noor University across Iran during the 2023–2024 academic year. A purposive and convenience sampling technique was used to ensure diversity in academic rank, teaching experience, and institutional type.

The main instrument for data collection was a researcher-designed questionnaire developed based on a comprehensive review of the literature, including prior international studies (Andiola et al., 2020; Cainas et al., 2024; Losi et al., 2022). The questionnaire contained three main sections: (1) demographic and professional information, (2) attitudes toward the inclusion of data analytics in the accounting curriculum, and (3) perceived challenges and institutional readiness.

The questionnaire was designed and distributed electronically via the "Porsline" platform and shared through academic mailing lists and faculty networks. Out of 74 distributed questionnaires, 49 valid responses were received, yielding a response rate of approximately 66%. The reliability of the questionnaire was confirmed through Cronbach's alpha ($\alpha = 0.717$), indicating acceptable internal consistency. Content validity was ensured through expert review and pilot testing.

Data were analyzed using descriptive statistics and thematic qualitative analysis. Charts, frequency distributions, and content coding were used to examine trends in awareness, preferences, competencies, and barriers related to teaching data analytics in accounting programs.

## 3. RESULTS AND DISCUSSION

The demographic analysis revealed a diverse and experienced respondent group: 77.5% male, 88% with over 10 years of teaching experience, and over 74% with relevant professional backgrounds. Most respondents held ranks of associate professor (40.4%) or

assistant professor (38.2%), which enhances the credibility of the collected opinions.

Key findings are summarized as follows: 1. Low Faculty Awareness and Competence: A significant knowledge gap exists among accounting faculty regarding the concept and application of data analytics. Most self-reported their familiarity and technical skills in this area as "low" or "moderate." This reflects a broader systemic issue of insufficient faculty training in emerging technological domains. 2. Learning Preferences and Training Needs: Respondents preferred learning methods such as group workshops, webinars, and hands-on training. These preferences suggest a need for active and collaborative professional development initiatives, rather than self-paced or theoretical formats. 3. Preferred Teaching Resources: Faculty members favored translated textbooks, case-based learning materials (e.g., Trueblood and ARC cases), and professional resources from organizations like AICPA and IMA. They also indicated interest in using practical examples from audit firms such as PwC and KPMG. This underscores the importance of using a blended mix of localized, experiential, and international sources for teaching. 4. Technical Gaps in Tool Proficiency: Faculty exhibited limited proficiency in essential data analytics tools such as Excel (advanced features), Power BI, Python, and R. This technological deficiency poses a significant obstacle to the effective delivery of the proposed course. 5. Curriculum Design Preferences: The majority believed that the graduate (Master's) level was the most suitable stage for introducing a dedicated data analytics course. Furthermore, they preferred either a standalone course or integration with existing subjects like "Accounting Information Systems". 6. Assessment and Evaluation Strategies: Project-based learning and collaborative assignments were considered the most effective methods for evaluating student competencies in data analytics. This aligns with the shift toward performance-based assessment in modern education. 7. Institutional Readiness and Policy Support: Alarmingly, most respondents reported that their departments lacked formal plans, goals, or policies for incorporating data analytics into

the curriculum. This highlights a gap in strategic planning and a lack of institutional commitment to curriculum modernization. 8. External Collaboration and Labor Market Alignment: Respondents acknowledged the importance of aligning academic content with industry expectations through structured engagement with professional bodies. However, such collaboration was described as ad hoc and underdeveloped in most institutions. 9. Key Implementation Challenges: The most frequently cited barriers were (a) shortage of qualified faculty, (b) insufficient technical infrastructure, and (c) resistance to change among faculty and administrators. These challenges require coordinated interventions at multiple levels—individual, departmental, and policy.

Overall, the findings confirm the urgency and necessity of integrating data analytics into accounting education in Iran. At the same time, they point to a multi-dimensional readiness gap that must be addressed through targeted faculty development, resource investment, and institutional change management.

## 4. CONCLUSION

This study provides compelling evidence that the integration of a "Data Analytics in Accounting" course into the academic curriculum is not only beneficial but essential for aligning higher education with the evolving demands of the accounting profession. While faculty members in Iran acknowledge the importance of data analytics, they also face significant challenges in terms of knowledge, skills, institutional support, and infrastructure.

To bridge these gaps, a holistic and strategic approach is recommended. Key recommendations include:

- Designing faculty training programs focused on practical data tools and instructional strategies;
- Developing localized teaching resources and case studies in Persian;
- Establishing formal curriculum review committees involving industry stakeholders;

• Promoting interdisciplinary collaboration with departments of IT, statistics, and data science;

• Allocating budget for necessary software and infrastructure upgrades.

If implemented effectively, these measures can transform the teaching of accounting in Iran and ensure that graduates are equipped with the data-driven competencies required in the 21st-century job market. Ultimately, this transformation depends on the proactive engagement of faculty as both beneficiaries and drivers of change.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# پذیرش و حمایت دانشگاهی از تلفیق درس تحلیل‌شناسی داده در حسابداری: مطالعه‌ای از منظر اعضای هیئت علمی [1]

**علی رحمانی [2*]، سمیرا پرماه [3] و زهرا موسوی [4]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۱ – ۲۸

تاریخ دریافت: ۱۴۰۴/۰۳/۲۹
تاریخ بازنگری: ۱۴۰۴/۰۵/۰۷
تاریخ پذیرش: ۱۴۰۴/۰۶/۱۱

## چکیده

*با گسترش فناوری‌های نوین و نقش فزاینده داده‌ها در تصمیم‌سازی‌های مالی، نیاز به تجهیز دانشجویان حسابداری به مهارت‌های تحلیل‌شناسی داده‌ها به‌عنوان یکی از الزامات برنامه‌های درسی نوین مطرح شده است. هدف پژوهش حاضر، شناسایی و تحلیل دیدگاه اعضای هیئت علمی گروه‌های حسابداری دانشگاه‌های ایران نسبت به ضرورت، شیوه و چالش‌های گنجاندن درس «تحلیل‌شناسی داده» در برنامه درسی این رشته است. این پژوهش از نظر هدف، کاربردی و از نظر روش، توصیفی-پیمایشی است. جامعه آماری شامل اعضای هیئت علمی حسابداری دانشگاه‌های کشور در سال تحصیلی ۱۴۰۳–۱۴۰۴ بوده و نمونه‌گیری به‌صورت هدفمند انجام شده است. داده‌ها با استفاده از پرسشنامه محقق‌ساخته، مبتنی بر مرور ادبیات و مطالعات پیشین گردآوری و با بهره‌گیری از تحلیل‌های توصیفی و تفسیری بررسی شده‌اند. یافته‌ها نشان دادند که سطح آگاهی و توانمندی اعضای هیئت علمی در حوزه تحلیل‌شناسی داده‌ها پایین است، منابع ترجمه‌شده و تجربی بیشترین اولویت آموزشی را دارند و چالش‌هایی نظیر کمبود استاد متخصص، ضعف زیرساخت‌های فنی و نبود سیاست‌گذاری نهادی از موانع اجرایی اصلی محسوب می‌شوند. همچنین، مقطع کارشناسی ارشد و ارائه درس به‌صورت مجزا یا تلفیقی، ساختار مطلوب‌تری برای اجرا شناخته شد. اجرای مؤثر این درس مستلزم رویکردی کل‌نگر شامل توانمندسازی اساتید، توسعه زیرساخت و بازنگری ساختار آموزشی است.*

**واژه‌های کلیدی:** *آموزش حسابداری، اعضای هیئت علمی دانشگاه، برنامه درسی، تحلیل‌شناسی داده، فناوری داده‌محور.*

**طبقه‌بندی موضوعی:** *M41 ، I23، C88، O33.*

---

[1] https://doi.org/10.22034/JISTA.2025.530859.1055

[1] مقاله منتخب دومین همایش حسابرسی رایانه‌ای و تحلیل‌شناسی داده

[2] استاد، گروه حسابداری، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران. (نویسنده مسئول). (rahmani@alzahra.ac.ir)

[3] گروه حسابداری، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران. (parmahsamira@gmail.com)

[4] گروه حسابداری، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران. (z.mousavi88@gmail.com)

**مقدمه**

در سال‌های اخیر، تحول دیجیتال و گسترش فناوری‌های نوظهور نظیر هوش مصنوعی، کلان‌داده و یادگیری ماشین، انتظارات از حرفه حسابداری را دگرگون کرده است. تحولات گسترده در حوزه فناوری اطلاعات و گسترش داده‌های حجیم، زمینه‌ساز ظهور حوزه‌ای نوین با عنوان تحلیل‌شناسی داده‌ها[1] در علوم مختلف، به‌ویژه در حسابداری شده است. تحلیل‌شناسی داده‌ها، به‌کارگیری داده‌ها، ابزارهای آماری و فناوری برای کشف الگوها، روابط و روندهایی است که می‌توانند در تحلیل صورت‌های مالی، ارزیابی ریسک و تصمیم‌گیری حرفه‌ای در حسابداری به کار روند (انجمن حسابداران رسمی آمریکا[2]، ۲۰۲۱: ۲۰). در دهه‌های اخیر، نهادهای حرفه‌ای حسابداری در سطح بین‌المللی از جمله انجمن حسابداران رسمی آمریکا و انجمن حسابداری آمریکا[3]، بر ضرورت تجهیز دانشجویان حسابداری به مهارت‌های داده‌محور تأکید ورزیده‌اند و بسیاری از دانشگاه‌های پیشرو در کشورهای توسعه‌یافته اقدام به بازنگری در محتوای برنامه‌های درسی خود به‌منظور تلفیق مفاهیم تحلیل‌شناسی داده در آموزش حسابداری نموده‌اند(چو و همکاران[4]، ۲۰۲۱: ۴۳-۴۲؛ جانورین و واتسون[5]، ۲۰۱۷: ۴-۳).

بسیاری از برنامه‌های درسی در حال بازطراحی برای انطباق با الزامات جدید همچون استاندارد A5 هستند (کایناس و همکاران[6]، ۲۰۲۴: ۲-۱؛ لوسی و همکاران[7]، ۲۰۲۲: ۱). در ایران نیز با رشد توجه به دیجیتالی شدن فرایندهای مالی و ظهور سامانه‌های اطلاعاتی پیشرفته در سازمان‌ها، نیاز به تربیت حسابداران آشنا با ابزارهای تحلیلی و قابلیت تفسیر داده‌های پیچیده بیش از پیش احساس می‌شود. با این حال، تجربه نشان داده است که تحقق چنین هدفی بدون همراهی و پذیرش اعضای هیئت علمی به‌عنوان طراحان و مجریان برنامه‌های درسی امکان‌پذیر نیست. در واقع، درک دیدگاه اساتید حسابداری درباره ضرورت، امکان‌پذیری و موانع ورود درس تحلیل‌شناسی داده‌ها به برنامه آموزشی، پیش‌نیاز اصلاحات ساختاری در آموزش عالی این حوزه محسوب می‌شود.

---

[1] Data Analytics
[2] American Institute of Certified Public Accountants (AICPA)
[3] American Accounting Association (AAA)
[4] Chu et al.
[5] Janvrin & Watson
[6] Cainas et al.
[7] Losi et al.

در ایران نیز فشارهای بیرونی ناشی از الزامات بازار کار و نیازهای درون‌سیستمی آموزش عالی، لزوم بازنگری در محتوای درسی رشته حسابداری را اجتناب‌ناپذیر کرده‌اند. با این حال، بررسی پیشینه پژوهش‌ها نشان می‌دهد که تاکنون پژوهشی جامع و نظام‌مند در سطح ملی برای شناسایی دیدگاه اعضای هیئت علمی حسابداری نسبت به گنجاندن درس تحلیل‌شناسی داده‌ها در برنامه درسی انجام نشده است. این در حالی است که نقش محوری اعضای هیئت علمی در تدوین، اجرا و اصلاح برنامه‌های درسی، آن‌ها را به یکی از مهم‌ترین ذی‌نفعان تغییرات آموزشی تبدیل کرده است (فالگو[1]، ۲۰۲۴: ۳۳-۳۱).

مطالعات پیشین عمدتاً به بررسی ابعاد مفهومی و ساختاری موضوع در فضای بین‌المللی پرداخته‌اند و کمتر پژوهشی به تحلیل شرایط بومی، به‌ویژه از منظر بازیگران کلیدی مانند هیئت علمی پرداخته است. از این‌رو، پژوهش حاضر با رویکردی کاربردی و با بهره‌گیری از ابزار پرسشنامه، درصدد شناسایی و تحلیل دیدگاه اعضای هیئت علمی گروه‌های حسابداری دانشگاه‌های ایران نسبت به ضرورت و نحوه گنجاندن درس تحلیل‌شناسی داده‌ها در برنامه درسی حسابداری است. نتایج این پژوهش می‌تواند راهنمای مناسبی برای سیاست‌گذاران آموزشی، برنامه‌ریزان درسی و مسئولان دانشکده‌های حسابداری در مسیر تحول دیجیتال در آموزش حسابداری باشد.

بنابراین، مسأله اصلی پژوهش حاضر آن است که دیدگاه اعضای هیئت علمی گروه‌های حسابداری دانشگاه‌های ایران نسبت به ضرورت، شیوه و چالش‌های گنجاندن درس تحلیل‌شناسی داده‌ها در برنامه درسی چیست و چه عواملی این دیدگاه را شکل می‌دهند؟ در راستای این هدف کلان، اهداف جزئی زیر نیز دنبال می‌شوند:

۱. بررسی میزان آشنایی اعضای هیئت علمی با مفهوم تحلیل‌شناسی داده‌ها و جایگاه آن در آموزش حسابداری؛

۲. سنجش میزان موافقت اعضای هیئت علمی با گنجاندن درس تحلیل‌شناسی داده‌ها در برنامه درسی رشته حسابداری؛

۳. شناسایی موانع و چالش‌های پیش‌روی اجرای این درس در دانشگاه‌های ایران از منظر هیئت علمی؛

[1] Falgout et al.

۴. ارائه پیشنهادهایی کاربردی برای بازنگری برنامه درسی حسابداری با محوریت تحلیل‌شناسی داده‌ها.

اهمیت این پژوهش از دو منظر قابل توجه است. نخست، از منظر تحول حرفه‌ای، تلفیق تحلیل‌شناسی داده در آموزش حسابداری نه تنها به پرورش حسابداران توانمند در تفسیر و تصمیم‌سازی داده‌محور کمک می‌کند، بلکه پاسخ مناسبی به نیازهای در حال تغییر بازار کار و آزمون‌های حرفه‌ای جدید مانند تکامل حسابدار رسمی[1] نیز به شمار می‌رود (انجمن حسابداران رسمی آمریکا و انجمن ملی هیئت‌های حسابداری ایالتی[2]، ۲۰۲۱: ۳) . غفلت از این نیازها، می‌تواند منجر به افزایش فاصله میان دانشگاه و صنعت شده و کارایی آموزش عالی حسابداری را تحت تأثیر قرار دهد.

دوم، از منظر سیاست‌گذاری آموزشی، شناخت واقع‌بینانه از ظرفیت‌ها، نگرش‌ها و محدودیت‌های موجود در نظام آموزش حسابداری کشور برای طراحی مداخلات مؤثر ضروری است. پژوهش حاضر با رویکردی اکتشافی و با تکیه بر نظرسنجی از اعضای هیئت علمی، تلاش دارد تصویری روشن از وضعیت موجود و مسیرهای ممکن آینده ترسیم نماید. نتایج حاصل می‌تواند برای نهادهای سیاست‌گذار، مدیران گروه‌های آموزشی، و طراحان برنامه‌های درسی به‌عنوان مبنایی برای تصمیم‌گیری‌های راهبردی مورد استفاده قرار گیرد.

پژوهش حاضر با هدف اصلی شناسایی و تحلیل دیدگاه اعضای هیئت علمی گروه‌های حسابداری دانشگاه‌های ایران درباره گنجاندن درس تحلیل‌شناسی داده‌ها در برنامه درسی حسابداری انجام شده است.

پژوهش حاضر از دو جهت دارای نوآوری است:

- این نخستین مطالعه‌ای است که به‌صورت میدانی و با بهره‌گیری از ابزار پرسشنامه، دیدگاه طیف متنوعی از اعضای هیئت علمی گروه‌های حسابداری در ایران را نسبت به درس تحلیل‌شناسی داده‌ها بررسی می‌کند؛

[1] CPA revolution
[2] National Association of State Boards of Accountancy (NASBA)

- یافته‌های این مطالعه می‌تواند به‌عنوان پیش‌نیاز طراحی یک مدل بومی برای تلفیق تحلیل‌شناسی داده‌ها در برنامه درسی حسابداری کشور مورد استفاده قرار گیرد، مدلی که متناسب با ظرفیت‌ها، محدودیت‌ها و ترجیحات اساتید ایرانی باشد.

## مبانی نظری

در سال‌های اخیر، گسترش فناوری‌های نوین و افزایش حجم داده‌ها، نظام آموزش حسابداری را در سطح جهانی و ملی با چالش‌ها و فرصت‌های جدیدی روبه‌رو کرده است. به‌ویژه تلفیق مفاهیم «تحلیل‌شناسی داده» و «فناوری اطلاعات» در برنامه درسی حسابداری، به یکی از محورهای کلیدی تحول در آموزش عالی این حوزه تبدیل شده است. تلفیق تحلیل‌شناسی داده‌ها در آموزش حسابداری در سطح جهانی مورد توجه جدی قرار گرفته است. تغییرات آزمون تکامل حسابدار رسمی، اصلاحات استانداردهای اعتباربخشی انجمن پیشبرد مدارس دانشگاهی بازرگانی[1] به‌ویژه استاندارد A5 از جمله مهم‌ترین محرک‌های این تحول هستند (انجمن پیشبرد مدارس دانشگاهی بازرگانی، ۲۰۱۸؛ انجمن حسابداران رسمی آمریکا و انجمن ملی هیئت‌های حسابداری ایالتی، ۲۰۲۱: ۳).

مطالعاتی نظیر پژوهش لوسی و همکاران (۲۰۲۲) نشان می‌دهند که بسیاری از دانشکده‌های حسابداری در حال بازنگری برنامه‌های خود برای پوشش مهارت‌های تحلیلی هستند، اما چالش‌هایی نظیر کمبود اعضای هیئت علمی متخصص، هزینه‌های پیاده‌سازی و نبود اجماع درباره مهارت‌های ضروری، همچنان مطرح است.

فالگو و همکاران (۲۰۲۴) نیز با انجام مصاحبه با مدیران گروه‌های حسابداری، نشان داده‌اند که بیشتر برنامه‌های درسی از رویکرد ترکیبی[2] برای تلفیق تحلیل‌شناسی داده‌ها بهره گرفته‌اند و اغلب به مشارکت سایر گروه‌های آموزشی (نظیر سیستم‌های اطلاعاتی یا مدیریت) نیاز دارند. همچنین پژوهش کایناس و همکاران (۲۰۲۴) با تحلیل دیدگاه ۱۹۲ عضو هیئت علمی نشان داد که در عین حال که تحلیل‌شناسی داده‌ها به برنامه‌های درسی وارد شده است، هنوز در ارزیابی شایستگی‌های دانشجویان و استفاده نظام‌مند از بازخورد کارفرمایان، شکاف‌های معناداری وجود دارد.

[1] Association to Advance Collegiate Schools of Business (AACSB)
[2] Hybrid

در همین راستا، مطالعات گوناگونی در داخل کشور انجام شده است که در ادامه مرور می‌شود:

باقریان (۱۴۰۲) در مقاله‌ای با عنوان «*فناوری (سیستم اطلاعاتی) و مهارت‌های تجزیه و تحلیل‌شناسی داده‌ها در برنامه درسی حسابداری*»، وضعیت فعلی آموزش تحلیل‌شناسی داده‌ها در برنامه درسی حسابداری ایران را بررسی کرده و نتیجه گرفته است که بسیاری از برنامه‌های درسی از نظر پوشش مهارت‌های تحلیلی با استانداردهای جهانی فاصله دارند. وی پیشنهاد می‌کند درس مستقلی با عنوان تحلیل‌شناسی داده در برنامه کارشناسی گنجانده شود.

صیفی (۱۴۰۲) در پژوهشی با عنوان «*شناسایی مؤلفه‌های تلفیق سیستم‌های نوین حسابداری با مدیریت مالی*»، با استفاده از رویکرد داده‌بنیاد، به استخراج مؤلفه‌های کلیدی مؤثر بر تلفیق فناوری در آموزش حسابداری پرداخته است. وی عواملی همچون زیرساخت سازمانی، حمایت مدیریتی و توانمندی فناورانه اعضای هیئت علمی را مؤثر دانسته است.

عزیزی (۱۴۰۲) در مقاله‌ای با عنوان «*واکاوی مبانی فناوری اطلاعات و تأثیر آن بر بهره‌وری حسابداران کم‌تجربه*»، تأکید دارد که مهارت‌های مرتبط با داده‌ها و فناوری اطلاعات به‌ویژه برای دانش‌آموختگان جوان حسابداری، بسیار تعیین‌کننده است و توان ارتقای عملکرد آنان را دارد.

مقصودی و سلطانی (۱۴۰۳) در مقاله‌ای تحت عنوان «*کاربرد هوش مصنوعی در حسابداری و چشم‌انداز آینده کلان‌داده‌ها در این حوزه*»، به فرصت‌های پیش‌روی حسابداری در استفاده از هوش مصنوعی و تجزیه‌وتحلیل‌شناسی داده‌های حجیم اشاره کرده‌اند و بر لزوم ورود این مباحث به برنامه درسی دانشگاهی تأکید دارند.

نقدی و همکاران (۱۴۰۳) در پژوهشی با عنوان «*تجزیه و تحلیل کلان‌داده در حسابرسی با استفاده از هوش مصنوعی و تکنیک‌های یادگیری ماشینی*»، بر مزیت رقابتی حسابرسانی که به ابزارهای نوین تجزیه و تحلیل مجهز هستند تأکید کرده و پیشنهاد داده‌اند تا سرفصل‌های جدیدی در این راستا تدوین شود.

یافته‌های مرور پیشینه نشان می‌دهد که:

- بیشتر پژوهش‌های داخلی بر اهمیت و ضرورت ورود مفاهیم تحلیل‌شناسی داده به آموزش حسابداری اتفاق‌نظر دارند؛

- چالش‌هایی همچون کمبود استاد متخصص، ضعف زیرساخت فنی و نبود راهبرد مشخص در سطح ملی، به‌عنوان موانع کلیدی شناسایی شده‌اند؛
- هنوز پژوهشی جامع که با رویکرد میدانی و مبتنی بر دیدگاه اعضای هیئت علمی حسابداری به این موضوع بپردازد، انجام نشده است.

بنابراین، پژوهش حاضر تلاش می‌کند تا با تحلیل دیدگاه اعضای هیئت علمی گروه‌های حسابداری دانشگاه‌های ایران، شکاف موجود در پیشینه را پوشش داده و تصویری روشن از ظرفیت‌ها، موانع و مسیرهای ممکن برای گنجاندن درس تحلیل‌شناسی داده‌ها در برنامه درسی فراهم آورد.

## روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، کاربردی و از نظر روش گردآوری داده‌ها، توصیفی–پیمایشی است. این مطالعه با بهره‌گیری از ابزار پرسشنامه و با هدف بررسی دیدگاه اعضای هیئت علمی حسابداری نسبت به ضرورت، امکان‌پذیری و چالش‌های گنجاندن درس تحلیل‌شناسی داده‌ها در برنامه درسی، انجام شده است.

جامعه آماری پژوهش شامل کلیه اعضای هیئت علمی گروه‌های حسابداری دانشگاه‌های دولتی، آزاد اسلامی و پیام نور در سراسر کشور در سال تحصیلی ۱۴۰۳–۱۴۰۴ می‌باشد. به منظور دسترسی به نمونه‌ای متنوع و دارای نمایندگی کافی از نظر مرتبه علمی، سابقه تدریس و محل خدمت، از روش نمونه‌گیری هدفمند و در دسترس استفاده شده است.

پرسشنامه الکترونیکی طراحی‌شده، با استفاده از سامانه «پُرس‌لاین» تهیه و از طریق ایمیل و شبکه‌های رسمی هیئت‌های علمی به‌صورت مستقیم برای پاسخ‌دهندگان ارسال گردید. از مجموع ۷۴ پرسشنامه ارسال‌شده، تعداد ۴۹ پرسشنامه قابل استفاده با نرخ بازگشت حدود ۶۶٪ جمع‌آوری و داده‌های گردآوری‌شده پس از پالایش اولیه، وارد نرم‌افزار اکسل و سپس تحلیل شدند. تحلیل‌ها به‌صورت توصیفی و تفسیری، با تمرکز بر ابعاد جمعیت‌شناختی، نگرشی و ساختاری پاسخ‌ها صورت گرفت. یافته‌ها، تصویری چندبعدی از سطح آگاهی، نیازهای آموزشی، چالش‌های اجرایی، و آمادگی نهادی برای گنجاندن درس تحلیل‌شناسی داده در آموزش حسابداری ارائه می‌دهند.

ابزار اصلی گردآوری داده‌ها در این پژوهش، پرسشنامه محقق‌ساخته بود که بر اساس مبانی نظری، پیشینه پژوهش‌های بین‌المللی (مانند آندیولا و همکاران[1]، ۲۰۲۰؛ کایناس و همکاران، ۲۰۲۴ و لوسی و همکاران، ۲۰۲۲) و الگوهای معتبر طراحی گردید. پرسشنامه شامل سه بخش اصلی است:

۱) اطلاعات دموگرافیک (مرتبه علمی، سابقه تدریس، نوع دانشگاه و محل خدمت)

۲) سنجش نگرش نسبت به ضرورت و مزایای گنجاندن درس تحلیل داده‌ها (با طیف لیکرت ۵ درجه‌ای)

۳) سنجش دیدگاه نسبت به چالش‌ها و موانع پیاده‌سازی درس تحلیل داده‌ها (سؤالات چندگزینه‌ای و باز پاسخ)

برای اطمینان از روایی صوری و محتوایی پرسشنامه، نسخه اولیه آن در اختیار چند نفر از اعضای هیئت علمی حسابداری و برنامه‌ریزان درسی قرار گرفت و بر اساس نظرات اصلاح شد. به علاوه طراحی سوالات بر مبنای مرور پیشینه نظری و مطالعات مشابه انجام شد که روایی محتوایی ابزار را تقویت می‌کند. همچنین، برای سنجش پایایی، ضریب آلفای کرونباخ برای بخش اصلی پرسشنامه محاسبه شد که برابر با ۰/۷۱۷ به‌دست آمد که نشان‌دهنده پایایی مناسب ابزار است.

در بخش نخست تجزیه‌وتحلیل، داده‌های دموگرافیک پاسخ‌دهندگان شامل جنسیت، مرتبه علمی، سابقه تدریس، حوزه تدریس و سوابق حرفه‌ای بررسی شد تا زمینه‌ای برای ارزیابی ترکیب تخصصی نمونه پژوهش فراهم شود. سپس، سؤالات اصلی پژوهش در قالب ۱۳ نمودار موضوعی تحلیل گردید. برای تحلیل این نمودارها، ابتدا فراوانی و درصد هر گزینه استخراج و سپس در چارچوب مفهومی مرتبط با اهداف پژوهش تفسیر شد. تمرکز اصلی تحلیل‌ها بر شناسایی وضعیت موجود (سطح آگاهی، مهارت، منابع و زیرساخت‌ها)، ترجیحات آموزشی (روش تدریس، منابع، ارزیابی)، و چالش‌های اجرایی (نهادی، زیرساختی، فرهنگی) بود.

در مرحله بعد، داده‌ها با رویکرد کیفی تفسیری مورد تجزیه‌وتحلیل قرار گرفت تا ضمن درک الگوهای پاسخ‌دهی، زمینه‌های سیاست‌گذاری و توصیه‌های راهبردی برای طراحی و اجرای درس «تحلیل‌شناسی داده» استخراج شود. در مجموع، روش تحلیل داده‌ها در این

[1] Andiola et al.

پژوهش، ترکیبی از آمار توصیفی و تحلیل محتوای کیفی بود که امکان بررسی عمیق‌تری از ادراکات، نگرش‌ها و آمادگی نهادی را فراهم ساخت و چارچوبی جامع برای استنتاج‌های راهبردی در حوزه طراحی برنامه‌های درسی بین‌رشته‌ای در اختیار قرار داد.

## یافته‌های پژوهش

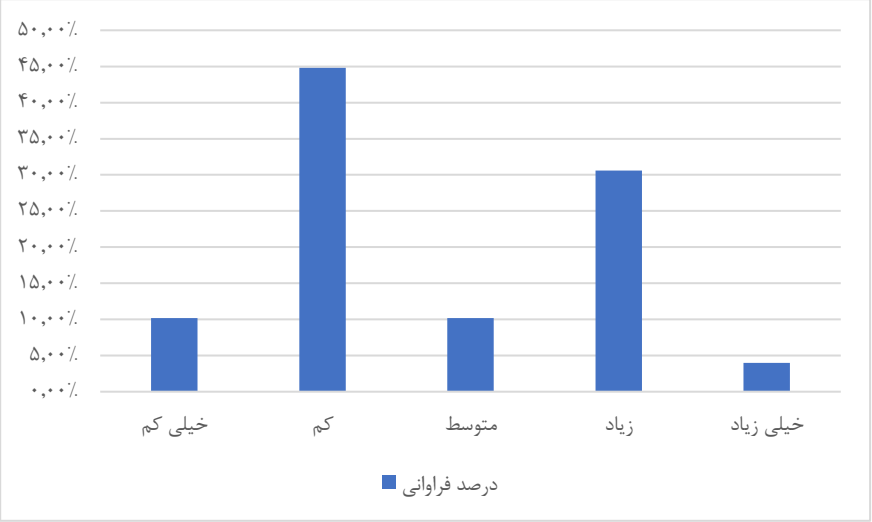
نتایج بخش دموگرافیک پاسخ‌دهندگان به پرسشنامه نشان می‌دهد که نمونه مورد بررسی از تنوع مناسبی از نظر ویژگی‌های فردی و حرفه‌ای برخوردار است. از مجموع ۴۹ عضو هیئت علمی پاسخ‌دهنده، ۷۷/۵ درصد مرد و ۲۲/۴ درصد زن بوده‌اند. از نظر سابقه تدریس، نزدیک به ۸۸ درصد دارای بیش از ۱۰ سال سابقه‌اند که بیانگر تجربه بالا در حوزه آموزش حسابداری است. همچنین، اکثریت پاسخ‌دهندگان دارای مرتبه علمی دانشیار (۴۰/۴ درصد) و استادیار (۳۸/۲ درصد) بوده‌اند که به اعتبار تخصصی نظرات آن‌ها می‌افزاید.

از منظر حرفه‌ای نیز، حدود ۷۴ درصد از پاسخ‌دهندگان سابقه فعالیت حرفه‌ای مرتبط دارند که بیش از نیمی از آن‌ها دارای سابقه‌ای بالای ۱۰ سال بوده‌اند. همچنین، ۸/۴۲ درصد عضو انجمن حسابداران خبره و به همان میزان نیز عضو کانون کارشناسان رسمی بوده‌اند. در حوزه تدریس، حسابداری مالی (۷۷/۵ درصد)، حسابداری مدیریت (۵۳ درصد) و حسابداری صنعتی (۳۶/۷ درصد) بیشترین فراوانی را داشته‌اند. این ترکیب از تجربیات دانشگاهی و حرفه‌ای، پشتوانه‌ای مناسب برای ارزیابی ضرورت گنجاندن درس تحلیل‌شناسی داده در برنامه درسی حسابداری فراهم می‌آورد، چراکه نظرات ارائه‌شده متکی بر درک عمیق از نیازهای آموزشی و بازار کار است.

تحلیل محتوایی پرسشنامه توزیع‌شده میان اعضای هیئت علمی حسابداری در دانشگاه‌های کشور، تصویری روشن از وضعیت موجود و نیازهای بالقوه برای گنجاندن درس «تحلیل‌شناسی داده» در برنامه درسی ارائه می‌دهد. داده‌ها در قالب ۱۱ محور موضوعی گردآوری شده‌اند که در ادامه به تفصیل تحلیل می‌شوند.

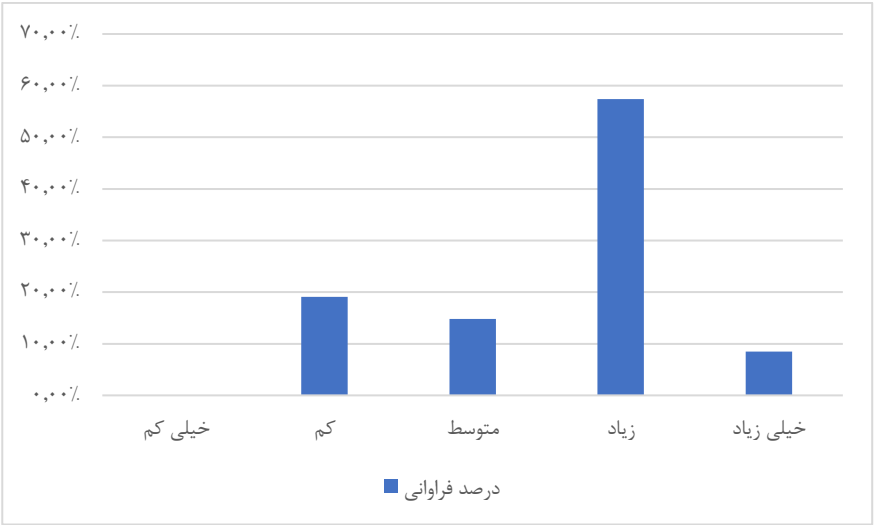
### ۱. شکاف دانشی در شناخت تحلیل‌شناسی داده

یافته‌های حاصل از نمودار ۱ حاکی از آن است که سطح آگاهی اعضای گروه‌های حسابداری نسبت به مفاهیم و کاربردهای تحلیل‌شناسی داده عموماً در سطح متوسط یا پایین قرار دارد. این امر بیانگر آن است که دانش میان‌رشته‌ای مرتبط با تحلیل داده هنوز جایگاه تثبیت‌شده‌ای در میان هیئت علمی گروه‌های حسابداری نیافته است. چنین شکاف دانشی، می‌تواند ناشی از فقدان برنامه‌ریزی برای ارتقاء دانش ضمن‌خدمت، کم‌توجهی به تحولات فناورانه حوزه حسابداری، و عدم گنجاندن موضوعات تحلیلی در برنامه‌های بازآموزی اساتید باشد.




**نمودار ۱.** ارزیابی سطح آگاهی اعضای گروه حسابداری درباره تحلیل‌شناسی داده

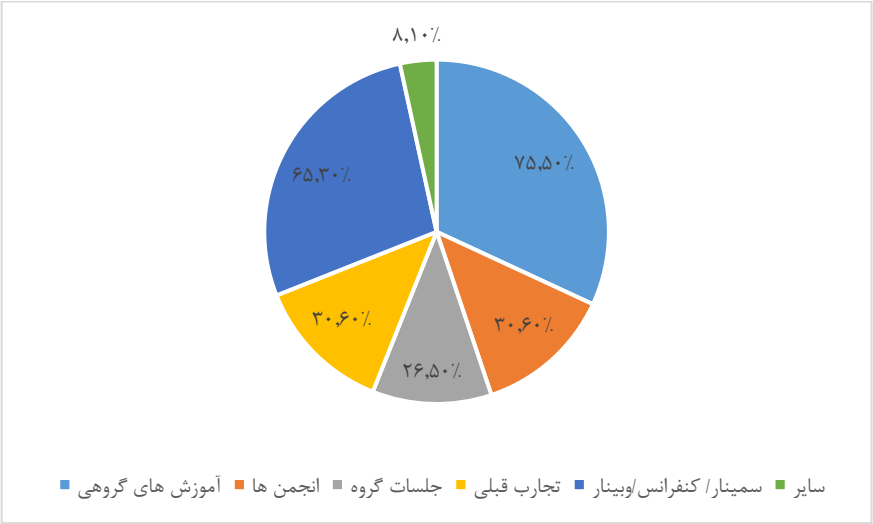
نمودار ۲ تکمیل‌کننده ارزیابی پیشین است و بر سطح پایین خودارزیابی اعضای هیئت علمی در آشنایی با مفاهیم تحلیل داده دلالت دارد. این یافته نه‌تنها نشان‌دهنده نبود حمایت نهادی در حوزه توانمندسازی حرفه‌ای است، بلکه از فقدان انگیزه یا فرصت کافی برای ارتقای دانش فردی نیز حکایت دارد. بنابراین، طراحی سیاست‌های حمایتی در سطوح فردی و سازمانی برای ارتقای آگاهی تحلیلی در بین اساتید ضروری به نظر می‌رسد.




**نمودار ۲.** ارزیابی سطح آگاهی خود فرد درباره تحلیل‌شناسی داده

## ۲. روش‌های مؤثر در یادگیری تحلیل داده

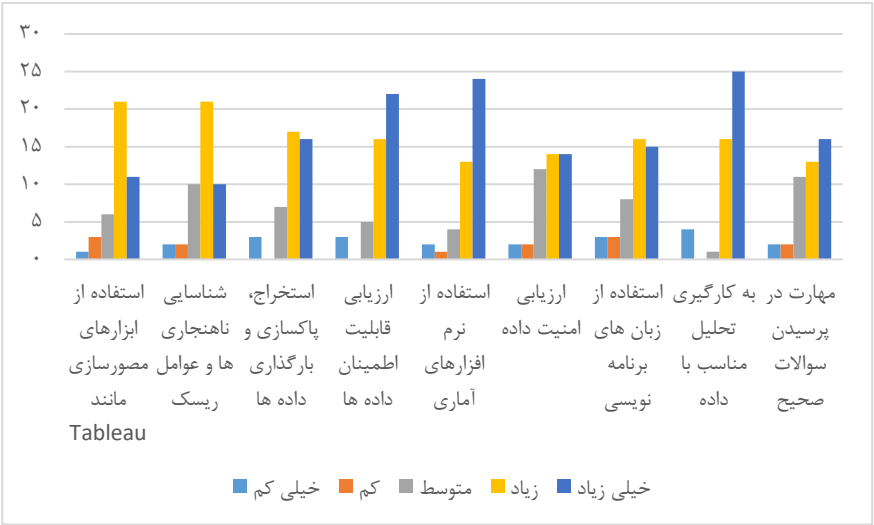
یافته‌های نمودار ۳ نشان می‌دهد که یادگیری این حوزه عمدتاً از طریق آموزش‌های گروهی و مشارکت فعال در دوره‌های تخصصی مانند سمینارها و وبینارها امکان‌پذیر است. این ترجیح بیانگر گرایش اساتید به روش‌های تعاملی و تجربی در یادگیری مفاهیم نوین است. یافته مذکور می‌تواند مبنایی برای طراحی برنامه‌های توانمندسازی با محوریت یادگیری فعال و گروه‌محور فراهم آورد.




**نمودار ۳.** موثرترین روش‌ها در شناخت مفهوم تحلیل‌شناسی داده

## ۳. مهارت‌های کلیدی برای آموزش

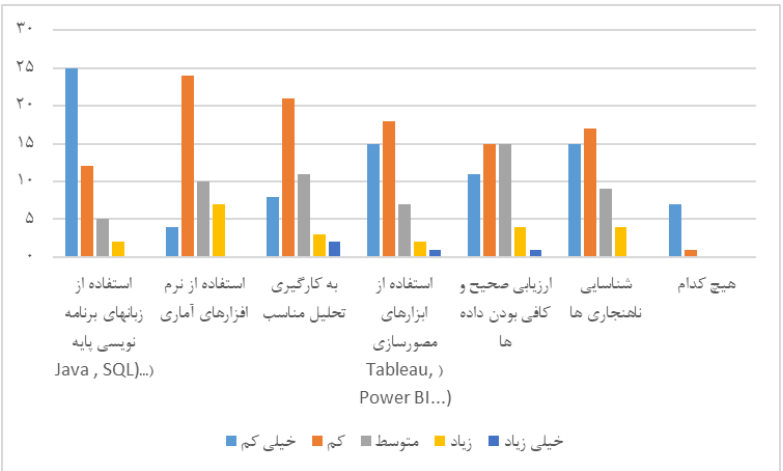
بر اساس نمودار ۴، مهارت‌هایی نظیر تحلیل داده‌های مالی، تسلط به نرم‌افزارهای آماری، توانایی تفکر انتقادی، و ارائه تصویری نتایج، به‌عنوان مهارت‌های کلیدی در آموزش این درس شناخته شده‌اند. این اولویت‌بندی، لزوم طراحی درسی با محوریت کاربردی و تحلیلی را گوشزد می‌کند و حاکی از تقاضای بازار برای مهارت‌هایی فراتر از دانش نظری صرف در حوزه حسابداری است.




**نمودار ٤.** مهم‌ترین مهارت‌ها در درس تحلیل‌شناسی داده

## ٤. ضعف جدی مهارتی در میان دانشجویان

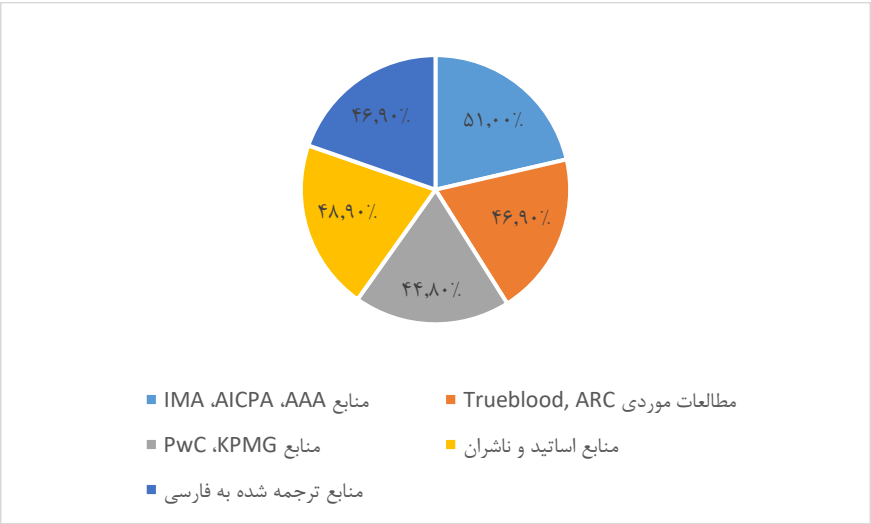
یافته‌های نمودار ۵ از ضعف آشکار دانشجویان در اغلب مهارت‌های تحلیلی پرده برمی‌دارند. این خلأ مهارتی بیانگر آن است که نه‌تنها محتوای دروس فعلی پاسخگوی نیازهای تحلیلی بازار نیست، بلکه روش‌های ارزیابی و آموزش نیز در ایجاد شایستگی‌های کاربردی ناکارآمد بوده‌اند. این امر ضرورت بازنگری فوری در شیوه‌های آموزشی را برجسته می‌سازد.




**نمودار ۵.** میزان مهارت دانشجویان در هریک از مهارت‌ها

## ۵. منابع آموزشی مطلوب

بر اساس نتایج ارائه‌شده در نمودار ۶، ترجیحات منابع آموزشی برای درس تحلیل‌شناسی داده در میان پاسخ‌دهندگان به‌صورت نسبتاً متوازن اما با اولویت‌های مشخص توزیع شده است.




**نمودار ٦.** بهترین منابع آموزشی برای درس تحلیل‌شناسی داده‌ها

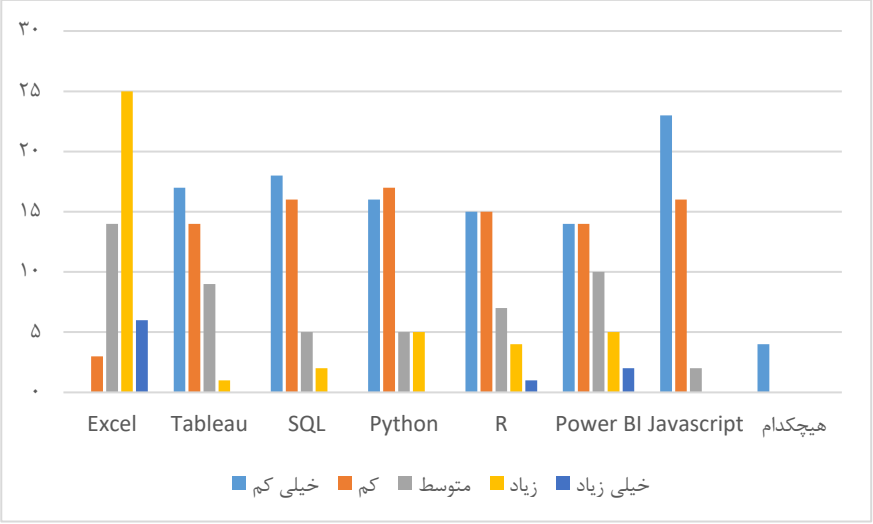
نتایج نشان می‌دهد که منابع ترجمه‌شده به فارسی با اختصاص ۵۱ درصد از آرا، بالاترین میزان استقبال را داشته‌اند. این یافته اهمیت انکارناپذیر دسترسی به منابع بومی‌سازی‌شده و قابل‌فهم برای دانشجویان، به‌ویژه در دروسی با محتوای تحلیلی و فنی را نشان می‌دهد. در رتبه‌های بعدی، مطالعات موردی Trueblood و ARC با ۴۹/۲ درصد و منابع اساتید و نشریات تخصصی با ۴۸/۷ درصد قرار دارند که این امر بیانگر تمایل قابل توجه به استفاده از منابع کاربردی و تجربی در کنار مبانی نظری است. همچنین منابع سازمان‌های حرفه‌ای همچون انجمن حسابداران مدیریت[1]، انجمن حسابداران رسمی آمریکا و انجمن حسابداران آمریکا با سهم ۴۸/۹ درصد نشان‌دهنده اهمیت استفاده از منابع استاندارد و معتبر بین‌المللی در فرایند آموزش تحلیل داده‌ها است. در نهایت، منابع موسسات حسابرسی پی‌دبلیوسی[2] و کی‌پی‌ام‌جی[3] با ۴۸/۶ درصد نیز در سطحی تقریباً مشابه مورد توجه قرار گرفته‌اند که نشان می‌دهد بهره‌گیری از تجربیات

[1] Institute of Management Accountants (IMA)
[2] PwC
[3] KPMG

عملی شرکت‌های پیشرو در حوزه تحلیل داده نیز برای آموزش مؤثر است. در مجموع، می‌توان نتیجه گرفت که هیچ منبعی به تنهایی پاسخگوی نیازهای آموزشی این درس نیست و استفاده ترکیبی از منابع بومی‌سازی‌شده، مطالعات موردی، منابع حرفه‌ای و تجربیات سازمانی می‌تواند اثربخش‌ترین راهکار آموزشی باشد.

### ۶. توانمندی اعضای هیئت علمی در استفاده از ابزارهای تحلیلی

نمودار ۷ بیانگر آن است که تسلط هیئت علمی به ابزارهای کلیدی تحلیل‌شناسی داده نظیر اکسل پیشرفته، Power BI، Python و R بسیار محدود است. این شکاف تکنولوژیکی می‌تواند چالشی جدی در مسیر تدریس موثر این درس باشد و نشان‌دهنده نیاز به سرمایه‌گذاری گسترده در آموزش این ابزارها به اساتید است.



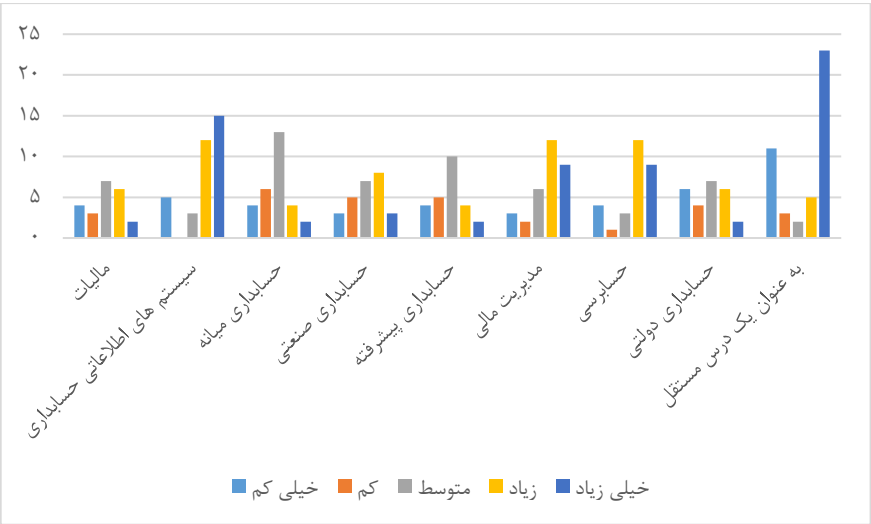

**نمودار ۷.** میزان تسلط اعضای هیئت علمی به هریک از نرم‌افزارها

### ۷ .ساختار مطلوب گنجاندن درس در برنامه درسی

یافته‌های نمودارهای ۸ و ۹ نشان می‌دهد که کارشناسی ارشد، مقطع مناسب‌تری برای گنجاندن این درس است.




**نمودار ۸.** مناسب‌ترین مقطع برای تدریس تحلیل‌شناسی داده



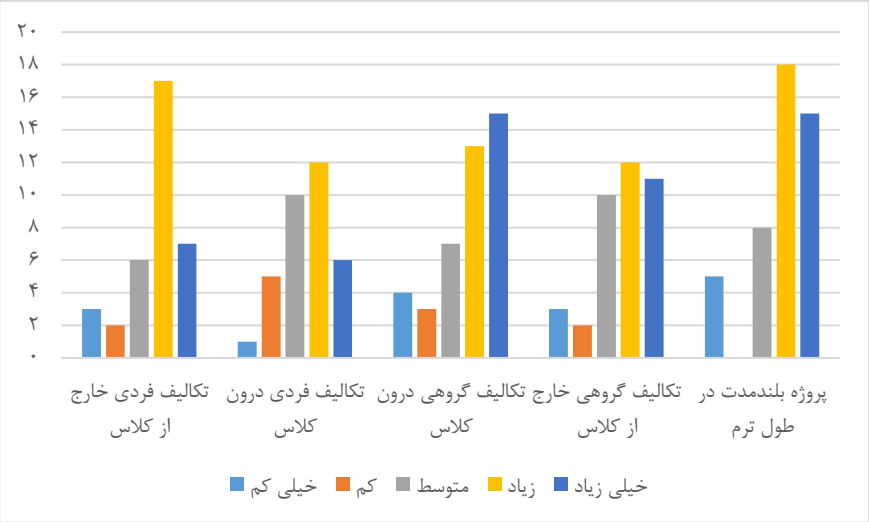

**نمودار ۹.** مناسب‌ترین درس برای تلفیق تحلیل‌شناسی داده

این انتخاب از منطق آموزش تخصصی و سطح‌بندی شناختی پیروی می‌کند و انتظار می‌رود دانشجویان در این مقطع از آمادگی مفهومی فنی بیشتری برای درک مباحث تحلیلی برخوردار باشند. پیشنهاد اساتید این است که این درس به صورت مستقل و مجزا از سایر دروس و در رتبه

بعدی به صورت تلفیقی در درس سیستم‌های اطلاعاتی گنجانده شود. این ساختار به دلیل ارتباط مستقیم این درس با تحلیل‌های عددی و تصمیم‌گیری مالی، منطبق با اهداف درس تحلیل‌شناسی داده است.

## ۸. سنجش اثربخش یادگیری

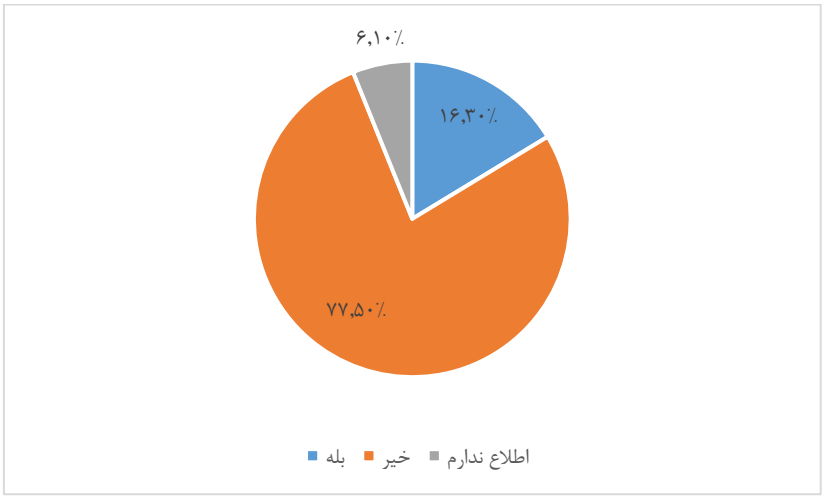
در نمودار ۱۰، تکالیفی مانند پروژه‌های بلندمدت در طول ترم و تکالیف گروهی درون کلاس به‌عنوان مؤثرترین ابزارهای سنجش معرفی شده‌اند. این رویکرد، ارزشیابی سنتی را به چالش کشیده و بر اهمیت ارزیابی مبتنی بر عملکرد تأکید می‌کند.




**نمودار ۱۰.** مناسب‌ترین تکالیف برای سنجش مهارت دانشجویان در تحلیل‌شناسی داده

## ۹ .فقدان سیاست‌گذاری و ساختار اجرایی

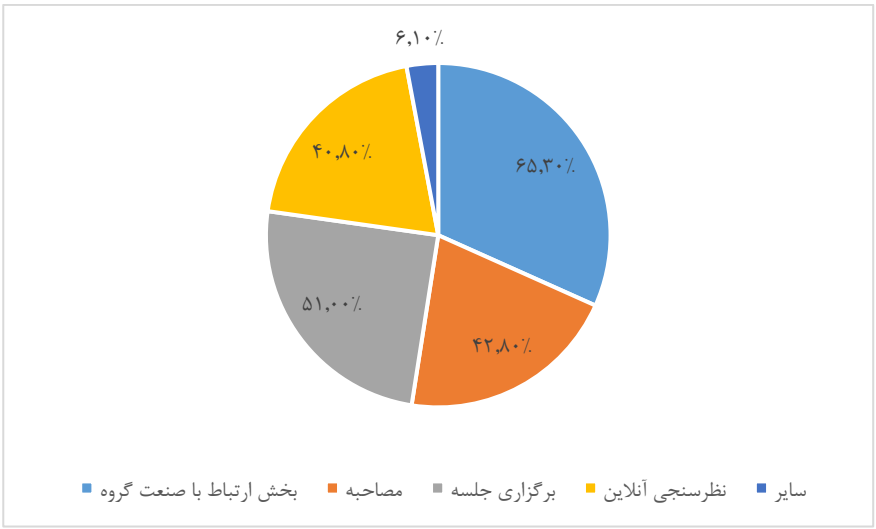
یافته‌های نمودار ۱۱ نشان می‌دهد که بیشتر گروه‌های آموزشی فاقد هدف یا برنامه مدون برای آموزش تحلیل‌شناسی داده هستند. این امر بیانگر ضعف راهبردی در سیاست‌گذاری درسی و خلأ راهبردی در تدوین برنامه‌های درسی به‌روز و عدم آمادگی ساختاری برای پذیرش دروس جدید است.




**نمودار ۱۱.** وجود برنامه/هدف در گروه حسابداری برای آموزش تحلیل‌شناسی داده

### ۱۰. ارتباط با نیازهای بازار کار

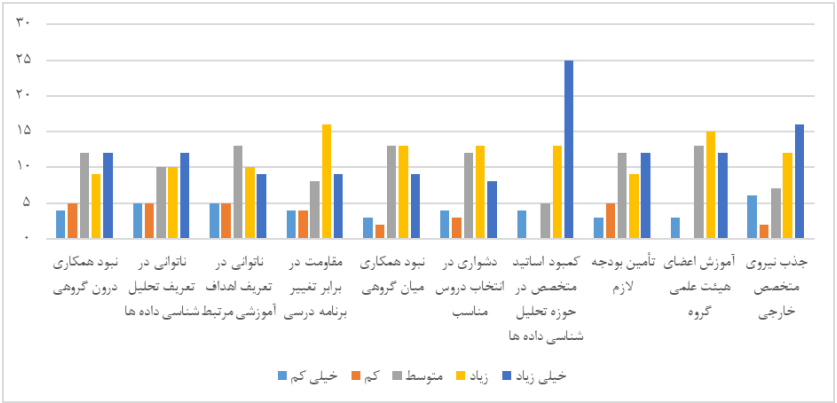
نمودار ۱۲ نشان می‌دهد که در همکاری با نهادهای حرفه‌ای، گروه ارتباط با صنعت و برگزاری جلسات با آنان از جمله مهم‌ترین ابزارها برای شناخت انتظارات کارفرمایان است. با این حال، استفاده مؤثر از این منابع در تصمیم‌گیری‌های آموزشی نیازمند ساختارمند شدن این کانال‌ها در قالب کمیته‌های برنامه‌ریزی درسی است.




**نمودار ۱۲.** بهترین کانال‌ها برای کسب اطلاع از نیاز و انتظارات کارفرمایان

## ۱۱. چالش‌های اجرایی

طبق نمودار ۱۳، مهم‌ترین موانع اجرای این درس شامل کمبود اساتید متخصص، ضعف زیرساخت آموزشی، و مقاومت فرهنگی در برابر تغییر است. رفع این چالش‌ها نیازمند برنامه‌ریزی کلان، حمایت نهادی و ایجاد انگیزه در بین اساتید و مدیران آموزشی است.




**نمودار ۱۳.** مهم‌ترین چالش‌ها در گنجاندن درس تحلیل‌شناسی داده در رشته حسابداری

تحلیل‌های فوق نشان می‌دهند که گنجاندن درس تحلیل‌شناسی داده در برنامه درسی رشته حسابداری نه‌تنها ضروری، بلکه اجتناب‌ناپذیر است. فقدان مهارت‌های تحلیلی در میان دانشجویان، ضعف آگاهی اعضای هیئت علمی، و تغییرات سریع در نیازهای بازار کار، همگی گواهی بر اهمیت طراحی و اجرای این درس دارند. با این حال، تحقق این هدف مستلزم ارتقاء مهارتی اساتید، تغییر ساختار ارزشیابی و اتخاذ سیاست‌های حمایتی از سوی نهادهای دانشگاهی و حرفه‌ای است.

## بحث و نتیجه‌گیری

یافته‌های این پژوهش نشان می‌دهد که گنجاندن درس «تحلیل‌شناسی داده» در برنامه درسی رشته حسابداری، نه‌تنها یک ضرورت آموزشی بلکه ضرورتی راهبردی برای هم‌راستاسازی نظام دانشگاهی با تحولات فناورانه و نیازهای بازار کار به‌شمار می‌رود. نتایج حاصل از تحلیل داده‌های گردآوری‌شده از اعضای هیئت علمی حسابداری دانشگاه‌های کشور در قالب ۱۳ محور موضوعی، مؤید آن است که ساختار موجود برنامه درسی در پاسخ‌گویی به تحولات مرتبط با داده‌محوری و تحلیل‌های پیشرفته، با نارسایی‌های چندگانه مواجه است.

از منظر دانشی، سطح آگاهی اساتید و گروه‌های آموزشی نسبت به مفاهیم تحلیل داده در سطح پایینی قرار دارد که بیانگر غفلت از آموزش‌های ضمن‌خدمت و فقدان چارچوب یادگیری رسمی در این حوزه است. این ضعف دانشی با توانمندی اندک اساتید در استفاده از نرم‌افزارهای تحلیلی نیز هم‌راستا بوده و به‌عنوان مانعی اساسی در تدریس مؤثر این درس تلقی می‌شود. همچنین، ارزیابی مهارت‌های دانشجویان نشان داد که شایستگی‌های تحلیلی در میان آن‌ها به‌شدت محدود است؛ امری که نشان از ناکارآمدی روش‌های فعلی آموزشی دارد.

از سوی دیگر، پاسخ‌دهندگان به منابع ترجمه‌شده، مطالعات موردی، منابع حرفه‌ای بین‌المللی و تجربیات سازمانی به‌عنوان منابع آموزشی ترجیحی اشاره کرده‌اند، که گویای لزوم طراحی دوره‌هایی با رویکرد یادگیری ترکیبی و تلفیق نظریه و عمل است. همچنین، مقطع کارشناسی ارشد و تلفیق با دروس سیستم‌های اطلاعاتی به‌عنوان ساختار مطلوب ارائه این درس شناخته شده‌اند.

با این حال، یافته‌ها نشان می‌دهد که اکثر گروه‌های حسابداری فاقد سیاست مدون یا ساختار اجرایی برای پذیرش و پیاده‌سازی این درس هستند و با چالش‌هایی چون کمبود اساتید متخصص، ضعف زیرساخت و مقاومت فرهنگی مواجه‌اند. از سوی دیگر، ارتباط گروه‌های آموزشی با نهادهای

حرفه‌ای و کارفرمایان که می‌تواند منبعی ارزشمند برای بازطراحی برنامه‌های درسی باشد، هنوز ساختارمند نشده و بهره‌برداری مناسبی از آن صورت نمی‌گیرد.

در مجموع، نتایج این مطالعه مؤید آن است که تحقق اثربخش درس تحلیل‌شناسی داده‌ها مستلزم رویکرد کل‌نگر است که از سویی توانمندسازی اعضای هیئت علمی و توسعه زیرساخت‌های نرم‌افزاری و سخت‌افزاری را هدف قرار دهد و از سوی دیگر، سیاست‌گذاری آموزشی را در راستای هم‌افزایی میان دانشگاه و صنعت هدایت کند. تحقق این امر می‌تواند زمینه‌ساز تربیت دانش‌آموختگانی با مهارت‌های تحلیلی پیشرفته، تصمیم‌گیری داده‌محور و آمادگی ورود به بازار کار رقابتی قرن بیست‌ویکم باشد.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع

باقریان، مهدی. (۱۴۰۲). فناوری (سیستم اطلاعاتی) و مهارت‌های تجزیه و تحلیل‌شناسی داده‌ها در برنامه درسی حسابداری. *دانش حسابداری مالی*، ۱۵(۴۹)، ۱۲۳–۱۴۰. https://doi.org/10.30479/jfak.2023.19432.3131

صیفی، الهام. (۱۴۰۲). شناسایی مؤلفه‌های تلفیق سیستم‌های نوین حسابداری با مدیریت مالی. *نهمین کنفرانس ملی یافته‌های نوین در مدیریت، کامپیوتر و حسابداری*، سنندج، ایران. https://civilica.com/doc/1751742

عزیزی، فهیمه. (۱۴۰۲). واکاوی مبانی فناوری اطلاعات و تأثیر آن بر بهره‌وری حسابداران کم‌تجربه در این حوزه. *مطالعات اقتصاد، مدیریت مالی و حسابداری*، ۹(۳)، ۷۱–۸۱. https://civilica.com/doc/1970500

مقصودی، نصرالله؛ سلطانی، رقیه. (۱۴۰۳). کاربرد هوش مصنوعی در حسابداری و چشم‌انداز آینده کلان‌داده‌ها در این حوزه. *نوزدهمین کنفرانس ملی اقتصاد، مدیریت و حسابداری*، تهران، ایران. https://civilica.com/p/1771973/

نقدی، سجاد؛ فضل‌زاده، علیرضا؛ احمدیان، وحید؛ عباس محسن الطیاوی، مریم. (۱۴۰۳). تجزیه و تحلیل کلان‌داده در حسابرسی با استفاده از هوش مصنوعی و تکنیک‌های یادگیری ماشینی. *سومین کنفرانس بین‌المللی اقتصاد و مدیریت کسب‌وکار*، مشهد، ایران. https://civilica.com/p/1790533/

## References


AICPA & NASBA. (2021). *CPA Evolution Model Curriculum*. American Institute of Certified Public Accountants. https://www.aicpa.org/resources/download/cpa-evolution-model-curriculum

Andiola, L. M., Masters, E., & Norman, C. (2020). Integrating technology and data analytic skills into the accounting curriculum: Accounting department leaders' experiences and insights. Journal of Accounting Education, 50, 100655. https://doi.org/10.1016/j.jaccedu.2020.100655

Association to Advance Collegiate Schools of Business (AACSB). (2018). 2018 accounting accreditation standards: Eligibility procedures and accreditation standards for accounting accreditation. Standard A5: Information technology skills.

Azizi, F. (2023). Exploring the foundations of information technology and its impact on the productivity of novice accountants. *Journal of Economic, Financial Management and Accounting Studies*, 9(3), 71–81. https://civilica.com/doc/1970500 (in Persian)

Bagherian, M. (2023). Information systems technology and data analytics skills in the accounting curriculum. *Financial Accounting Knowledge*, 15(49), 123–140. https://doi.org/10.30479/jfak.2023.19432.3131 (in Persian)

Cainas, J. M., Hasson, B. K., & Kralik, J.M. (2024). Accounting faculty perspectives on data analytics: Course design, competency assessment, and employer needs and response. *Issues in Accounting Education*, 40(2), 23-44. https://doi.org/10.2308/ISSUES-2022-031

Chu, M. K., & Yong, K. O. (2021). Big data analytics for business intelligence in accounting and audit. Open Journal of Social Sciences, 9(9), 42–52. https://doi.org/10.4236/jss.2021.99004

Falgout, S., Boyle, D. M., Gaydon, D. J., & Hermanson, D. R. (2024). Data analytics integration approaches: Insights from accounting chairs. *Issues in Accounting Education*, 39(3), 31–44. https://doi.org/10.2308/ISSUES-2022-030

Janvrin, D. J., & Watson, M. W. (2017). Big data: A new twist to accounting. *Journal of Accounting Education*, 38, 3–8. https://doi.org/10.1016/j.jaccedu.2016.12.009

Losi, H. J., Isaacson, E. V., & Boyle, D. M. (2022). Integrating data analytics into the accounting curriculum: Faculty perceptions and insights. *Issues in Accounting Education*, 37(4), 1–23. https://doi.org/10.2308/ISSUES-2021-086

Maghsoudi, N., & Soltani, R. (2024). Application of artificial intelligence in accounting and the future outlook of big data in the field. *In 19th National Conference on Economics, Management and Accounting*, Tehran, Iran. https://civilica.com/p/1771973/ (in Persian)

Naghdi, S., Fazlzadeh, A., Ahmadian, V., & Abbas-Mohsen Altiavi, M. (2024). Big data analytics in auditing using artificial intelligence and machine learning techniques. *In 3rd International Conference on Economics and Business Management*, Mashhad, Iran. https://civilica.com/p/1790533/ (in Persian)

Seifi, E. (2023). Identifying components of integrating modern accounting systems with financial management. *In 9th National Conference on New Findings in Management, Computer and Accounting*, Sanandaj, Iran. https://civilica.com/doc/1751742 (in Persian)



COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Research Paper**

# IT Governance through a Novel Ranking Model for COBIT Information Technology Security Controls [1]

**Saeed Rouhani* [2] and Mohammad Nikbakht[3]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 29-60

Received: 2026.08.18
Revised: 2026.10.02
Accepted: 2026.10.30

## Abstract

With organizations' increasing dependence on information technology (IT), the risk of security threats has grown significantly. Therefore, organizations must prioritize the protection of IT security and the implementation of appropriate security controls. COBIT 2019 is a comprehensive framework for IT governance that provides numerous security controls to maintain IT security. This framework addresses IT security through two processes—"APO13: Managed Security" and "DSS05: Managed Security Services"—and defines a total of 10 security controls for this purpose. The aim of this paper is to use a multi-criteria decision-making (MCDM) approach to determine the importance of security controls in the COBIT 2019 framework. To achieve this goal, two MCDM methods, namely AHP and TOPSIS, were used to compare and rank the security controls of the COBIT 2019 framework based on five COBIT information criteria. First, the weights of the criteria were calculated using the AHP method, and then the TOPSIS method was used to rank the security controls based on their scores. According to the results, the "Protect Against Malicious Software" control achieved the highest rank, with a score of 0.763, whereas the "Manage Sensitive Documents and Output Devices" control ranked lowest, with a score of 0.280. The findings of this study can serve as a valuable resource for various security teams, enabling them to enhance the effectiveness and precision of their organizations' IT security management practices. The proposed model provides a valuable decision-support tool for security teams, enabling them to implement more effective controls to prevent security threats. In turn, this can contribute to reducing implementation time and costs, improving organizational performance, and enhancing operational efficiency.

**Keywords**: Technology Governance, Security Controls, COBIT 2019, MCDM, AHP, TOPSIS, Ranking.

**JEL classification:** *M15, C44, L86.*

---

[1] https://doi.org/10.22034/JISTA.2026.608452.1113
[2] Associate Professor, Department of Management, University of Tehran, Tehran, Iran. (Corresponding Author). Email: srouhani@ut.ac.ir
[3] Ph.D. Student, Saman Bank, Tehran, Iran. Email: mohammadnikbakht @ut.ac.ir

## 1. INTRODUCTION And OBJECTIVE

Organizations are increasingly dependent on information technology (IT), and this dependence has significantly increased the risk of security threats (Xu and Lu, 2022; Taherdoost, 2023). Security is therefore an essential aspect of IT governance, and organizations must protect IT systems as they protect other assets (Ghelani et al., 2022). COBIT 2019 is a comprehensive IT governance framework that defines 40 processes in five domains (ISACA, 2018). It addresses security through two processes, "APO13: Managed Security" and "DSS05: Managed Security Services," and defines 10 security controls for these processes. However, COBIT does not specify a clear priority for selecting and implementing these controls. This gap can confuse organizations about which controls to implement first, especially when resources are limited. Previous studies have applied MCDM methods to COBIT 5 process prioritization (Almeida et al., 2018) and IT project portfolio selection (Ahriz et al., 2018), but the security controls of COBIT 2019 have not been ranked through a combined AHP–TOPSIS model. The objective of this paper is therefore to compare and rank the 10 COBIT 2019 security controls using five COBIT information criteria and a multi-criteria decision-making (MCDM) approach.

## 2. MATERIALS AND METHODS

The study uses a combination of the analytic hierarchy process (AHP) and the technique for order of preference by similarity to ideal solution (TOPSIS). AHP is used to calculate the weights of the criteria, and TOPSIS is used to rank the alternatives. This combination is appropriate because AHP performs well in weighting and consistency checking (Saaty, 1980), while TOPSIS performs well when the number of alternatives is large and requires fewer calculations (Hwang and Yoon, 1981). The criteria are the five COBIT information criteria: confidentiality (C1), integrity (C2), availability (C3), compliance (C4), and reliability (C5). The alternatives are the 10 security controls defined in APO13 and DSS05. A single decision-maker with 11 years of experience in IT

governance and COBIT completed the pairwise comparison and decision matrices. In the AHP stage, a pairwise comparison matrix of the criteria was formed, its consistency ratio (CR) was calculated, and the criteria weights were obtained. In the TOPSIS stage, a 10×5 decision matrix was constructed, normalized by vector normalization, weighted by the AHP weights, and evaluated against the positive ideal solution (PIS) and negative ideal solution (NIS). The relative closeness coefficient was then used to rank the controls.

## 3. RESULTS AND DISCUSSION

The AHP consistency ratio was 0.037, which is below 0.1 and therefore acceptable. The criteria weights were: confidentiality = 0.369, compliance = 0.291, integrity = 0.190, reliability = 0.107, and availability = 0.043. Confidentiality was thus the most important criterion, followed by compliance. The TOPSIS results are presented in Table 1. The control "protect against malicious software" achieved the highest rank with a score of 0.763, followed by "manage network and connectivity security" with 0.746 and "establish and maintain an information security management system (ISMS)" with 0.698. The lowest-ranked control was "manage sensitive documents and output devices" with 0.280.

**Table 1**

*Ranking of COBIT 2019 security controls*

| Rank | Control | Score |
|---|---|---|
| **1** | Protect against malicious software | 0.763 |
| **2** | Manage network and connectivity security | 0.746 |
| **3** | Establish and maintain an ISMS | 0.698 |
| **4** | Manage user identity and logical access | 0.528 |
| **5** | Manage endpoint security | 0.518 |
| **6** | Define and manage an information security and privacy risk treatment plan | 0.494 |
| **7** | Manage vulnerabilities and monitor the infrastructure for security-related events | 0.414 |
| **8** | Manage physical access to I&T assets | 0.343 |
| **9** | Monitor and review the ISMS | 0.308 |
| **10** | Manage sensitive documents and output devices | 0.280 |

These findings show that controls directly aimed at preventing malware and protecting network connectivity are perceived as the

most critical. However, the ranking does not imply that lower-ranked controls should be ignored. Many controls are interdependent; for example, network security and endpoint security require integration, and establishing an ISMS should be accompanied by monitoring and reviewing it. The results therefore support prioritized implementation rather than selective abandonment of controls. The findings are consistent with the view that MCDM methods can structure complex IT governance decisions and incorporate multiple information criteria into security prioritization.

## 4. CONCLUSION AND SUGGESTIONS

This paper presented a combined AHP–TOPSIS model for ranking the security controls of COBIT 2019. The model produced a clear priority list, with "protect against malicious software" ranked first and "manage sensitive documents and output devices" ranked last. The results can help security managers, IT managers, auditors, and board members allocate resources more effectively, improve risk management, reduce time and costs, and enhance IT governance. The study also demonstrates that MCDM methods are useful for prioritizing COBIT security controls. Future work should examine the cost-effectiveness of implementing the ranked controls, rank processes in other COBIT domains, and apply other MCDM methods such as ANP, ELECTRE, PROMETHEE, or fuzzy and group decision-making approaches.

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# حاکمیت فناوری از مسیر مدل رتبه‌بندی نوین برای کنترل‌های امنیت فناوری اطلاعات COBIT[1]

**سعید روحانی[2]* و محمد نیکبخت[3]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۲۹ - ۶۰

تاریخ دریافت: ۱۴۰۵/۰۵/۲۷
تاریخ بازنگری: ۱۴۰۵/۰۷/۱۰
تاریخ پذیرش: ۱۴۰۵/۰۸/۰۸

## چکیده

*با وابستگی بیشتر سازمان‌ها به فناوری اطلاعات (IT)، خطر تهدیدهای امنیتی به‌طور قابل‌توجهی افزایش یافته است. بنابراین سازمان‌ها باید حفاظت از امنیت فناوری اطلاعاتو پیاده‌سازی کنترل‌های امنیتی مناسب را در اولویت قرار دهند. COBIT 2019چارچوبی جامع برای حاکمیت فناوری اطلاعاتاست که کنترل‌های امنیتی متعددی برای حفظ امنیت فناوری اطلاعاتارائه می‌دهد. این چارچوب امنیت فناوری اطلاعاترا از طریق دو فرایند :APO13» مدیریت امنیت» و :DSS05»مدیریت خدمات امنیتی» بررسی می‌کند و در مجموع ۱۰ کنترل امنیتی برای این منظور تعریف شده است. هدف این مقاله استفاده از رویکرد تصمیم‌گیری چندمعیاره (MCDM) برای تعیین اهمیت کنترل‌های امنیتی در چارچوب COBIT 2019 است.برای دستیابی به این هدف، دو روش MCDM یعنی AHP و TOPSIS برای مقایسه و رتبه‌بندی کنترل‌های امنیتی چارچوب COBIT 2019 بر اساس پنج معیار اطلاعاتی COBIT استفاده شد. ابتدا وزن معیارها با روش AHP محاسبه و سپس در روش TOPSIS برای رتبه‌بندی کنترل‌های امنیتی بر اساس امتیازهای آن‌ها استفاده شد. بر اساس نتایج، کنترل «حفاظت در برابر نرم‌افزارهای مخرب» با امتیاز ۰/۷۶۳ بالاترین رتبه را کسب کرد، در حالی که کنترل «مدیریت اسناد حساس و دستگاه‌های خروجی» با امتیاز ۰/۲۸۰ پایین‌ترین رتبه را به دست آورد. نتایج این مطالعه می‌تواند به‌عنوان منبعی ارزشمند برای تیم‌های امنیتی مختلف جهت بهبود مؤثرتر و دقیق‌تر مدیریت امنیت فناوری اطلاعاتسازمان‌ها استفاده شود. این مدل منبعی ارزشمند برای تیم‌های امنیتی مختلف است و به آن‌ها امکان می‌دهد کنترل‌های مؤثرتری برای جلوگیری از تهدیدهای امنیتی پیاده‌سازی کنند. این امر به‌نوبه خود می‌تواند به کاهش زمان و هزینه، بهبود عملکرد سازمانی و افزایش کارایی منجر شود.*

**واژه‌های کلیدی:** *حاکمیت فناوری، کنترل‌های امنیتی، COBIT 2019، MCDM، AHP، TOPSIS، رتبه‌بندی.*
**طبقه‌بندی موضوعی:** *M15, C44, L86.*

---

[1] https://doi.org/10.22034/JISTA.2026.608452.1113
[2] دانشیار، گروه مدیریت، دانشگاه تهران، تهران ، ایران. (نویسنده مسئول). (srouhani@ut.ac.ir)
[3] دانشجوی دکتری، بانک سامان، تهران، ایران. (mohammadnikbakht@ut.ac.ir)

**مقدمه**

در جهان امروز که رقابت شدیدی وجود دارد، فناوری اطلاعات به بخشی جدایی‌ناپذیر از سازمان‌ها تبدیل شده است. گسترش روزافزون کاربردهای فناوری اطلاعات موجب تأکید بیشتر بر استفاده از آن شده است، تا جایی که بسیاری از سازمان‌ها اکنون به‌طور گسترده از آن برای تسهیل عملیات داخلی خود استفاده می‌کنند (شو و لو، ۲۰۲۲؛ طاهر دوست، ۲۰۲۳). فناوری‌هایی مانند اینترنت، اینترنت اشیا(IoT) ، شبکه‌های محلی(LAN) ، رایانش ابری، ایمیل و پایگاه‌های داده نمونه‌های بارز این نوع فناوری‌ها هستند.

پژوهش‌ها نشان می‌دهند سازمان‌هایی که در فناوری اطلاعات سرمایه‌گذاری می‌کنند و نوآوری را می‌پذیرند، می‌توانند سهم بازار، صورت‌های مالی و موقعیت رقابتی خود را به‌طور قابل‌توجهی بهبود دهند (طاهر دوست، ۲۰۲۳؛ صدرالدین و چن، ۲۰۲۳؛ وانگ و همکاران، ۲۰۲۲). یکی از جنبه‌های حیاتی این سرمایه‌گذاری، پیاده‌سازی حاکمیت فناوری اطلاعات است که شامل مدیریت همه منابع فناوری اطلاعات در راستای اولویت‌ها و اهداف سازمان می‌شود (جوشی و همکاران، ۲۰۲۲). پیاده‌سازی این حاکمیت بر عهده هیئت‌مدیره و مدیران ارشد سازمان است و نتیجه آن هم‌راستایی فناوری اطلاعات با اهداف کسب‌وکار، سرمایه‌گذاری بهینه، مدیریت کارآمد ریسک، توجه به نیازهای ذی‌نفعان و خلق ارزش است (د هاس و همکاران، ۲۰۱۹).

امنیت یکی از جنبه‌های اساسی حاکمیت فناوری اطلاعات است که در این مقاله بر آن تمرکز می‌کنیم. با رشد فناوری اطلاعات، تهدیدهای امنیتی نیز افزایش می‌یابند و سازمان‌ها باید مانند سایر دارایی‌های خود از آن محافظت کنند (گهلانی و همکاران، ۲۰۲۲؛ فبریانا و همکاران، ۲۰۲۲). نمونه‌ای از این تهدیدها حملات سایبری است که با هدف سرقت اطلاعات حساس مانند داده‌های مشتریان، جزئیات پرداخت، مالکیت فکری و اسرار تجاری، یا آسیب به اعتبار سازمان‌ها انجام می‌شود (سعید و اسعد، ۲۰۲۲). پیچیدگی‌ها و آسیب‌پذیری‌های فزاینده این حملات، اهمیت ایجاد و تقویت کنترل‌های امنیتی در فناوری اطلاعات را نشان می‌دهد. کنترل‌های امنیتی، راهبردها، روش‌ها و ابزارهای مورد استفاده برای حفاظت از محرمانگی، دسترس‌پذیری و یکپارچگی سیستم‌های فناوری اطلاعات را توصیف می‌کنند (کوری و نایک، ۲۰۲۳). سیستم‌های فناوری اطلاعات شامل سخت‌افزار و نرم‌افزار، برنامه‌ها، نقاط پایانی،

ارتباطات، شبکه‌ها، مراکز داده و پایگاه‌های داده است (راینر و پرینس، ۲۰۲۱؛ ماخشود، ۲۰۲۱). کنترل‌های امنیت فناوری اطلاعات ریسک‌های مهم را پیش‌بینی، شناسایی و کاهش می‌دهند و هزینه‌های کلی امنیت را کم می‌کنند (راینر و پرینس، ۲۰۲۱).

برای دستیابی به امنیت در حاکمیت فناوری اطلاعات، چارچوب‌های مختلفی مانند ISO 27001 و COBIT توسعه یافته‌اند که مجموعه‌ای جامع از کنترل‌های امنیتی ضروری را به سازمان‌ها ارائه می‌دهند. برای مثال، ) ISO 27001 یا (ISO/IEC 27001 استانداردی بین‌المللی است که الزامات ایجاد، پیاده‌سازی، نگهداشت و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات (ISMS) را مشخص می‌کند. این استاندارد رویکردی نظام‌مند برای مدیریت اطلاعات حساس شرکت ارائه می‌دهد و محرمانگی، یکپارچگی و دسترس‌پذیری آن را تضمین می‌کند. این استاندارد بر مدیریت ریسک تأکید دارد و از سازمان‌ها می‌خواهد ریسک‌های امنیت اطلاعات را متناسب با نیازهای خاص خود ارزیابی و درمان کنند (مالاتجی، ۲۰۲۳).

چارچوبCOBIT ، در حالی که چارچوبی جامع برای حاکمیت فناوری اطلاعات است، در چندین حوزه خود به‌طور مؤثر به امنیت سازمانی می‌پردازد. جدیدترین نسخه آن COBIT 2019است که شامل ۴۰ فرایند سازمان‌یافته در پنج حوزه و پوشش اهداف حاکمیت و مدیریت است (ایساکا، ۲۰۱۸).

در این پژوهش، چارچوب COBIT 2019 را در زمینه امنیت فناوری اطلاعات بررسی می‌کنیم. در حالی که سایر چارچوب‌ها مانند ISO 27001 نیز اهمیت خاص خود را دارند، COBIT 2019ویژگی‌های منحصربه‌فردی ارائه می‌دهد که آن را در جای خود مهم می‌کند. برخی دلایل اینکه COBIT 2019 ممکن است در زمینه‌های خاص مهم‌تر یا مناسب‌تر تلقی شود عبارت‌اند از (استوپرت، ۲۰۱۹؛ ایساکا، ۲۰۰۷؛ ایساکا، ۲۰۱۸):

- رویکرد جامع COBIT 2019 :جنبه‌های مختلف حاکمیت و مدیریت فناوری اطلاعات، از جمله راهبرد، مدیریت ریسک، بهینه‌سازی منابع و اندازه‌گیری عملکرد را پوشش می‌دهد. این رویکرد جامع به سازمان‌ها کمک می‌کند IT را با اهداف کسب‌وکار هم‌راستا کنند و حاکمیت مؤثر فرایندهای فناوری اطلاعات را تضمین کنند.

- تأکید بر حاکمیت IT: COBIT 2019 بر حاکمیت فناوری اطلاعات تأکید زیادی دارد که شامل رهبری، ساختارها و فرایندهایی برای تصمیم‌گیری آگاهانه، اولویت‌بندی منابع و مدیریت ریسک است.
- یکپارچگی با سایر استانداردها COBIT 2019 :به‌گونه‌ای طراحی شده است که با استانداردها و چارچوب‌های شناخته‌شده مانند ISO 27001 ، ITILو COSO یکپارچه و هم‌راستا شود. این یکپارچگی به سازمان‌ها امکان می‌دهد از نقاط قوت چندین چارچوب استفاده کنند و یک زیست‌بوم منسجم حاکمیت و مدیریت ایجاد کنند.
- مدل بلوغ COBIT 2019 :مدل بلوغی را دربر می‌گیرد که به سازمان‌ها کمک می‌کند فرایندهای فناوری اطلاعات خود را در طول زمان ارزیابی و بهبود دهند. این مدل نقشه راهی ارائه می‌دهد تا سازمان‌ها از شیوه‌های موردی و واکنشی به شیوه‌های پیش‌نگر و بهینه‌شده حرکت کنند. بهبود مستمر برای تقویت توانمندی‌های حاکمیت و مدیریت فناوری اطلاعات حیاتی است.
- شناخت و پذیرش صنعتی COBIT :در سطح جهانی شناخت و پذیرش قابل‌توجهی به دست آورده است، به‌ویژه در صنایعی مانند بانکداری، مالی، بهداشت و دولت. مطالعات متعددی نقش COBIT و کاربردهای آن را در مدیریت موفق فناوری اطلاعات در سازمان‌های بزرگ نشان داده‌اند.

در سال ۲۰۲۳، تولوس و تاناماه اثربخشی و کارایی حسابرسی با COBIT 2019 را در بهبود فرایندهای کسب‌وکار، مدیریت ریسک و امنیت در مؤسسات آموزشی نشان دادند (تولوس و تاناماه، ۲۰۲۳). در مطالعه دیگری که در سال ۲۰۲۳ توسط توینِر و اسفنریانتو انجام شد، آن‌ها از فرایند :DSS05» مدیریت خدمات امنیتی» چارچوب COBIT5 برای حفاظت از دارایی‌های اطلاعاتی یک شرکت استفاده کردند (توینِر و اسفنریانتو، ۲۰۲۳). همچنین در سال ۲۰۲۳، اوتاماجایا و همکاران اثربخشی استفاده از فرایند :APO12» مدیریت ریسک» چارچوب COBIT 2019 را در مدیریت ریسک سیستم‌های اطلاعاتی هتل نشان دادند (اوتاماجایا و همکاران، ۲۰۲۳).

این دلایل موجب شد چارچوب COBIT 2019 را برای ارزیابی در این مطالعه انتخاب کنیم. چارچوب COBIT به دلیل دامنه و فرایندهای گسترده خود، برای پیاده‌سازی به زمان و منابع قابل‌توجهی نیاز دارد. با این حال، به سازمان‌ها انعطاف می‌دهد فقط فرایندهایی را انتخابی پیاده‌سازی کنند که با اهداف و نیازهای خاص آن‌ها هم‌راستاست، نه اینکه پیاده‌سازی همه فرایندها الزامی باشد. این انعطاف مزیتی است، اما می‌تواند به سردرگمی نیز منجر شود، زیرا سازمان‌ها ممکن است درباره اینکه کدام فرایندها را انتخاب کنند و با چه ترتیبی پیاده‌سازی کنند، با توجه به نبود یک نظام اولویت‌بندی مشخص، مطمئن نباشند. در چنین شرایطی، اولویت‌بندی عناصر کلیدی در چارچوب COBIT برای مدیریت مؤثر فناوری اطلاعات ضروری می‌شود. سازمان‌ها باید با تحلیل و انتخاب فرایندهایی آغاز کنند که بیشترین ارزش افزوده را ارائه می‌دهند. این رویکرد نه‌تنها بهره‌وری سازمانی را افزایش می‌دهد، بلکه با تمرکز بر فرایندهای مرتبط و حیاتی، اثربخشی پیاده‌سازی را بهبود می‌بخشد. نتیجه آن بهبود کیفیت حاکمیت فناوری اطلاعات، خلق ارزش افزوده و کاهش ریسک در سازمان است. در مقابل، چارچوب‌هایی مانند ISO 27001 این انعطاف انتخابی را ارائه نمی‌دهند ISO 27001 . یک الزام مقرراتی تلقی می‌شود که سازمان‌ها باید آن را به‌طور کامل، از ابتدا تا انتها و بدون نیاز به اولویت‌بندی میان اجزای آن، پیاده‌سازی کنند. اما COBIT به سازمان‌ها امکان می‌دهد هر حوزه فناوری اطلاعات را به‌صورت هدفمند و اولویت‌محور و بر اساس نیازهای خاص مدیریت کنند. در نتیجه، ISO 27001نیازمند اولویت‌بندی اعمال‌شده در این مطالعه نیست.

یکی از رویکردهای اولویت‌بندی فرایندها در چارچوب COBIT استفاده از MCDM است. روش‌های MCDM مدل‌های ریاضی هستند که با در نظر گرفتن چندین معیار امکان رتبه‌بندی را فراهم می‌کنند و در حل مسائل پیچیده سازمانی بسیار مفیدند (امون و اوگه‌نریووهو، ۲۰۲۰؛ زاوادسکاس و همکاران، ۲۰۱۴). برای مثال، در سال ۲۰۱۸، اهریز و همکاران از ترکیب روش‌های AHP و TOPSIS با معیارهای توانمندساز COBIT5 برای اولویت‌بندی و انتخاب سبد پروژه‌های IT یک دانشگاه استفاده کردند (اهریز و همکاران، ۲۰۱۸). همچنین در سال ۲۰۱۸، آلمیدا و همکاران از روش AHP برای کمک به سازمان‌ها در تعیین اولویت‌های فرایند COBIT5 استفاده کردند (آلمیدا و همکاران، ۲۰۱۸).

بنابراین هدف این مقاله ارائه یک مدل رتبه‌بندی برای کنترل‌های امنیت فناوری اطلاعات از طریق COBIT و MCDM است. امنیت در COBIT 2019 در دو فرایند مهم از حوزه‌های «هم‌راستاسازی، برنامه‌ریزی و سازمان‌دهی «(APO) و «تحویل، خدمات و پشتیبانی «(DSS)، یعنی :APO13» مدیریت امنیت» و :DSS05» مدیریت خدمات امنیتی» بررسی شده و در مجموع ۱۰ کنترل امنیتی برای این فرایندها تعریف شده است (ایساکا، ۲۰۱۸). ما این ۱۰ کنترل امنیتی را با ترکیب دو روش MCDM مقایسه و رتبه‌بندی می‌کنیم. پرسش پژوهش عبارت است از:

- *روش‌های MCDM چگونه می‌توانند در اولویت‌بندی کنترل‌های امنیتی چارچوب COBIT 2019 مفید باشند؟*

## مرور پیشینه

### حاکمیت فناوری اطلاعات

حاکمیت فناوری اطلاعات سازمان‌ها را توانمند می‌سازد تا سرمایه‌گذاری‌های فناوری اطلاعات خود را به‌طور مؤثر نظارت و ارزش آن را بیشینه کنند و از هم‌راستایی با اهداف کلی کسب‌وکار اطمینان یابند (جوشی و همکاران، ۲۰۲۲؛ هارگوم و همکاران، ۲۰۲۲). این چارچوب حاکمیت شامل استانداردها، فرایندها، سیاست‌ها و رویه‌هایی است که به کاهش ریسک‌های فناوری اطلاعات و در همان حال تقویت امنیت، کارایی و کیفیت خدمات کمک می‌کند (د هاس و همکاران، ۲۰۱۹).

اگرچه چارچوب‌های رسمی حاکمیت فناوری اطلاعات بعدها ایجاد شدند، مفاهیم بنیادی آن به دهه ۱۹۷۰ بازمی‌گردد، زمانی که سازمان‌ها نیاز به نظارت ساختاریافته بر منابع فناوری اطلاعات خود را تشخیص دادند. مطالعات اولیه بر اهمیت راهبردی مدیریت فناوری اطلاعات و نقش رهبری اجرایی در نظارت بر سیستم‌های فناوری اطلاعات برای افزایش کارایی و مزیت رقابتی تأکید اشتند.

**اهداف کنترل برای اطلاعات و فناوری‌های مرتبط(COBIT)**

COBIT چارچوبی شناخته‌شده برای حاکمیت و مدیریتفناوری اطلاعات است که توسط انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی (ISACA) توسعه یافته است COBIT . مجموعه‌ای جامع از راهنماها و بهترین شیوه‌ها را در سه سطح مختلف ارائه می‌دهد: حوزه‌ها، فرایندها و کنترل‌ها، که به سازمان‌ها کمک می‌کندفناوری اطلاعات خود را به‌طور مؤثر مدیریت و کنترل کنند (نوگروهو، ۲۰۱۹؛ ایساکا، ۲۰۰۷). پایین‌ترین سطح شامل کنترل‌هاست و در سطح بعدی، فرایندها مجموعه‌ای از کنترل‌ها را تعریف می‌کنند و در بالاترین سطح، مجموعه‌ای از فرایندها حوزه‌ها را تشکیل می‌دهند (ایساکا، ۲۰۰۷).

اولین نسخه COBIT در سال ۱۹۹۶ معرفی شد و از آن زمان نسخه‌های مختلفی شامل نسخه‌های ۲، ۳، ۴، ۴٫۱ و ۵ منتشر شده‌اند. هر نسخه در جنبه‌های مختلفی مانند فرایندها، کنترل‌ها و تکنیک‌های مدیریتی بهبود یافته است (فصیح‌الدین و همکاران، ۲۰۲۲). جدیدترین نسخه فعلی COBIT 2019 است که اهداف حاکمیت و مدیریت را در ۴۰ فرایند سازمان‌یافته در پنج حوزه توصیف می‌کند (ایساکا، ۲۰۱۸) COBIT 2019 .به سازمان‌ها امکان می‌دهد یک نظام حاکمیت متناسب با نیازهای خود را طراحی، اجرا و بهبود دهند (استوپرت، ۲۰۱۹).

پنج حوزه اهداف حاکمیت و مدیریت در COBIT 2019 عبارت‌اند از (ایساکا، ۲۰۱۸):

- اهداف حاکمیت - ارزیابی، هدایت و پایش :(EDM) در این حوزه، نهاد حاکم گزینه‌های راهبردی را ارزیابی می‌کند، مدیریت ارشد را در گزینه‌های راهبردی انتخاب‌شده هدایت می‌کند و دستیابی به راهبرد را پایش می‌کند.
- اهداف مدیریت - هم‌راستاسازی، برنامه‌ریزی و سازمان‌دهی :(APO) به سازمان کلی، راهبرد و فعالیت‌های پشتیبان I&T می‌پردازد.
- ساخت، کسب و پیاده‌سازی :(BAI) به تعریف، کسب و پیاده‌سازی راه‌حل‌های I&Tو یکپارچه‌سازی آن‌ها در فرایندهای کسب‌وکار می‌پردازد.
- تحویل، خدمات و پشتیبانی :(DSS) به تحویل عملیاتی و پشتیبانی خدمات I&T ، از جمله امنیت، می‌پردازد.
- نظارت، ارزیابی و سنجش :(MEA) به پایش عملکرد و انطباق I&T با اهداف عملکرد داخلی، اهداف کنترل داخلی و الزامات خارجی می‌پردازد.

### تصمیم‌گیری چندمعیاره(MCDM)

ابزارهای MCDM عموماً برای رسیدن به یک تصمیم بهینه در مواجهه با گزینه‌های متعدد دارای معیارهای تصمیم‌گیری چندگانه، متضاد و غیرقابل‌مقایسه به کار می‌روند (امون و اوگه‌نریووهو، ۲۰۲۰). این تکنیک ابزاری به‌طور گسترده شناخته‌شده برای حل مسائل پیچیده دنیای واقعی است (روحانی و رواسان، ۲۰۱۴)، زیرا می‌تواند گزینه‌های مختلف را بر اساس معیارهای متعدد به‌طور مؤثر ارزیابی و بهترین گزینه را انتخاب کند (زاوادسکاس و همکاران، ۲۰۱۴). روش‌های MCDM مدل‌های ریاضی هستند که با تعیین اهمیت معیارها و گزینه‌ها، تصمیم‌های مؤثر را به‌صورت ساختاریافته اتخاذ می‌کنند (طاهر دوست و مدنچیان، ۲۰۲۳). یک مسئله MCDM از عناصر اصلی زیر تشکیل شده است:

- هدف: نتیجه مشخص و مورد انتظار از یک تصمیم است.
- معیارها: برای ارزیابی و مقایسه گزینه‌ها استفاده می‌شوند. معیارها باید مستقل از یکدیگر، مرتبط با گزینه‌ها و تصمیم‌گیری، دارای مقیاس یکسان و قابل اندازه‌گیری باشند.
- گزینه: گزینه‌ها یا انتخاب‌های مختلفی هستند که در اختیار تصمیم‌گیرنده قرار دارند تا آن‌ها را ارزیابی، مقایسه و انتخاب کند. گزینه‌ها باید واقع‌گرایانه، در دسترس و قابل مقایسه باشند.
- تصمیم‌گیرنده: یک خبره یا گروهی از خبرگان که گزینه‌ها و معیارهای مسئله را نسبت به یکدیگر با استفاده از مقیاس نسبی ارزیابی می‌کنند. به دلیل تأثیر قابل‌توجه نظر تصمیم‌گیرنده بر نتایج، انتخاب خبره بسیار مهم است.

### فرایند تحلیل سلسله‌مراتبی(AHP)

AHPیکی از روش‌های MCDM است که توسط توماس ال. ساعتی در سال ۱۹۸۰ توسعه یافت (ساعتی، ۱۹۸۰). به آن مدل سلسله‌مراتبی می‌گویند زیرا ساختاری درختی دارد که هر سطح به سطح بالای خود وابسته است .AHP یک مسئله بزرگ تصمیم‌گیری را به بخش‌های کوچک‌تری تقسیم می‌کند که از طریق مقایسه‌های زوجی به بخش‌های بزرگ‌تر متصل می‌شوند (ساعتی، ۱۹۸۸).

**تکنیک ترجیح بر اساس شباهت به راه‌حل ایده‌آل(TOPSIS)**

TOPSISیکی دیگر از روش‌های MCDM است که توسط هوانگ و یون در سال ۱۹۸۱ توسعه یافت (هوانگ و یون، ۱۹۸۱). این روش گزینه‌ها را با استفاده از دو مفهوم رتبه‌بندی می‌کند: راه‌حل ایده‌آل مثبت (PIS) و راه‌حل ایده‌آل منفی PIS .(NIS) نشان‌دهنده بالاترین مقادیر و NIS نشان‌دهنده پایین‌ترین سود و هزینه بالا برای معیارهاست و گزینه انتخاب‌شده باید کوتاه‌ترین فاصله را به PIS و بیشترین فاصله را از NIS داشته باشد (بهزادیان و همکاران، ۲۰۱۲).

## روش‌شناسی پژوهش

برای حل مؤثر یک مسئلهMCDM ، تعریف دقیق هدف، معیارها، زیرمعیارها، گزینه‌ها و تصمیم‌گیرنده مسئله ضروری است. این عناصر باید به‌خوبی شناخته و به‌درستی مدل‌سازی شوند.

هدف: رتبه‌بندی کنترل‌های امنیتی چارچوب.COBIT 2019

معیارها COBIT :چندین معیار اطلاعاتی برای تأمین اهداف کسب‌وکار تعریف کرده است. این معیارها بر اساس الزامات کیفیت، امانت‌داری و امنیت فرایندها تعریف می‌شوند (ایساکا، ۲۰۰۷). معیارهای اطلاعاتی COBIT برای گنجاندن در روش‌های MCDM بسیار مناسب‌اند، زیرا هر معیار جنبه‌ای حیاتی از کیفیت فرایند را نشان می‌دهد و به تضمین صحت تصمیم‌های حاصل کمک می‌کند. بر اساس این چارچوب، تضمین امنیت سیستم شامل پنج معیار اطلاعاتی است: محرمانگی، یکپارچگی، دسترس‌پذیری، انطباق و قابلیت اعتماد (ایساکا، ۲۰۰۷). در مدل ما، این معیارهای اطلاعاتی را به‌عنوان معیارهای اصلی در نظر می‌گیریم و هیچ زیرمعیار مرتبطی ندارند. بنابراین، در مدل ما زیرمعیاری گنجانده نشده است. جدول ۱ این پنج معیار را همراه با توضیحاتشان نشان می‌دهد.

**جدول ۱**

معیارها با توضیحات آن‌ها (ایساکا، ۲۰۰۷)

| معیار | نام | توضیح |
|---|---|---|
| **C1** | محرمانگی | به حفاظت از اطلاعات حساس در برابر افشای غیرمجاز مربوط می‌شود. |
| **C2** | یکپارچگی | به دقت و کامل بودن اطلاعات و همچنین اعتبار آن مطابق با ارزش‌ها و انتظارات کسب‌وکار مربوط می‌شود. |
| **C3** | دسترس‌پذیری | به در دسترس بودن اطلاعات در زمان نیاز فرایند کسب‌وکار، اکنون و در آینده، مربوط می‌شود. همچنین به حفاظت از منابع لازم و قابلیت‌های مرتبط مربوط است. |
| **C4** | انطباق | به انطباق با قوانین، مقررات و ترتیبات قراردادی که فرایند کسب‌وکار تابع آن‌هاست، یعنی معیارهای کسب‌وکار تحمیل‌شده از بیرون و همچنین سیاست‌های داخلی، مربوط می‌شود. |
| **C5** | قابلیت اعتماد | به ارائه اطلاعات مناسب برای مدیریت جهت اداره واحد و ایفای مسئولیت‌های امانت‌داری و حاکمیتی آن مربوط می‌شود. |

گزینه‌ها: گزینه‌ها کنترل‌های COBIT برای امنیتفناوری اطلاعات هستند که در دو فرایند از حوزه‌های «هم‌راستاسازی، برنامه‌ریزی و سازمان‌دهی «(APO) و «تحویل، خدمات و پشتیبانی«(DSS) ، یعنی :APO13» مدیریت امنیت» و :DSS05» مدیریت خدمات امنیتی»، تعریف شده‌اند APO13 .یک سیستم مدیریت امنیت اطلاعات را تعریف، اجرا و پایش می کند و DSS05 از اطلاعات سازمان حفاظت می کند تا سطح ریسک امنیت اطلاعات قابل‌قبول برای سازمان مطابق با سیاست امنیتی حفظ شود، نقش‌ها و امتیازهای دسترسی امنیت اطلاعات را ایجاد و نگه‌داری می کند و پایش امنیتی را انجام می‌دهد (ایساکا، ۲۰۱۸). برای دستیابی به اهداف این دو فرایند، COBIT 2019در مجموع ۱۰ کنترل تعریف کرده است که ما آن‌ها را به‌عنوان گزینه در نظر گرفته و با یکدیگر مقایسه کرده‌ایم. این ۱۰ کنترل در جدول ۲ فهرست شده‌اند.

**جدول ۲**

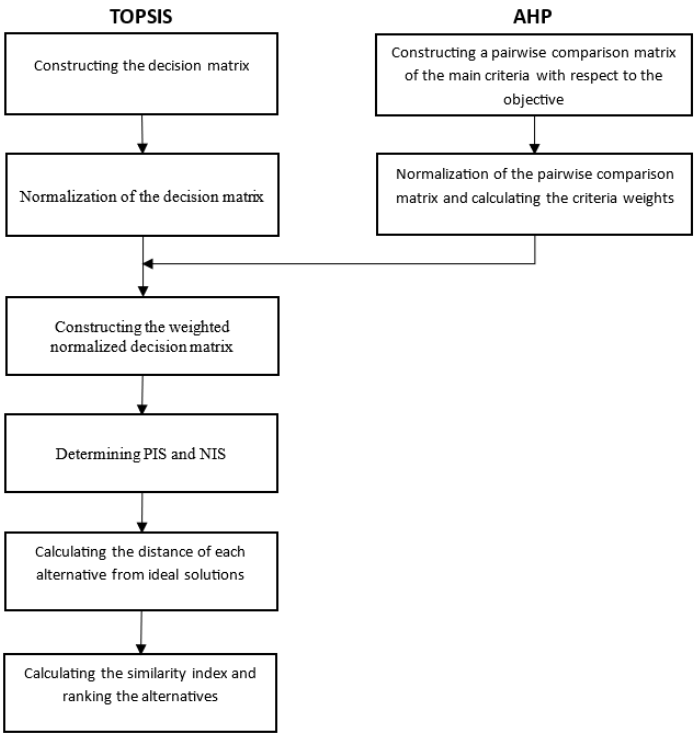
کنترل‌های امنیتی COBIT 2019 به‌عنوان گزینه‌ها

| نماد | نام کنترل |
|---|---|
| **A1** | استقرار و نگهداشت سیستم مدیریت امنیت اطلاعات(ISMS) |
| **A2** | تعریف و مدیریت برنامه درمان ریسک امنیت اطلاعات و حریم خصوصی |
| **A3** | پایش و بازبینی سیستم مدیریت امنیت اطلاعات(ISMS) |
| **A4** | حفاظت در برابر نرم‌افزارهای مخرب |
| **A5** | مدیریت امنیت شبکه و اتصال‌پذیری |
| **A6** | مدیریت امنیت نقاط پایانی |
| **A7** | مدیریت هویت کاربر و دسترسی منطقی |
| **A8** | مدیریت دسترسی فیزیکی به دارایی‌های I&T |
| **A9** | مدیریت اسناد حساس و دستگاه‌های خروجی |
| **A10** | مدیریت آسیب‌پذیری‌ها و پایش زیرساخت برای رویدادهای مرتبط با امنیت |

تصمیم‌گیرنده: فردی است با ۱۱ سال تجربه در حاکمیت فناوری اطلاعات و COBIT .

## انتخاب روش

ما از ترکیب دو روش AHP و TOPSIS برای ارزیابی و رتبه‌بندی کنترل‌های امنیتی چارچوب COBIT 2019 استفاده می‌کنیم. روش شامل نخست استفاده از روش AHP برای محاسبه وزن معیارهاست که سپس در روش TOPSIS برای رتبه‌بندی گزینه‌ها استفاده می‌شود. شکل ۲ نمای کلی دو روش استفاده‌شده را ارائه می‌دهد.




**شکل ۱.** مراحل مدل حاکمیت فناوری از روش رتبه بندی کنترل ها

در این بخش، منطق خود را برای ترکیب این دو روش توضیح می‌دهیم. هر روش MCDMدر مراحل مختلف فرایند تصمیم‌گیری نقاط قوت و ضعف خاص خود را دارد و ترکیب آن‌ها هم کارایی و هم دقت را افزایش می‌دهد. وقتی تعداد گزینه‌های مسئله زیاد است (مانند این مطالعه)، روش TOPSIS در رتبه‌بندی در مقایسه با سایر روش‌های MCDM عملکرد خوبی دارد. این رویکرد فرایند مقایسه را با استفاده از ماتریس تصمیم‌گیری به‌طور قابل‌توجهی ساده می‌کند. تکمیل ماتریس تصمیم ساده است و مقیاس‌های مختلفی می‌تواند استفاده شود. علاوه بر این، برخلاف AHP ، TOPSISنیازی به محاسبه CR ندارد.

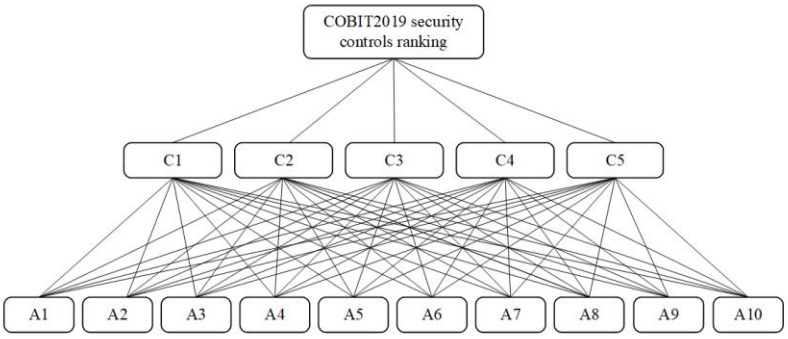
در مقابل، روش AHP به دلیل نیاز به ساخت ماتریس‌های مقایسه زوجی برای هر معیار و محاسبه مقدارCR ، فرایندی طولانی و پیچیده دارد. وزن‌دهی ماتریس‌ها توسط تصمیم‌گیرنده نیز یکی از چالش‌های این روش است.

با این حال، یکی از ضعف‌های TOPSIS این است که برای محاسبه وزن معیارها به روش‌های دیگر مانند AHP و آنتروپی وابسته است. در این مطالعه، از روش AHP برای محاسبه وزن معیارها استفاده کردیم، زیرا فرض می‌شود اگر گزینه‌ها در AHP به‌درستی رتبه‌بندی شوند، روش TOPSIS نیز می‌تواند با همان وزن‌های معیار رتبه‌بندی دقیقی ارائه دهد. جدول ۷ نقاط قوت و ضعف این دو روش را مقایسه می‌کند.

## نتایج و تحلیل داده‌ها

### محاسبه وزن‌ها باAHP

گام ۱ – ساخت نمودار سلسله‌مراتبی: شکل ۳ نمودار سلسله‌مراتبی مدل را نشان می‌دهد.




**شکل ۲.** ساختار سلسله مراتبی مدل

گام ۲ – ساخت ماتریس‌های مقایسه زوجی: برای محاسبه وزن معیارها، تنها به ماتریس مقایسه زوجی معیارها نسبت به هدف نیاز داریم که بر اساس نظر تصمیم‌گیرنده تکمیل شده است، مطابق جدول ۳.

**جدول ۳**

*مقایسه زوجی*

| | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| **C1** | 1 | 3 | 7 | 1 | 4 |
| **C2** | 0.333 | 1 | 5 | 0.5 | 3 |
| **C3** | 0.143 | 0.2 | 1 | 0.167 | 0.333 |
| **C4** | 1 | 2 | 6 | 1 | 2 |
| C5 | 0.25 | 0.333 | 3 | 0.5 | 1 |

گام ۳ - بررسی نسبت سازگاری: مقدار CR برابر ۰/۰۳۷ محاسبه شد. چون CR کمتر از ۰/۱ است، ماتریس مقایسه زوجی سازگار است. جزئیات محاسبه CR در پیوست ۱ آمده است.

گام ۴ - نرمال‌سازی ماتریس‌های مقایسه زوجی: برای نرمال‌سازی ماتریس مقایسه زوجی از روش جمع خطی (فرمول ۳) استفاده شده است. برای نمونه، فرمول ۱۲ مقدار \(r_{11}\) را محاسبه می‌کند. ماتریس مقایسه زوجی نرمال‌شده در جدول ۴ نشان داده شده است.

$$r_{11} = \frac{1}{1 + 0.333 + 0.143 + 1 + 0.25} = 0.367$$

گام ۵ - محاسبه وزن معیارها: وزن‌ها با محاسبه میانگین حسابی (فرمول ۴) هر سطر در ماتریس مقایسه زوجی نرمال‌شده تعیین می‌شوند. برای نمونه، فرمول ۱۳ وزن معیار ۱ را محاسبه می‌کند. جدول ۵ معیارها را به ترتیب اولویت وزنی آن‌ها نشان می‌دهد.

$$w_{C1} = \frac{0.367 + 0.459 + 0.318 + 0.316 + 0.387}{5} = 0.369$$

**جدول ٤**

*نرمال سازی شده*

| | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| **C1** | 0.367 | 0.459 | 0.318 | 0.316 | 0.387 |
| **C2** | 0.122 | 0.153 | 0.227 | 0.158 | 0.290 |
| **C3** | 0.052 | 0.031 | 0.045 | 0.053 | 0.032 |
| **C4** | 0.367 | 0.306 | 0.273 | 0.316 | 0.194 |
| **C5** | 0.092 | 0.051 | 0.136 | 0.158 | 0.097 |

**جدول ۵**

*وزن معیارها*

| NO | Criteria | Name | Weights |
|---|---|---|---|
| 1 | C1 | Confidentiality | 0.369 |
| 2 | C4 | Compliance | 0.291 |
| 3 | C2 | Integrity | 0.190 |
| 4 | C5 | Reliability | 0.107 |
| 5 | C3 | Availability | 0.043 |

## رتبه‌بندی گزینه‌ها باTOPSIS

گام ۱ – ساخت ماتریس تصمیم: ماتریس تصمیم بر اساس نظر تصمیم‌گیرنده تکمیل شده است، مطابق جدول ۶.

**جدول ٦**

*ماتریس تصمیم تکمیل‌شده*

| | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| **A1** | 6 | 7 | 3 | 8 | 4 |
| **A2** | 5 | 6 | 2 | 5 | 3 |
| **A3** | 3 | 4 | 6 | 4 | 3 |
| **A4** | 8 | 7 | 4 | 6 | 5 |
| **A5** | 9 | 4 | 3 | 7 | 3 |
| **A6** | 4 | 7 | 5 | 6 | 4 |
| **A7** | 7 | 1 | 2 | 5 | 7 |
| **A8** | 5 | 3 | 9 | 3 | 6 |
| **A9** | 6 | 2 | 4 | 1 | 2 |
| **A10** | 4 | 5 | 9 | 4 | 8 |

گام ۲ – نرمال‌سازی ماتریس تصمیم: برای نرمال‌سازی ماتریس تصمیم از نرمال‌سازی برداری استفاده شده است. برای نمونه، فرمول ۱۴ مقدار \(r_{11}\) را محاسبه می‌کند. ماتریس تصمیم نرمال‌شده در جدول ۷ نشان داده شده است.

$$r_{11} = \frac{6}{\sqrt{6^2 + 5^2 + 3^2 + 8^2 + 9^2 + 4^2 + 7^2 + 5^2 + 6^2 + 4^2}} = 0.318$$

**جدول ۷**

*ماتریس تصمیم نرمال‌شده*

| | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| A1 | 0.318 | 0.439 | 0.179 | 0.481 | 0.260 |
| **A2** | 0.265 | 0.376 | 0.119 | 0.300 | 0.195 |
| **A3** | 0.159 | 0.251 | 0.358 | 0.240 | 0.195 |
| **A4** | 0.423 | 0.439 | 0.239 | 0.361 | 0.325 |
| **A5** | 0.476 | 0.251 | 0.179 | 0.421 | 0.195 |
| **A6** | 0.212 | 0.439 | 0.298 | 0.361 | 0.260 |
| **A7** | 0.370 | 0.063 | 0.119 | 0.300 | 0.455 |
| **A8** | 0.265 | 0.188 | 0.537 | 0.180 | 0.390 |
| **A9** | 0.318 | 0.125 | 0.239 | 0.060 | 0.130 |
| **A10** | 0.212 | 0.314 | 0.537 | 0.240 | 0.520 |

گام ۳ – ساخت ماتریس تصمیم نرمال‌شده وزن‌دار: از وزن‌های معیارهای به‌دست‌آمده با AHP استفاده می‌کنیم و سپس ماتریس تصمیم نرمال‌شده وزن‌دار مطابق جدول ۸ ساخته می‌شود.

**جدول ۸**

*ماتریس تصمیم نرمال‌شده وزن‌دار*

| | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| **A1** | 0.117 | 0.083 | 0.008 | 0.140 | 0.028 |
| **A2** | 0.098 | 0.072 | 0.005 | 0.087 | 0.021 |
| **A3** | 0.059 | 0.048 | 0.015 | 0.070 | 0.021 |
| **A4** | 0.156 | 0.083 | 0.010 | 0.105 | 0.035 |
| **A5** | 0.176 | 0.048 | 0.008 | 0.122 | 0.021 |
| **A6** | 0.078 | 0.083 | 0.013 | 0.105 | 0.028 |
| **A7** | 0.137 | 0.012 | 0.005 | 0.087 | 0.049 |
| **A8** | 0.098 | 0.036 | 0.023 | 0.052 | 0.042 |
| **A9** | 0.117 | 0.024 | 0.010 | 0.017 | 0.014 |
| **A10** | 0.078 | 0.060 | 0.023 | 0.070 | 0.056 |

گام ۴ – تعیین PIS و NIS: همه معیارها ویژگی مثبت دارند؛ بنابراین بر اساس معادلات حداکثر مقدار و NIS حداقل مقدار هر معیار در ماتریس تصمیم نرمال‌شده وزن‌دار است که در جدول ۹ نشان داده شده است.

**جدول ۹**

*PIS و NIS*

| | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| $A^+$ | 0.176 | 0.083 | 0.023 | 0.140 | 0.056 |
| $A^-$ | 0.059 | 0.012 | 0.005 | 0.017 | 0.014 |

گام ۵ – محاسبه فاصله از راه‌حل‌های ایده‌آل: فاصله هر گزینه از PIS و NIS با استفاده از فرمول‌های ذیل محاسبه می‌شود که در جدول ۱۰۵ نشان داده شده است. برای نمونه، فرمول‌های زیر فاصله گزینه اول را محاسبه می‌کنند.

$$S_1^+ = \sqrt{(0.117-0.176)^2+(0.083-0.083)^2+(0.008-0.023)^2+(0.140-0.140)^2+(0.028-0.056)^2} = 0.067$$

$$S_1^- = \sqrt{(0.117-0.059)^2+(0.083-0.012)^2+(0.008-0.005)^2+(0.140-0.017)^2+(0.028-0.014)^2} = 0.154$$

**جدول ۱۰**

*فاصله هر گزینه از PIS و NIS*

| Alternatives | $S^+$ | $S^-$ |
|---|---|---|
| A1 | 0.067 | 0.154 |
| A2 | 0.103 | 0.100 |
| A3 | 0.145 | 0.065 |
| A4 | 0.047 | 0.151 |
| A5 | 0.055 | 0.161 |
| A6 | 0.108 | 0.116 |
| A7 | 0.099 | 0.110 |
| A8 | 0.127 | 0.066 |
| A9 | 0.154 | 0.060 |
| A10 | 0.122 | 0.086 |

گام ۶ – محاسبه شاخص شباهت: فرمول ذیل شاخص شباهت گزینه اول را محاسبه می‌کند. جدول ۱۱ مقادیر شاخص شباهت را برای همه گزینه‌ها نشان می‌دهد.

$$C_1^* = \frac{S_1^-}{(S_1^+ + S_1^-)} = \frac{0.154}{(0.067 + 0.154)} = 0.698$$

**جدول ۱۱**

*مقادیر شاخص شباهت برای همه گزینه‌ها*

| Alternatives | $C^*$ |
|---|---|
| A1 | 0.698 |
| A2 | 0.494 |
| A3 | 0.308 |
| A4 | 0.763 |
| A5 | 0.746 |
| A6 | 0.518 |
| A7 | 0.528 |
| A8 | 0.343 |
| A9 | 0.280 |
| A10 | 0.414 |

گام ۷ – رتبه‌بندی گزینه‌ها: رتبه‌بندی بر اساس شاخص شباهت انجام می‌شود. جدول ۱۲ نتایج رتبه‌بندی گزینه‌ها (یا کنترل‌های امنیتی) را همراه با نام و امتیاز آن‌ها نشان می‌دهد.

بر اساس جدول ۱۲، کنترل «حفاظت در برابر نرم‌افزارهای مخرب» با امتیاز ۰/۷۶۳ بالاترین رتبه را کسب کرد، در حالی که کنترل «مدیریت اسناد حساس و دستگاه‌های خروجی» با امتیاز ۰/۲۸۰ پایین‌ترین رتبه را دریافت کرد. با این حال، توجه به این نکته ضروری است که این کنترل‌ها کاملاً مستقل از یکدیگر پیاده‌سازی نمی‌شوند؛ بسیاری از آن‌ها به هم مرتبط‌اند و باید به‌صورت نظام‌مند اعمال شوند. برای نمونه، کنترل‌های «مدیریت امنیت شبکه و اتصال‌پذیری» و «مدیریت امنیت نقاط پایانی» برای تضمین حفاظت مؤثر از محیط‌هایفناوری اطلاعات به یکپارچگی و همکاری متقابل نیاز دارند. همچنین کنترل‌های «استقرار و نگهداشت ISMS» و «پایش و بازبینی ISMS» باید همراه با یکدیگر انجام شوند تا امنیت پایدار تضمین شود. بنابراین،

این رتبه‌بندی به این معنا نیست که پیاده‌سازی کنترل‌های با امتیاز پایین‌تر باید نادیده گرفته شود؛ بلکه هدف آن تسهیل استقرار مؤثرتر کنترل‌های COBIT برای ارتقای سطح امنیت سازمان است.

**جدول ۱۲**

*نتایج رتبه‌بندی گزینه‌ها*

| Rank | Alternatives | Name | Score |
|---|---|---|---|
| 1 | A4 | Protect against malicious software | 0.763 |
| 2 | A5 | Manage network and connectivity security | 0.746 |
| 3 | A1 | Establish and maintain an information security management system (ISMS) | 0.698 |
| 4 | A7 | Manage user identity and logical access | 0.528 |
| 5 | A6 | Manage endpoint security | 0.518 |
| 6 | A2 | Define and manage an information security and privacy risk treatment plan | 0.494 |
| 7 | A10 | Manage vulnerabilities and monitor the infrastructure for security-related events | 0.414 |
| 8 | A8 | Manage physical access to I&T assets | 0.343 |
| 9 | A3 | Monitor and review the information security management system (ISMS) | 0.308 |
| 10 | A9 | Manage sensitive documents and output devices | 0.280 |

## مباحثه و تحلیل یافته‌ها

تضمین امنیت، مؤلفه‌ای حیاتی در حاکمیت مؤثرفناوری اطلاعات است. چارچوب COBIT 2019ده کنترل جامع ارائه می‌دهد که امنیتفناوری اطلاعات را پوشش می‌دهند. با این حال، اولویت انتخاب و پیاده‌سازی این کنترل‌ها در این چارچوب مشخص نیست. بنابراین، از روش‌های MCDM برای مقایسه و رتبه‌بندی آن‌ها استفاده کردیم. در ادامه این بخش، به پرسش‌های پژوهش که در بخش مقدمه معرفی شدند پاسخ می‌دهیم تا بحث جامع‌تری درباره روش‌شناسی و دستاوردهای این مقاله تسهیل شود.

### روش‌های MCDM چگونه می‌توانند در اولویت‌بندی کنترل‌های امنیتی چارچوب COBIT 2019مفید باشند؟

روش‌های MCDM به ما امکان می‌دهند گزینه‌های مختلف را بر اساس معیارهای متعدد ارزیابی و اولویت‌بندی کنیم. این روش‌ها به دلیل توانایی در گنجاندن معیارهای اطلاعاتی COBITدر رتبه‌بندی کنترل‌های امنیتی، می‌توانند نتایج دقیق و واقع‌گرایانه‌ای به دست دهند. در مدل ما، گزینه‌ها شامل ۱۰ کنترل امنیتی از چارچوب COBIT 2019 بودند که در فرایندهای :APO13» مدیریت امنیت» و :DSS05» مدیریت خدمات امنیتی» تعریف شده‌اند. این گزینه‌ها بر اساس پنج معیار اطلاعاتی COBIT (محرمانگی، یکپارچگی، دسترس‌پذیری، انطباق و قابلیت اعتماد) ارزیابی شدند.

### کدام روش MCDM برای رتبه‌بندی کنترل‌های امنیتی چارچوب COBIT 2019 استفاده می‌شود؟ روش انتخاب‌شده چگونه کار می‌کند؟

استفاده از روش‌های MCDM برای رتبه‌بندی کنترل‌های امنیتی چارچوب COBIT 2019امکان‌پذیر است. هر روش مزایا و معایب خود را دارد و تعیین مؤثرترین رویکرد به محدودیت‌ها و شرایط مسئله بستگی دارد.

در این مقاله، از ترکیب روش‌های AHP و TOPSIS استفاده کردیم. روش AHP برای رتبه‌بندی گزینه‌ها فرایندی طولانی است، زیرا شامل ایجاد مقایسه‌های زوجی گزینه‌ها نسبت به معیارهاست. در مواردی که گزینه‌های زیادی وجود دارد، روش TOPSIS بهتر عمل می‌کند. با این حال، روش TOPSIS نمی‌تواند وزن معیارها را محاسبه کند، بنابراین وزن‌ها

باید با روش‌های دیگر تعیین و سپس به روش TOPSIS وارد شوند. به همین دلیل، ابتدا از روش AHP برای محاسبه وزن معیارها و سپس از روش TOPSIS برای رتبه‌بندی گزینه‌ها با استفاده از وزن‌های به‌دست‌آمده از AHP استفاده کردیم.

بر اساس نتایج، ۱۰ کنترل امنیتی ارزیابی‌شده از بالاترین به پایین‌ترین بر اساس امتیازهایشان رتبه‌بندی شدند. برای نمونه، کنترل «حفاظت در برابر نرم‌افزارهای مخرب» با امتیاز ۰٫۷۶۳ بالاترین رتبه را کسب کرد، در حالی که کنترل «مدیریت اسناد حساس و دستگاه‌های خروجی» با امتیاز ۰٫۲۸۰ پایین‌ترین رتبه را به دست آورد.

این نتایج می‌تواند به مدیران امنیتی در اتخاذ تصمیم‌های بهتر در حوزه امنیت از طریق اولویت‌بندی صحیح وظایف کمک کند. آن‌ها می‌توانند از مزایایی مانند مدیریت بهتر ریسک، افزایش کارایی، بهبود برنامه‌ریزی و هماهنگی، ارتقای کیفیت خدمات، افزایش اعتماد عمومی و در نهایت دستیابی به اهداف حاکمیتفناوری اطلاعات بهره‌مند شوند. نتایج این مطالعه می‌تواند به‌عنوان منبعی ارزشمند توسط گروه‌های مختلف، از جمله اعضای هیئت‌مدیره، مدیران ارشد، مدیرانفناوری اطلاعات، مدیران کسب‌وکار، خبرگان کنترل‌های امنیتی، حسابرسان داخلی و حتی دانشجویان و پژوهشگران، استفاده شود.

## نتیجه‌گیری

این مقاله از ترکیب دو روشMCDM ، یعنی AHP وTOPSIS ، برای رتبه‌بندی کنترل‌های امنیتی چارچوب COBIT 2019 استفاده کرد. نتایج فهرستی از کنترل‌های امنیتی را ارائه داد که از بالاترین به پایین‌ترین بر اساس امتیاز کلی آن‌ها رتبه‌بندی شده بودند. نتایج می‌تواند منبعی ارزشمند برای تیم‌های امنیتی مختلف باشد و به آن‌ها امکان دهد کنترل‌های مؤثرتری برای جلوگیری از تهدیدهای امنیتی پیاده‌سازی کنند. این امر به‌نوبه خود می‌تواند به کاهش زمان و هزینه، بهبود عملکرد سازمانی و افزایش کارایی منجر شود .به‌عنوان بخشی از تحقیقات آینده پیشنهاد می کنیم، هزینه‌اثربخشی پیاده‌سازی کنترل‌های تحلیل‌شده را در یک سازمان بررسی کنیم. جنبه دیگر کار آینده ما رتبه‌بندی فرایندهای مرتبط با سایر حوزه‌های چارچوب COBIT است. علاوه بر این، می‌توانیم از روش‌های MCDM دیگر مانندANP ، ELECTRE، PROMETHEEو روش‌های مشابه برای رتبه‌بندی استفاده کنیم. استفاده

از روش‌های MCDM فازی یا گروهی نیز می‌تواند گزینه‌های مناسبی برای رتبه‌بندی باشد، زیرا می‌تواند به تعیین بهترین کنترل‌ها در حوزه‌های مختلف حاکمیتفناوری اطلاعات و ارتقای عملکرد و کارایی سازمان‌ها کمک کند.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## References

Ahriz, S., El Yamami, A., Mansouri, K. and Qbadou, M. (2018), "Cobit 5-based approach for IT project portfolio management: application to a Moroccan university", International Journal of Advanced Computer Science and Applications, Vol. 9 No. 4, pp. 88-95, doi: 10.14569/IJACSA.2018.090416.

Almeida, R., Souza Neto, J. and Mira da Silva, M. (2018), "Using analytic hierarchy process for COBIT 5 process prioritization", in 24th Americas Conference on Information Systems, Los Angeles, USA.

Behzadian, M., Otaghssara, S. K., Yazdani, M. and Ignatius, J. (2012), "A state-of-the-art survey of TOPSIS applications", Expert Systems with Applications, Vol. 39 No. 17, pp. 13051-13069, doi: 10.1016/j.eswa.2012.05.056.

De Haes, S., Van Grembergen, W., Joshi, A. and Huygh, T. (2019), Enterprise governance of information technology: achieving alignment and value in digital organizations, Springer International Publishing, New York, NY.

Emovon, I. and Oghenenyerowho, O. S. (2020), "Application of MCDM method in material selection for optimal design: a review", Results in Materials, Vol. 7, p. 100115, doi: 10.1016/j.rinma.2020.100115.

Fasihuddin, H., Alharbi, S., Alshehri, A., Alzahrani, A. and Fatani, H. (2022), "Measuring the maturity of information technology governance based on COBIT", Romanian Journal of Information Technology & Automatic Control, Vol. 32 No. 2, pp. 65-78, doi: 10.33436/v32i2y202205.

Febriana, H., Ginting, D. S. B. and Manik, F. Y. (2022), "The applied approach impact information security for government and company (a review)", Data Science: Journal of Computing and Applied Informatics, Vol. 6 No. 1, pp. 45-54, doi: 10.32734/jocai.v6.11-7935.

Franek, J. and Kresta, A. (2014), "Judgment scales and consistency measure in AHP", Procedia Economics and Finance, Vol. 12, pp. 164-173, doi: 10.1016/S2212-5671(14)00332-3.

Ghelani, D., Hua, T. K. and Koduru, S. K. R. (2022), "Cyber security threats, vulnerabilities, and security solutions models in banking", Authorea Preprints, doi: 10.22541/au.166385206.633111335/v1.

Ginting, G., Fadlina, M., Siahaan, A. P. U. and Rahim, R. (2017), "Technical approach of TOPSIS in decision making", International Journal of Recent Trends in Engineering, Vol. 3 No. 8, pp. 58-64.

Gorry, G. A. and Scott Morton, M. S. (1971), "A framework for management information systems", Sloan Management Review, Vol. 13 No. 1, pp. 55-70.

Harguem, S., Boubaker, K. B. and Echatti, H. (2022), "Information technology governance in the Tunisian banking industry: an exploratory study", Academic Journal of Interdisciplinary Studies, Vol. 11 No. 3, pp. 121-133, doi: 10.36941/ajis-2022-0072.

Hwang, C. L. and Yoon, K. (1981), "Multiple attribute decision making", in Wallenius, J. (Ed.), Lecture Notes in Economics and Mathematical Systems, Berlin, pp. 58-191.

ISACA (2007), COBIT 4.1: framework, control objectives, management guidelines, maturity models, IT Governance Institute, Schaumburg, USA.

ISACA (2018), COBIT 2019 framework: governance and management objectives, IT Governance Institute, Schaumburg, USA.

Joshi, A., Benitez, J., Huygh, T., Ruiz, L. and De Haes, S. (2022), "Impact of IT governance process capability on business performance: theory and empirical evidence", Decision Support Systems, Vol. 153, p. 113668, doi: 10.1016/j.dss.2021.113668.

Kori, D. and Naik, R. (2023), "Information security awareness among postgraduate students: a study of Mangalore University", in Holland, B. J. (Ed.), Handbook of Research on Technological Advances of Library and Information Science in Industry 5.0, IGI Global, Pennsylvania, USA, pp. 270-286, doi: 10.4018/978-1-6684-4755-0.ch014.

Makhsud, U. (2021), "Practical security management", International Journal of Academic Engineering Research (IJAER), Vol. 5 No. 1, pp. 71-74.

Malatji, M. (2023), "Management of enterprise cyber security: a review of ISO/IEC 27001: 2022", in 2023 International Conference on Cyber Management and Engineering (CyMaEn), Bangkok, Thailand, pp. 117-122, doi: 10.1109/CyMaEn57228.2023.10051114.

Nugroho, H. (2019), "A review on information system audit using COBIT framework", International Journal of Applied Information Technology, Vol. 3 No. 2, pp. 46-52, doi: 10.25124/ijait.v3i02.2114.

Rahim, R., Supiyandi, S., Siahaan, A., Listyorini, T., Utomo, A. P., Triyanto, W. A., Irawan, Y., Aisyah, S., Khairani, M. and Sundari, S. (2018), "TOPSIS method application for decision support system in internal control for selecting best employees", Journal of Physics: Conference Series, Vol. 1028, p. 012052, doi: 10.1088/1742-6596/1028/1/012052.

Rainer, R. K. and Prince, B. (2021), Introduction to information systems, John Wiley & Sons, New York, NY.

Ramanathan, R. (2006), "Data envelopment analysis for weight derivation and aggregation in the analytic hierarchy process", Computers & Operations Research, Vol. 33 No. 5, pp. 1289-1307, doi: 10.1016/j.cor.2004.09.020.

Rouhani, S. and Ravasan, A. Z. (2014), "A fuzzy TOPSIS based approach for ITSM software selection", International Journal of IT/Business Alignment and Governance (IJITBAG), Vol. 5 No. 2, pp. 1-26.

Saaty, R. W. (1987), "The analytic hierarchy process—what it is and how it is used", Mathematical Modelling, Vol. 9 No. 3-5, pp. 161-176, doi: 10.1016/0270-0255(87)90473-8.

Saaty, T. L. (1977), "A scaling method for priorities in hierarchical structures", Journal of Mathematical Psychology, Vol. 15 No. 3, pp. 234-281, doi: 10.1016/0022-2496(77)90033-5.
Saaty, T. L. (1980), The analytic hierarchy process: planning, priority setting, resource allocation, McGraw Hill, New York, NY.
Saaty, T. L. (1988), What is the analytic hierarchy process?, Springer, Berlin, DE.
Saaty, T. L. (1990), "How to make a decision: the analytic hierarchy process", European Journal of Operational Research, Vol. 48 No. 1, pp. 9-26, doi: 10.1016/0377-2217(90)90057-1.
Saaty, T. L. (2008), "Decision making with the analytic hierarchy process", International Journal of Services Sciences, Vol. 1 No. 1, pp. 83-98, doi: 10.1504/IJSSCI.2008.017590.
Sadreddin, A. and Chan, Y. E. (2023), "Pathways to developing information technology-enabled capabilities in born-digital new ventures", International Journal of Information Management, Vol. 68, p. 102572, doi: 10.1016/j.ijinfomgt.2022.102572.
Saeed, V. A. and Asaad, R. (2022), "A cyber security threats, vulnerability, challenges and proposed solution", Applied Computing Journal, Vol. 2 No. 4, pp. 227-244.
Smith, K. J. (2017), The practical guide to world-class IT service management, Outskirts Press, Colorado, USA.
Steuperaert, D. (2019), "COBIT 2019: a significant update", EDPACS, Vol. 59 No. 1, pp. 14-18, doi: 10.1080/07366981.2019.1578474.
Symons, C., Cecere, M., Young, O. and Lambert, N. (2005), IT governance framework: structures, processes and communication, Forrester Research Inc.
Taherdoost, H. (2023), "An overview of trends in information systems: emerging technologies that transform the information technology industry", Cloud Computing and Data Science, Vol. 4 No. 1, pp. 1-16, doi: 10.37256/ccds.4120231653.
Taherdoost, H. and Madanchian, M. (2023), "Multi-criteria decision making (MCDM) methods and concepts", Encyclopedia, Vol. 3 No. 1, pp. 77-87, doi: 10.3390/encyclopedia3010006.
Toyner, L. G. and Sfenrianto, S. (2023), "Information system security evaluation using Cobit 5 framework", Journal of Information System Management (JOISM), Vol. 4 No. 2, pp. 147-157, doi: 10.24076/joism.2023v4i2.992.
Tulus, B. V. and Tanaamah, A. R. (2023), "Design of information technology governance in educational institutions using COBIT 2019 framework", Journal of Information Systems and Informatics, Vol. 5 No. 1, pp. 31-43, doi: 10.51519/journalis.v5i1.408.
Utamajaya, J. N., Supangat, S. H., Gaol, F. L. and Ranti, B. (2023), "Hotel information system management audit using COBIT 2019-APO12", in 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, pp. 1-7, doi: 10.1109/INOCON57975.2023.10101245.
Vafaei, N., Ribeiro, R. A. and Camarinha-Matos, L. M. (2016), "Normalization techniques for multi-criteria decision making: analytical hierarchy process case study", in Technological Innovation for Cyber-Physical Systems, pp. 261-269, doi: 10.1007/978-3-319-31165-4_26.
Van Schaik, E. A. (1985), A management system for the information business: organizational analysis, Prentice-Hall Inc, New Jersey, NJ.
Wang, Y., Peng, X. and Prybutok, V. (2022), "The importance of information technology to organizational results within the Baldrige award", Quality Management Journal, Vol. 29 No. 1, pp. 3-17, doi: 10.1080/10686967.2021.2006584.

Xu, J. and Lu, W. (2022), “Developing a human-organization-technology fit model for information technology adoption in organizations”, Technology in Society, Vol. 70, p. 102010, doi: 10.1016/j.techsoc.2022.102010.
Yoon, K. P. and Kim, W. K. (2017), “The behavioral TOPSIS”, Expert Systems with Applications, Vol. 89, pp. 266-272, doi: 10.1016/j.eswa.2017.07.045.
Zavadskas, E. K., Turskis, Z. and Kildienė, S. (2014), “State of art surveys of overviews on MCDM/MADM methods”, Technological and Economic Development of Economy, Vol. 20 No. 1, pp. 165-179, doi: 10.3846/20294913.2014.892037.

## پیوست ۱

*فهرست کنترل ها و فعالیت مرتبط رتبه بندی شده*

| NO | Controls | Activities (ISACA, 2018) |
|---|---|---|
| 1 | Protect against malicious software | 1. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).<br>2. Filter incoming traffic, such as emails and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).<br>3. Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and to not install shared or unapproved software.<br>4. Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management<br>5. Regularly review and evaluate information on new potential threats (e.g., reviewing vendors’ products and services security advisories) |
| 2 | Manage network and connectivity security | 1. Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry<br>2. Implement network filtering mechanisms, such as firewalls and intrusion detection software. Enforce appropriate policies to control inbound and outbound traffic.<br>3. Apply approved security protocols to network connectivity<br>4. Configure network equipment in a secure manner<br>5. Encrypt information in transit according to its classification<br>6. Based on risk assessments and business requirements, establish and maintain a policy for the security of connectivity<br>7. Establish trusted mechanisms to support the secure transmission and receipt of information<br>8. Carry out periodic penetration testing to determine adequacy of network protection<br>9. Carry out periodic testing of system security to determine adequacy of system protection. |

| NO | Controls | Activities (ISACA, 2018) |
|---|---|---|
| 3 | Establish and maintain an information security management system (ISMS) | 1. Define the scope and boundaries of the information security management system (ISMS) in terms of the characteristics of the enterprise, the organization, its location, assets, and technology. Include details of and justification for any exclusions from the scope.<br>2. Define an ISMS in accordance with enterprise policy and the context in which the enterprise operates<br>3. Align the ISMS with the overall enterprise approach to the management of security<br>4. Obtain management authorization to implement and operate or change the ISMS.<br>5. Prepare and maintain a statement of applicability that describes the scope of the ISMS<br>6. Define and communicate Information security management roles and responsibilities<br>7. Communicate the ISMS approach |
| 4 | Manage user identity and logical access | 1. Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles<br>2. Administer all changes to access rights (creation, modifications and deletions) in a timely manner based only on approved and documented transactions authorized by designated management individuals.<br>3. Segregate, reduce to the minimum number necessary and actively manage privileged user accounts. Ensure monitoring on all activity on these accounts<br>4. Uniquely identify all information processing activities by functional roles. Coordinate with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications.<br>5. Authenticate all access to information assets based on the individual's role or business rules. Coordinate with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered<br>6. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable<br>7. Maintain an audit trail of access to information depending upon its sensitivity and regulatory requirements<br>8. Perform regular management review of all accounts and related privileges |
| 5 | Manage endpoint security | 1. Configure operating systems in a secure manner<br>2. Implement device lockdown mechanisms<br>3. Manage remote access and control (e.g., mobile devices, teleworking)<br>4. Manage network configuration in a secure manner |

| NO | Controls | Activities (ISACA, 2018) |
|---|---|---|
| | | 5. Implement network traffic filtering on endpoint devices<br>6. Protect system integrity<br>7. Provide physical protection of endpoint devices<br>8. Dispose of endpoint devices securely<br>9. Manage malicious access through email and web browsers. For example, block certain websites and deactivate click-through on links for smartphones<br>10. Encrypt information in storage according to its classification |
| 6 | Define and manage an information security and privacy risk treatment plan | 1. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk<br>2. Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage securityrelated risk.<br>3. Develop proposals to implement the information security risk treatment plan, supported by suitable business cases that include consideration of funding and allocation of roles and responsibilities<br>4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan<br>5. Implement information security and privacy training and awareness programs<br>6. Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt prevention, detection of security events, and response to security incidents.<br>7. Define how to measure the effectiveness of the selected management practices. Specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results |
| 7 | Manage vulnerabilities and monitor the infrastructure for security-related events | 1. Continually use a portfolio of supported technologies, services and assets (e.g., vulnerability scanners, fuzzers and sniffers, protocol analyzers) to identify information security vulnerabilities<br>2. Define and communicate risk scenarios, so they can be easily recognized, and the likelihood and impact understood<br>3. Regularly review the event logs for potential incidents<br>4. Ensure that security-related incident tickets are created in a timely manner when monitoring identifies potential incidents.<br>5. Log security-related events and retain records for appropriate period. |
| 8 | Manage physical access to I&T assets | 1. Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.<br>2. Ensure all personnel display properly approved identification at all times<br>3. Require visitors to be escorted at all times while on-site |

| NO | Controls | Activities (ISACA, 2018) |
|---|---|---|
| | | 4. Restrict and monitor access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls and security devices on interior and exterior doors.<br>5. Manage requests to allow appropriately authorized access to the computing facilities.<br>6. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.<br>7. Conduct regular physical information security awareness training. |
| 9 | Monitor and review the information security management system (ISMS) | 1. Undertake regular reviews of the effectiveness of the ISMS. Include meeting ISMS policy and objectives and reviewing security and privacy practices<br>2. Conduct ISMS audits at planned intervals.<br>3. Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified<br>4. Record actions and events that could have an impact on the effectiveness or performance of the ISMS<br>5. Provide input to the maintenance of the security plans to take into account the findings of monitoring and reviewing activities |
| 10 | Manage sensitive documents and output devices | 1. Establish procedures to govern the receipt, use, removal and disposal of sensitive documents and output devices into, within, and outside of the enterprise<br>2. Ensure cryptographic controls are in place to protect sensitive electronically stored information<br>3. Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements<br>4. Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.<br>5. Establish appropriate physical safeguards over sensitive documents |

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Research Paper**

# Proposing an Exploratory Conceptual Framework for Algorithmic Governance, Intelligent Audit Supervision and Data-Driven Entrepreneurship Development: A Fuzzy Delphi Study in Kermanshah, Iran [1]

**Bijan Rezaee [*2], Arash Khademi [3] and Rasoul Mohammadi[4]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 61-96

Received: 2026.07.25
Revised: 2026.09.24
Accepted: 2026.10.21

## Abstract

This study aimed to develop an exploratory conceptual framework to elucidate the requirements for algorithm-based governance, intelligent audit oversight, and data-driven entrepreneurship development. The city of Kermanshah served as the empirical setting for developing the conceptual framework. However, the proposed framework is not confined to the specific characteristics of this city, and the identified factors may also be examined in other urban contexts. An exploratory mixed-methods approach was adopted. Components were identified through semi-structured interviews and subsequently refined and prioritized using the fuzzy Delphi method based on expert judgments. The findings yielded 15 factors grouped into five dimensions. The results reflect expert consensus on the identified factors and their relative priorities and do not constitute evidence of causal relationships among the framework's dimensions. The study contributes to the literature by offering an integrated framework that connects algorithm-based governance, intelligent auditing, and data-driven entrepreneurship at the urban level.

**Keywords**: Algorithmic Governance, Intelligent Audit Oversight, Data-Driven Entrepreneurship, Fuzzy Delphi Method, Kermanshah.

**JEL classification:** *M42.*

---

[1] https://doi.org/10.22034/JISTA.2026.593648.1091
[2] Associate Professor,Department of Management and Entrepreneurship, Razi University, Kermanshah, Iran. (Corresponding Author). Email: b.rezaee@razi.ac.ir
[3] PhD Student of Entrepreneurship Management,Department of Management and Entrepreneurship, Razi University, Kermanshah, Iran. Email: arashkhademi705@gmail.com
[4] PhD Student of Entrepreneurship Management,Department of Management and Entrepreneurship, Razi University, Kermanshah, Iran. Email: rasolmohamadi108@gmail.com

## 1. INTRODUCTION

Public and municipal organizations generate large volumes of financial, contractual, transactional, and operational data. However, data volume alone does not prevent error, misconduct, or fraud. Periodic, sample-based, and retrospective audits can leave high-risk transactions unexamined until corrective action becomes costly. Intelligent audit supervision addresses this limit by combining continuous data analysis, control rules, artificial intelligence, and professional judgment. It can screen broader transaction populations and identify unusual patterns near the time of occurrence, but it must support rather than replace the auditor's judgment (Appelbaum et al., 2017; Issa et al., 2016).

Algorithmic governance provides the institutional rules for the use of data and algorithms in risk assessment, prioritization, monitoring, and public decision-making. A valid governance arrangement must combine technical performance with data quality, transparency, explainability, accountability, privacy protection, human oversight, and a clear right to review decisions (Abraham et al., 2019; Tabassi, 2023; Yeung, 2018). These safeguards are also important for data-driven entrepreneurship. Reliable and responsibly shared public data can support opportunity recognition, service design, and business innovation, whereas poor-quality or unrestricted data can reduce trust and create legal and ethical risks (Grimaldi et al., 2026).

Previous studies usually examine algorithmic governance, intelligent auditing, and data-driven entrepreneurship as separate fields. This separation is important in Kermanshah, where effective entrepreneurial development depends on coordination among public agencies, municipal management, universities, financial institutions, and private firms (Shakiba et al., 2020). No integrated local model has shown which governance principles can improve audit supervision while enabling the responsible reuse of trusted data. Therefore, this study aimed to develop and prioritize an urban-level algorithmic governance model for intelligent audit supervision and data-driven entrepreneurship in Kermanshah, Iran.

## 2. MATERIALS AND METHODS

This applied study employed a sequential exploratory mixed-method design. The study population consisted of academic and executive experts in accounting and auditing, public and urban management, information technology, artificial intelligence, data governance, and entrepreneurship in Kermanshah. Thirty experts were selected through criterion-based purposive sampling with limited snowball recruitment. All participants held at least a master's degree and had a minimum of five years of relevant professional experience.

The qualitative phase used semi-structured interviews with nine main questions. Each interview lasted 30-45 minutes and was recorded with participant consent. The researchers used ATLAS.ti for open and in-vivo coding. They reviewed the codes repeatedly, removed duplicates, and combined similar concepts. This process reduced 146 initial codes to 53 independent codes, which formed 15 factors in five dimensions. The quantitative phase used a two-round fuzzy Delphi questionnaire. Five linguistic ratings, from very low to very high, were converted to triangular fuzzy numbers, and the centroid method produced a defuzzified score (Ishikawa et al., 1993). After round one, the anonymous group mean was returned to the panel. A factor was retained when its score was at least 0.50 and at least 75% of experts selected high or very high. Consensus was reached when the change between rounds was less than 0.10. The method identified and prioritized factors; it did not test direct, indirect, or causal relations.

## 3. RESULTS AND DISCUSSION

The The panel included 21 men and 9 women. Nineteen participants (63.3%) held doctoral degrees, and 11 (36.7%) held master's degrees. The four expertise groups were relatively balanced in size. academic and research experts and audit and financial management experts each represented 26.7% of the panel, while information technology and data experts and entrepreneurship and innovation experts each represented 23.3%. The qualitative analysis

produced three factors for data and technology infrastructure, four for algorithmic governance, four for intelligent audit supervision, two for organizational requirements, and two for data-driven entrepreneurship.

All 15 factors passed both acceptance criteria. Defuzzified scores ranged from 0.683 to 0.822 in round one and from 0.747 to 0.856 in round two. The change between rounds ranged from 0.028 to 0.069, which was below the 0.10 consensus threshold for every factor. Table 1 presents the six highest priorities. Information security and privacy ranked first. Data quality and integration and continuous monitoring and intelligent alerts shared second place, followed by anomaly and fraud detection.

**Table 1**

*Highest-ranked factors in the second fuzzy Delphi round*

| Rank | Factor | Final score |
|---|---|---|
| 1 | Information security and privacy | 0.856 |
| 2 | Data quality and integration | 0.850 |
| 2 | Continuous monitoring and intelligent alerts | 0.850 |
| 4 | Anomaly and fraud detection | 0.844 |
| 5 | Algorithm transparency and explainability | 0.831 |
| 5 | Legal and regulatory framework for algorithms | 0.831 |

The priority pattern shows that intelligent supervision requires a trusted data foundation before advanced analytics can produce valid audit evidence. The high scores for transparency, explainability, and a legal and regulatory framework also show that technical accuracy is not sufficient. Auditors and managers must be able to inspect the basis of a high-risk classification, identify responsibility, preserve an audit trail, and use human review for sensitive actions. The factor 'conversion of data into entrepreneurial opportunities' received a score of 0.808. Controlled access to public data received the lowest score, 0.747, but remained well above the acceptance threshold.

Thus, the panel did not reject public-data reuse; it treated secure, classified, and accountable access as a condition for reuse. These results connect oversight and economic value creation in one framework. However, the close factor weights and the Delphi design support a conclusion about expert consensus and priority only. They do not prove that one factor causes another or that intelligent auditing directly increases entrepreneurship.

## 4. CONCLUSION

The proposed model integrates data and technology infrastructure, algorithmic governance, intelligent audit supervision, organizational requirements, and data-driven entrepreneurship in one contingent urban framework. The results show that a city should not begin with automation alone. It should first improve data quality, interoperability, security, and privacy. It should then establish explainable decision rules, clear accountability, human review, traceable audit records, and a legal basis for data use. Management support, auditor digital competence, interorganizational cooperation, and controlled data access can then support both continuous supervision and responsible entrepreneurial use. The study is limited by purposive sampling in one city and by the non-causal nature of fuzzy Delphi analysis. Future studies should validate the model with structural equation modeling and larger samples, compare it across cities, and test pilot applications in municipal contracts, tenders, and payments.

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# ارائه چارچوب مفهومی اکتشافی حکمرانی الگوریتمیک در نظارت هوشمند حسابرسی و توسعه کارآفرینی داده‌محور با رویکرد دلفی فازی[1]

**بیژن رضایی[2]*، آرش خادمی[3] و رسول محمدی[4]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۶۱ - ۹۶

تاریخ دریافت: ۱۴۰۵/۰۵/۰۳
تاریخ بازنگری: ۱۴۰۵/۰۷/۰۲
تاریخ پذیرش: ۱۴۰۵/۰۷/۲۹

## چکیده

*پژوهش حاضر با هدف ارائه چارچوب مفهومی اکتشافی برای تبیین الزامات حکمرانی مبتنی بر الگوریتم، نظارت هوشمند حسابرسی و توسعه کارآفرینی داده‌محور انجام شد. شهر کرمانشاه در این پژوهش، بستر تجربی تدوین چارچوب مفهومی بوده است؛ بااین‌حال، چارچوب پیشنهادی به ویژگی‌های خاص این شهر محدود نیست و عوامل شناسایی‌شده قابلیت بررسی در سایر محیط‌های شهری را نیز دارند. این پژوهش با رویکرد آمیخته اکتشافی انجام شد. مؤلفه‌ها از طریق مصاحبه نیمه‌ساختاریافته استخراج و با استفاده از دلفی فازی توسط خبرگان پالایش و اولویت‌بندی شدند. یافته‌ها به شناسایی ۱۵ عامل در پنج بُعد منجر شد. نتایج بیانگر اجماع تخصصی و اولویت نسبی عوامل است و به معنای آزمون روابط علّی میان ابعاد چارچوب نیست .دانش‌افزایی پژوهش در ارائه چارچوبی یکپارچه برای پیوند حکمرانی الگوریتمیک، حسابرسی هوشمند و کارآفرینی داده‌محور در سطح شهری است .*

**واژه‌های کلیدی:** *حکمرانی الگوریتمیک، نظارت هوشمند حسابرسی، کارآفرینی داده‌محور، دلفی فازی، شهر کرمانشاه.*

**طبقه‌بندی موضوعی:** *M42*

---

[1] https://doi.org/10.22034/JISTA.2026.593648.1091

[2] دانشیار گروه مدیریت و کارآفرینی، دانشکده مدیریت و اقتصاد، دانشگاه رازی، کرمانشاه، ایران. (نویسنده مسئول). (b.rezaee@razi.ac.ir)

[3] دانشجوی دکتری تخصصی مدیریت کارآفرینی، گروه مدیریت و کارآفرینی ، دانشکده مدیریت و اقتصاد، دانشگاه رازی ،کرمانشاه، ایران. (arashkhademi705@gmail.com)

[4] دانشجوی دکتری تخصصی مدیریت کارآفرینی، گروه مدیریت و کارآفرینی ، دانشکده مدیریت و اقتصاد، دانشگاه رازی ،کرمانشاه، ایران. (rasolmohamadi108@gmail.com)

## مقدمه

افزایش حجم داده‌های مالی و معاملاتی، الزاماً به کاهش تخلف و انحراف منجر نمی‌شود. سازمان‌های عمومی و مدیریت‌های شهری می‌توانند روزانه هزاران داده مربوط به قراردادها، پرداخت‌ها، مناقصه‌ها، درآمدها، هزینه‌ها و عملکرد واحدهای اجرایی تولید کنند؛ اما هنگامی که فرایند حسابرسی همچنان دوره‌ای، نمونه‌محور و پس از وقوع رویداد باشد، بخش قابل‌توجهی از ظرفیت این داده‌ها برای پیشگیری، هشداردهی و اصلاح به‌موقع بلااستفاده باقی می‌ماند. مسئله اصلی کمبود داده نیست. مسئله، فقدان سازوکاری است که داده را به تصمیم نظارتی معتبر تبدیل کند. افزایش حجم و پیچیدگی فعالیت‌های دستگاه‌های عمومی، در کنار محدودیت منابع انسانی و زمانی حسابرسان، سبب شده است روش‌های سنتی نتوانند تمام قلمروهای پرریسک را با سرعت، دقت و جامعیت کافی پوشش دهند (مطلبی کربکندی و همکاران، ۱۴۰۱: ۸۲-۷۹) .

عبور از این محدودیت، صرفاً با خرید نرم‌افزار یا خودکارسازی چند فعالیت اداری امکان‌پذیر نیست؛ زیرا مسئله پیش‌گفته، ماهیتی نهادی و حکمرانی دارد. «حکمرانی الگوریتمیک» به مجموعه ترتیبات، قواعد و فرایندهایی اطلاق می‌شود که در آن داده‌ها و الگوریتم‌ها برای شناخت وضعیت، ارزیابی ریسک، اولویت‌بندی موارد، تخصیص منابع، پایش رفتار و پشتیبانی یا اجرای تصمیم‌ها به کار گرفته می‌شوند. در این الگو، الگوریتم تنها یک ابزار محاسباتی نیست، بلکه در نحوه توزیع اختیار، مسئولیت و قدرت تصمیم‌گیری نقش پیدا می‌کند. تنظیم‌گری الگوریتمی نیز بر گردآوری مستمر داده و تولید دانش محاسباتی برای تشخیص انحراف از استانداردها و اصلاح عملکرد نظام استوار است (یانگ[1]، ۲۰۱۸ :۵۰۵-۵۰۸).

بااین‌حال، افزایش سرعت تصمیم‌گیری می‌تواند با کاهش قابلیت فهم آن همراه شود. تصمیم‌های مبتنی بر الگوریتم ممکن است تحت تأثیر کیفیت نامطلوب داده، سوگیری مدل، طراحی نادرست شاخص‌ها یا منافع طراحان سامانه قرار گیرند. ازاین‌رو، حکمرانی الگوریتمیک مطلوب مستلزم شفافیت، توضیح‌پذیری، پاسخ‌گویی، امکان اعتراض، حفاظت از حریم خصوصی و استمرار نظارت انسانی است. پژوهش‌های حقوق اداری ایران نیز نشان داده‌اند که استفاده از تصمیم‌گیری الگوریتمی، در کنار مزایایی مانند افزایش سرعت و کاهش هزینه،

[1] Yeung

می‌تواند اصولی چون عدالت رویه‌ای، بی‌طرفی، منع تبعیض و نظارت بر صلاحیت اداره را با چالش مواجه کند (مرادی‌برلیان و تنگستانی، ۱۴۰۲: ۱۷۲-۱۶۳) .این دوگانگی اهمیت دارد. کارایی بدون پاسخ‌گویی کافی نیست. مشروعیت سازوکارهای الگوریتمی زمانی تقویت می‌شود که آثار آنها بر ذی‌نفعان قابل بررسی باشد و مسئولیت خطا میان مدیر، حسابرس، طراح سامانه و نهاد مالک داده مبهم باقی نماند (داناهر و همکاران[1] ، ۲۰۱۷ :۱-۶).

الزامات شفافیت، پاسخ‌گویی و نظارت انسانی در حکمرانی مبتنی بر الگوریتم، مبنای تبیین «نظارت هوشمند حسابرسی» در پژوهش حاضر است. در این چارچوب، نظارت هوشمند حسابرسی به سازوکاری یکپارچه برای پایش داده‌های مالی، عملیاتی، قراردادی و عملکردی اشاره دارد که در آن، تحلیل داده، هوش مصنوعی و قواعد کنترلی در کنار قضاوت حرفه‌ای حسابرس به کار گرفته می‌شوند. هدف این سازوکار، شناسایی به‌موقع معاملات غیرعادی، الگوهای پرریسک، ضعف‌های کنترل داخلی و نشانه‌های احتمالی تقلب است. استفاده از این قابلیت‌ها می‌تواند دامنه رسیدگی را گسترش دهد و توان حسابرس را برای شناسایی روابط و الگوهای پنهان در تراکنش‌ها افزایش دهد (اپلبام و همکاران[2]، ۲۰۱۷: ۵-۱). بااین‌حال، تفسیر نتایج و تصمیم‌گیری درباره موارد شناسایی‌شده همچنان مستلزم قضاوت حرفه‌ای است و هوش مصنوعی در این فرایند نقشی مکمل دارد (عیسی و همکاران[3]، ۲۰۱۶: ۷-۱). از این منظر، تبیین نظارت هوشمند حسابرسی مستلزم توجه هم‌زمان به قابلیت‌های فنی تحلیل داده و ترتیبات نهادیِ دسترسی به داده‌ها، پاسخ‌گویی در قبال نتایج و تعیین مسئولیت تصمیم‌هاست؛ پیوندی که ضرورت بررسی جایگاه این ترتیبات در ادبیات حسابرسی هوشمند را مطرح می‌کند. نقطه کور ادبیات حسابرسی هوشمند آن است که بیشتر پژوهش‌ها بر افزایش کارایی فنی، کشف تقلب، تحلیل کلان‌داده یا تحول حرفه حسابرسی تمرکز کرده‌اند، درحالی‌که قواعد مالکیت داده، مسئولیت الگوریتم، حق دسترسی ذی‌نفعان و نحوه استفاده ثانویه از داده‌های نظارتی کمتر در قالب یک مدل واحد بررسی شده است. حتی پژوهش‌های داخلی که مفهوم حسابرسی هوشمند را در سازمان‌های عالی نظارتی تبیین کرده‌اند، اذعان دارند که مطالعات قبلی غالباً به کاربردهای پراکنده فناوری در حسابرسی صورت‌های مالی محدود بوده و ابعاد حسابرسی هوشمند در سطح

[1] Danaher at al.
[2] Appelbaum et al.
[3] Issa et al.

یک نظام نظارتی به‌صورت جامع صورت‌بندی نشده است (مطلبی کربکندی و همکاران، ۱۴۰۱: ۸۹-۸۵) . در نتیجه، مشخص نیست داده‌های تولیدشده در فرایند نظارت چگونه باید علاوه بر کنترل انحراف، به یادگیری نهادی و خلق ارزش اقتصادی منجر شوند.

در این نقطه، مفهوم «کارآفرینی داده‌محور» اهمیت پیدا می‌کند. کارآفرینی داده‌محور فرایندی است که در آن داده و قابلیت تحلیل آن، به منبعی برای شناسایی مسئله، کشف فرصت، شناخت نیازهای بازار، طراحی محصول یا خدمت، اصلاح مدل کسب‌وکار و ایجاد نوآوری تبدیل می‌شود. در این رویکرد، کارآفرین تنها از ابزارهای دیجیتال برای عرضه محصول استفاده نمی‌کند؛ بلکه تصمیم‌های اصلی کسب‌وکار را بر پایه گردآوری، ترکیب و تفسیر داده‌ها شکل می‌دهد. داده می‌تواند میان خلق دانش، تشخیص فرصت‌های کارآفرینانه و ظهور نتایج نوآورانه پیوند برقرار کند (گریمالدی و همکاران[1]، ۲۰۲۶ :۱۳۴۱-۱۳۴۸). بااین‌حال، ادبیات این حوزه بیشتر بر قابلیت‌های بنگاه، مدیریت داده و نوآوری بازار تمرکز دارد و نقش اعتماد نهادی، کیفیت داده‌های عمومی و قابلیت حسابرسی منابع اطلاعاتی را کمتر وارد مدل‌های کارآفرینی کرده است.

در این پژوهش، کرمانشاه به‌عنوان بستر مطالعه انتخاب شده است. ویژگی‌های خاص این شهر مانند تعامل چندنهادی میان مدیریت شهری، سازمان‌های عمومی، دانشگاه‌ها و بازیگران اکوسیستم کارآفرینی، زمینه مناسبی برای بررسی کاربرد چارچوب فراهم می‌کنند؛ با این حال، ابعاد اصلی چارچوب (کیفیت داده، امنیت، شفافیت، نظارت انسانی و الزامات سازمانی) به دلیل ماهیت عمومی خود محدود به این شهر نیستند.

انتخاب شهر کرمانشاه به‌عنوان بستر مطالعه، از منظر چالش‌های تعامل نهادی در اکوسیستم کارآفرینی این شهر نیز قابل تبیین است. مطالعه شکیبا و همکاران نشان داده است که اختلاف ترجیحات و منافع بازیگران اکوسیستم کارآفرینی فراگیر کرمانشاه می‌تواند تداوم وضع موجود را به نتیجه‌ای محتمل‌تر از اصلاح ساختاری تبدیل کند (شکیبا و همکاران، ۱۳۹۹: ۱۳۱-۱۲۳). این یافته، اهمیت توجه به نحوه هماهنگی و همکاری بازیگران را در بررسی زمینه‌های توسعه کارآفرینی شهر برجسته می‌کند. در پژوهش حاضر، این مسئله از منظر ترتیبات حاکم بر تولید، تبادل و استفاده از داده بررسی می‌شود؛ به این معنا که دسترسی بازیگران به داده‌های قابل اتکا،

[1] Grimaldi et al.

حدود مسئولیت آنان در استفاده از داده‌ها و نقش نظارت حسابرسی در ارزیابی اعتبار اطلاعات، در چارچوبی مشترک مورد توجه قرار می‌گیرد. طرح این موضوع در بستر کرمانشاه، زمینه تبیین ضرورت پیوند میان حکمرانی مبتنی بر الگوریتم، نظارت هوشمند حسابرسی و کارآفرینی داده‌محور را فراهم می‌سازد.

با وجود مطالعات انجام‌شده، سه جریان پژوهشی حکمرانی الگوریتمیک، حسابرسی هوشمند و کارآفرینی داده‌محور عمدتاً به‌صورت جداگانه توسعه یافته‌اند. ادبیات حکمرانی الگوریتمیک بر مشروعیت و پاسخ‌گویی تصمیم‌ها تمرکز دارد؛ مطالعات حسابرسی هوشمند بیشتر به قابلیت‌های فنی نظارت می‌پردازند؛ و پژوهش‌های کارآفرینی داده‌محور، داده را منبع کشف فرصت و نوآوری تلقی می‌کنند. حلقه اتصال این حوزه‌ها هنوز ضعیف است. تاکنون مدلی بومی که مشخص کند اصول حکمرانی الگوریتمیک چگونه می‌توانند به‌طور هم‌زمان نظارت حسابرسی را هوشمندتر و بستر کارآفرینی داده‌محور را در شهر کرمانشاه تقویت کنند، به‌صورت منسجم ارائه نشده است. این خلأ، شکاف اصلی پژوهش حاضر را شکل می‌دهد.

بر این اساس، هدف پژوهش حاضر ارائه یک چارچوب مفهومی اکتشافی برای سازمان‌دهی ابعاد و عوامل مرتبط با حکمرانی الگوریتمیک، نظارت هوشمند حسابرسی و کارآفرینی داده‌محور در بستر شهری کرمانشاه است. این چارچوب مجموعه‌ای از ابعاد، مؤلفه‌ها و شاخص‌های شناسایی‌شده توسط خبرگان را در کنار یکدیگر قرار می‌دهد و ادعای آزمون روابط علّی یا پیش‌بینی اثر میان ابعاد را ندارد.

بر این اساس، هدف پژوهش حاضر ارائه مدل حکمرانی الگوریتمیک در نظارت هوشمند حسابرسی و توسعه کارآفرینی داده‌محور در شهر کرمانشاه است. منظور از مدل، مجموعه‌ای نظام‌مند از ابعاد، مؤلفه‌ها و شاخص‌هایی است که پنج بُعد زیرساخت داده و فناوری، حکمرانی الگوریتمیک، نظارت هوشمند حسابرسی، الزامات سازمانی و کارآفرینی داده‌محور را در چارچوبی یکپارچه قرار می‌دهد. اهمیت نظری پژوهش در پیوند دادن سه حوزه نسبتاً پراکنده است. اهمیت عملی آن نیز به ارائه چارچوبی برای استفاده پیشگیرانه، مسئولانه و ارزش‌آفرین از داده‌های مالی و شهری مربوط می‌شود. چنین مدلی می‌تواند از تبدیل نظارت هوشمند به سازوکاری صرفاً کنترل‌محور جلوگیری کند و در عین حال، مانع استفاده نامنظم، تبعیض‌آمیز یا غیرشفاف از داده‌های عمومی شود.

ازآنجاکه ابعاد مدل پیشنهادی در منابع موجود پراکنده‌اند و اهمیت آنها به قضاوت تخصصی و شرایط بومی وابسته است، پژوهش حاضر با رویکرد آمیخته کیفی و کمی و با استفاده از دلفی فازی اجرا می‌شود. در مرحله کیفی، مؤلفه‌ها از طریق بررسی ادبیات و مصاحبه نیمه‌ساختاریافته با خبرگان حسابرسی، حسابداری، مدیریت دولتی و شهری، فناوری اطلاعات، حقوق و کارآفرینی استخراج خواهند شد. سپس دیدگاه خبرگان در قالب متغیرهای زبانی دریافت و به اعداد فازی تبدیل می‌شود. تکنیک دلفی فازی، ابهام موجود در قضاوت‌هایی مانند «اهمیت زیاد» یا «اهمیت متوسط» را کاهش داده و امکان تجمیع نظام‌مند دیدگاه‌های تخصصی را فراهم می‌کند (ایشیکاوا و همکاران[1]، ۱۹۹۳ :۲۴۱-۲۵۳).کاربرد این روش در پژوهش‌های حسابرسی ایران نیز نشان داده است که می‌توان از آن برای شناسایی و اولویت‌بندی پیشران‌های فناورانه و دستیابی به اجماع خبرگان استفاده کرد (عزیزی، ۱۴۰۴: ۱۳۰-۱۲۳).

## مبانی نظری و چارچوب مفهومی پژوهش

حکمرانی الگوریتمیک در این پژوهش به سازوکاری اطلاق می‌شود که در آن قواعد نهادی، داده‌ها، مدل‌های محاسباتی و نظارت انسانی به‌صورت هماهنگ برای تشخیص ریسک، اولویت‌بندی پرونده‌ها، تخصیص منابع نظارتی و پشتیبانی از تصمیم‌های عمومی به کار گرفته می‌شوند. این مفهوم به نظریه سایبرنتیک و تنظیم‌گری بازخوردی متصل است؛ زیرا سامانه الگوریتمی ابتدا استاندارد مطلوب را تعیین می‌کند، سپس داده‌های محیط را پایش می‌کند و در نهایت، انحراف مشاهده‌شده را از طریق هشدار، پیشنهاد اصلاح یا مداخله اجرایی کاهش می‌دهد (یانگ، ۲۰۱۸ :۵۰۷-۵۱۴). در بستر نهادهای شهری، کارآمدی چنین چرخه‌ای تنها به قدرت محاسباتی وابسته نیست و مشروعیت آن به شفافیت معیارها، توضیح‌پذیری خروجی، قابلیت اعتراض، مسئولیت‌پذیری و استمرار کنترل انسانی بستگی دارد (مرادی‌برلیان و تنگستانی، ۱۴۰۲: ۱۷۶-۱۶۹) .

نظارت هوشمند حسابرسی، کاربرد عملی این منطق در قلمرو پاسخ‌گویی مالی است. این سازه بر نظریه حسابرسی مستمر و دیدگاه سیستم‌های اجتماعی ـ فنی استوار است؛ بر این اساس، حسابرسی از یک رسیدگی پسینی و نمونه‌محور به فرایندی پیوسته، داده‌محور و هشداردهنده

[1] Ishikawa et al.

تبدیل می‌شود. در حسابرسی مستمر، داده‌های تراکنشی و کنترلی با قواعد تحلیلی مقایسه می‌شوند تا استثناها و الگوهای غیرعادی در فاصله‌ای کوتاه از زمان وقوع شناسایی شوند (واسارهیلی و همکاران[1]، ۲۰۰۴ :۱-۸). بااین‌حال، فناوری به‌تنهایی عملکرد نظارتی را تضمین نمی‌کند. انطباق‌پذیری سامانه‌ها، کیفیت داده، مهارت تحلیلی حسابرسان، طراحی فرایند و پذیرش سازمانی باید هم‌زمان بهینه شوند؛ زیرا حسابرسی هوشمند ماهیتی اجتماعی ـ فنی دارد (مطلبی کربکندی و همکاران، ۱۴۰۱: ۹۵-۸۳) .

در این مطالعه، حکمرانی الگوریتمیک به‌عنوان مفهوم فراگیر ناظر بر قواعد، مسئولیت‌ها، شفافیت و کنترل تصمیم‌های مبتنی بر داده در نظر گرفته می‌شود. ابعاد زیرساخت داده و فناوری، نظارت هوشمند حسابرسی، الزامات سازمانی و کارآفرینی داده‌محور، حوزه‌های کاربرد و الزامات تحقق این حکمرانی هستند و هم‌سطح با مفهوم فراگیر تلقی نمی‌شوند.

کارآفرینی داده‌محور نیز در این تحقیق صرفاً به استفاده از ابزار دیجیتال برای فروش یا تبلیغات محدود نیست؛ بلکه فرایندی است که طی آن داده معتبر به دانش قابل بهره‌برداری، فرصت اقتصادی و نوآوری تبدیل می‌شود. مبنای نظری این سازه را می‌توان در دیدگاه مبتنی بر دانش و نظریه قابلیت‌های پویا جست‌وجو کرد. طبق منطق قابلیت‌های پویا، سازمان یا کارآفرین باید فرصت را احساس کند، منابع لازم را برای بهره‌برداری از آن بسیج سازد و ترکیب منابع خود را متناسب با تغییر محیط بازآرایی کند. (تیس و همکاران[2]، ۱۹۹۷ :۵۰۹-۵۱۶). داده در هر سه مرحله نقش دارد؛ اما تنها زمانی ارزش‌آفرین می‌شود که زیرساخت فناوری، ذهنیت داده‌محور، سرمایه انسانی و شبکه همکاری در کنار یکدیگر قرار گیرند (گریمالدی و همکاران، ۲۰۲۶ :۱۳۴۱-۱۳۵۲).

هم‌نشینی سه حوزه حکمرانی الگوریتمیک، نظارت هوشمند حسابرسی و کارآفرینی داده‌محور، مبنای سازمان‌دهی چارچوب مفهومی پژوهش است. در این چارچوب، قواعد کیفیت، دسترسی، امنیت، پاسخ‌گویی و نظارت انسانی در کنار قابلیت‌های پایش، هشداردهی و کشف ناهنجاری قرار می‌گیرند و امکان استفاده مسئولانه از داده برای شناسایی مسائل و فرصت‌های شهری را توضیح می‌دهند. این صورت‌بندی، روابط علّی یا اثر مستقیم و غیرمستقیم

[1] Vasarhelyi et al.
[2] Teece et al.

میان سازه‌ها را مفروض نمی‌گیرد؛ بلکه قلمرو عوامل قابل شناسایی و اولویت‌بندی از طریق دلفی فازی را مشخص می‌کند.

حکمرانی الگوریتمیک به مجموعه‌ای از ترتیبات ساختاری، رویه‌ای و ارتباطی گفته می‌شود که از طریق آن، طراحی، استقرار و ارزیابی سامانه‌های مبتنی بر داده و الگوریتم هدایت و کنترل می‌شود. در این پژوهش، حکمرانی الگوریتمیک صرفاً به استفاده سازمان از هوش مصنوعی اشاره ندارد؛ بلکه تعیین می‌کند چه داده‌ای گردآوری شود، چه کسی به آن دسترسی داشته باشد، الگوریتم بر اساس چه معیارهایی تصمیم بگیرد، مسئولیت خطا بر عهده چه شخص یا نهادی باشد و ذی‌نفعان چگونه بتوانند تصمیم‌های سامانه را بررسی یا به آن اعتراض کنند. مرور پژوهش‌های انجام‌شده درباره حکمرانی مسئولانه هوش مصنوعی نشان می‌دهد که تبدیل اصولی مانند شفافیت، انصاف و پاسخ‌گویی به رویه‌های اجرایی، همچنان یکی از نقاط ضعف اصلی سازمان‌هاست. بر همین اساس، حکمرانی مسئولانه هوش مصنوعی در سه دسته سازوکارهای ساختاری، ارتباطی و فرایندی صورت‌بندی شده است (پاپاجیانیدیس و همکاران[1]، ۲۰۲۵ : ۱۰۱۸۸۵).

این مسئله در ایران نیز اهمیت دارد. مرادی‌برلیان و تنگستانی با بررسی حکمرانی الگوریتمی در عرصه عمومی نتیجه گرفتند که نبود نهاد تنظیم‌گر تخصصی، ضعف نظام ارزیابی سامانه‌های هوشمند و ابهام در حدود مسئولیت تصمیم‌های الگوریتمی، از شکاف‌های مهم سیاست‌گذاری کشور به شمار می‌روند (مرادی‌برلیان و تنگستانی، ۱۴۰۴: ۷۵–۶۸). این یافته نشان می‌دهد که استفاده از الگوریتم در نظارت مالی، بدون تعریف قواعد شفاف نهادی و حقوقی، ممکن است سرعت تصمیم‌گیری را افزایش دهد؛ اما لزوماً به افزایش مشروعیت و پاسخ‌گویی منجر نمی‌شود. بنابراین، مؤلفه‌هایی مانند توضیح‌پذیری، نظارت انسانی، حفاظت از اطلاعات، قابلیت اعتراض و تعیین مسئولیت باید بخشی از مدل حکمرانی الگوریتمیک باشند.

## مقایسه مدل‌های حکمرانی داده و انتخاب مبنای نظری پژوهش

برای انتخاب مبنای نظری متناسب با مسئله پژوهش، چهار چارچوب پرکاربرد مقایسه شد. الگوی خاتری و براون حوزه‌های تصمیم‌گیری و محل پاسخ‌گویی را محور حکمرانی داده قرار

[1] Papagiannidis et al.

می‌دهد (خاتری و براون[1]، ۲۰۱۰ :۱۴۸-۱۵۲). الگوی اقتضایی وبر و همکاران بر تناسب نقش‌ها، قلمروهای تصمیم و مسئولیت‌ها با شرایط سازمان تأکید دارد (وبر و همکاران[2]، ۲۰۰۹ :۱:۴-۲۷:۴). چارچوب آبراهام و همکاران سازوکارهای ساختاری، رویه‌ای و ارتباطی حکمرانی داده را در یک الگوی جامع تلفیق می‌کند (آبراهام و همکاران، ۲۰۱۹ :۴۲۴-۴۳۸). چارچوب مدیریت ریسک هوش مصنوعیِ مؤسسه ملی استاندارد و فناوری آمریکا[3] نیز چهار کارکرد حکمرانی، زمینه‌شناسی، سنجش و مدیریت ریسک را برای سامانه‌های هوش مصنوعی پیشنهاد می‌کند (تبسی[4]، ۲۰۲۳ :۱-۴۸).

***جدول ۱***

*مقایسه مدل‌های حکمرانی داده و انتخاب مبنای نظری پژوهش*

| منبع | کانون اصلی | مزیت برای پژوهش حاضر | محدودیت در موضوع حاضر |
|---|---|---|---|
| **خاتری و براون (۲۰۱۰)** | حقوق تصمیم و پاسخ‌گویی در حوزه‌های داده | تفکیک روشن مالکیت، کیفیت، دسترسی و چرخه عمر داده | پوشش محدود ریسک‌های خاص الگوریتم و کارآفرینی |
| **وبر و همکاران (۲۰۰۹)** | طراحی اقتضایی نقش‌ها، تصمیم‌ها و مسئولیت‌ها | انطباق با بافت چندنهادی و محلی شهر کرمانشاه | نیازمند تکمیل با معیارهای شفافیت و ریسک الگوریتمی |
| **آبراهام و همکاران (۲۰۱۹)** | سازوکارهای ساختاری، رویه‌ای و ارتباطی | پوشش جامع فرایند و هماهنگی بین‌سازمانی | فاقد تمرکز مستقیم بر حسابرسی هوشمند |
| **چارچوب مدیریت ریسک هوش مصنوعی (۲۰۲۳)** | حکمرانی، زمینه‌شناسی، سنجش و مدیریت ریسک | پوشش شفافیت، پایش و کنترل ریسک الگوریتم | فاقد تمرکز مستقیم بر خلق فرصت کارآفرینانه |

[1] Khatri & Brown
[2] Weber et al.
[3] National Institute of Standards and Technology (NIST)
[4] Tabassi

بر پایه این مقایسه، رویکرد اقتضایی وبر و همکاران به‌عنوان مناسب‌ترین مبنای سازمان‌دهنده انتخاب شد؛ زیرا ساختار چندنهادی، تفاوت سطح بلوغ داده و تنوع بازیگران شهر کرمانشاه با یک الگوی ثابت سازگار نیست. برای رفع محدودیت این رویکرد، حوزه‌های تصمیم الگوی خاتری و براون، سازوکارهای حکمرانی آبراهام و همکاران و کارکردهای مدیریت ریسک الگوریتمی چارچوب مؤسسه ملی استاندارد و فناوری در مدل تلفیق شدند .بنابراین، مدل نهایی یک چارچوب اقتضایی و تلفیقی است که به‌وسیله دلفی فازی بومی‌سازی و اولویت‌بندی شد.

نظارت هوشمند حسابرسی نظامی است که در آن داده‌های مالی، معاملاتی، قراردادی و عملکردی به‌صورت مستمر گردآوری و تحلیل می‌شوند تا انحراف‌ها، معاملات غیرعادی، ضعف‌های کنترل داخلی و نشانه‌های تقلب در فاصله کوتاهی از زمان وقوع شناسایی شوند. این مفهوم به نظریه حسابرسی مستمر و دیدگاه سیستم‌های اجتماعی ـ فنی متصل است. مطابق این دیدگاه، کارایی حسابرسی تنها از قدرت نرم‌افزار ناشی نمی‌شود؛ بلکه نتیجه تعامل میان فناوری، ساختار سازمانی، مهارت حسابرس، کیفیت داده و قواعد حرفه‌ای است.

مطلبی کربکندی و همکاران در طراحی مدل حسابرسی هوشمند دیوان محاسبات کشور، چهارده عنصر را در سه گروه «پیشران‌ها و الزامات»، «عناصر طراحی و اجرا» و «خروجی‌ها» شناسایی کردند. نتایج آنان نشان داد که تحقق حسابرسی هوشمند بدون اجرای هم‌زمان زیرساخت‌های اطلاعاتی، حمایت مدیریتی، منابع انسانی متخصص و فرایندهای اجرایی یکپارچه امکان‌پذیر نیست (مطلبی کربکندی و همکاران، ۱۴۰۱: ۳۲-۵). محدودیت این مطالعه آن است که تمرکز آن بر ساختار ملی دیوان محاسبات بوده و پیوند حسابرسی هوشمند با حکمرانی الگوریتمی و توسعه فرصت‌های اقتصادی در سطح شهری را بررسی نکرده است .

عزیزی نیز با استفاده از پانل خبرگان، مصاحبه و دلفی فازی، پیشران‌های آینده هوش مصنوعی در حسابرسی ایران را بررسی کرد. نتایج نشان داد توسعه سیستم‌های خبره و سامانه‌های حسابرسی هوشمند از مهم‌ترین نیروهای مؤثر بر آینده حرفه حسابرسی هستند؛ بااین‌حال، وضعیت موجود سامانه‌های حسابرسی ایران مطلوب ارزیابی نشده است (عزیزی، ۱۴۰۴: ۱۱۹- ۱۲۳). این پژوهش اهمیت فناوری را مشخص می‌کند، اما درباره قواعد مالکیت داده، قابلیت توضیح الگوریتم، ثبت مسیر تصمیم و مسئولیت ناشی از خروجی‌های اشتباه، مدل نهادی جامعی ارائه نمی‌دهد.

پیوند نظارت هوشمند حسابرسی و کارآفرینی داده‌محور در این چارچوب مبتنی بر استفاده مجدد مسئولانه از داده است .داده‌های حاصل از حسابرسی و نظارت، در صورت تجمیع، ناشناس‌سازی و رعایت محدودیت‌های دسترسی، می‌توانند برای شناسایی مسائل شهری، طراحی خدمات عمومی یا ایجاد فرصت‌های نوآورانه مورد استفاده قرار گیرند. داده‌های محرمانه حسابرسی مستقیماً در اختیار فعالیت‌های کارآفرینانه قرار نمی‌گیرند و تنها داده‌های مجاز و دارای چارچوب دسترسی می‌توانند نقش ارزش‌آفرین داشته باشند.

پژوهش‌های خارجی نیز همین خلأ را از زاویه دیگری تأیید می‌کنند. لی و گوئل [1] با بررسی دیدگاه ۸۹ حسابرس فناوری اطلاعات نشان دادند که نگهداری گزارش‌های سیستمی، تدوین استانداردهای حسابرسی، استقرار فرایندهای حکمرانی داده و توضیح‌پذیری مدل از مهم‌ترین الزامات حسابرسی فرایندهای مبتنی بر هوش مصنوعی هستند (لی و گوئل، ۲۰۲۵ :۱۰۰۸۴۲). آنان همچنین دریافتند که حسابرسان معمولاً مهارت‌های فنی را بر شایستگی‌های اخلاقی و ارزیابی سطح مدل مقدم می‌دانند. این عدم تعادل می‌تواند کیفیت اطمینان‌بخشی را کاهش دهد؛ زیرا یک سامانه از نظر فنی دقیق ممکن است از نظر عدالت، حریم خصوصی یا پاسخ‌گویی همچنان مسئله‌دار باشد.

مرور نظام‌مند موریکا و همکاران [2] نیز نشان داد که کاربرد هوش مصنوعی در حسابرسی، در کنار افزایش ظرفیت تحلیل داده‌های پیچیده، با خطراتی مانند سوگیری الگوریتمی، فقدان شفافیت، تضعیف پاسخ‌گویی و نقض انصاف همراه است (موریکا و همکاران، ۲۰۲۴). بنابراین، نظارت هوشمند باید علاوه بر کشف انحراف مالی، خود الگوریتم و کیفیت تصمیم‌های تولیدشده را نیز در معرض ارزیابی قرار دهد .

کارآفرینی داده‌محور فرایندی است که طی آن داده‌های خام پس از گردآوری، پالایش، ترکیب و تحلیل، به دانش قابل استفاده برای تشخیص فرصت، طراحی محصول یا خدمت و ایجاد کسب‌وکار تبدیل می‌شوند. این مفهوم بر دیدگاه مبتنی بر دانش و نظریه قابلیت‌های پویا استوار است. اگر داده به‌عنوان یک منبع راهبردی پذیرفته شود، ارزش آن زمانی آشکار می‌شود

[1] Li & Goel
[2] Murikah et al.

که سازمان یا کارآفرین بتواند فرصت را شناسایی کند، منابع موردنیاز را بسیج سازد و مدل کسب‌وکار خود را متناسب با اطلاعات جدید بازآرایی کند.

گریمالدی و همکاران چهار بعد جهت‌گیری کارآفرینانه داده‌محور، زیرساخت فناورانه، مدیریت منابع و قابلیت‌های دانشی را به‌عنوان ارکان کارآفرینی داده‌محور معرفی کردند. آنان استدلال کردند که تبادل و یکپارچه‌سازی داده می‌تواند از مرحله تولید ایده و شناسایی فرصت تا تولید، بازاریابی و توزیع، فرایند ایجاد کسب‌وکار جدید را پشتیبانی کند (گریمالدی و همکاران، ۲۰۲۶ :۱۳۴۱-۱۳۵۲). بااین‌حال، تمرکز این الگو بیشتر بر ظرفیت داخلی بنگاه است و نقش داده‌های نظارتی معتبر و قواعد عمومی دسترسی به داده را کمتر بررسی می‌کند .

این خلأ در شهر کرمانشاه اهمیت بیشتری دارد. شکیبا و همکاران نشان دادند که با ترجیحات و روابط موجود میان بازیگران اکوسیستم کارآفرینی شهر کرمانشاه، ادامه وضعیت موجود محتمل‌تر از اجرای اصلاحات اساسی است (شکیبا و همکاران، ۱۳۹۹: ۱۳۷-۱۲۳). این نتیجه نشان می‌دهد که توسعه کارآفرینی صرفاً به وجود دانشگاه، نهاد حمایتی یا سرمایه‌گذار وابسته نیست؛ بلکه به هماهنگی بازیگران، اعتماد نهادی و دسترسی منصفانه به منابع و اطلاعات نیز نیاز دارد. محدودیت این پژوهش آن است که داده‌های مالی و نظارتی را به‌عنوان منبع تشخیص فرصت‌های کارآفرینانه وارد مدل نکرده است .

## سؤالات پژوهش

### سؤال اصلی:

مدل حکمرانی الگوریتمیک در نظارت هوشمند حسابرسی و توسعه کارآفرینی داده‌محور شهر کرمانشاه از چه ابعاد و مؤلفه‌هایی تشکیل شده است؟

### سؤالات فرعی:

۱. عوامل تشکیل‌دهنده هر یک از پنج بُعد زیرساخت داده و فناوری، حکمرانی الگوریتمیک، نظارت هوشمند حسابرسی، الزامات سازمانی و کارآفرینی داده‌محور کدام‌اند؟

۲. خبرگان چه الزامات و قابلیت‌هایی را برای شکل‌گیری نظارت هوشمند حسابرسی ضروری می‌دانند؟

۳. کدام عوامل مرتبط با بهره‌برداری مسئولانه و کارآفرینانه از داده در مدل پذیرفته می‌شوند؟

٤. اولویت عوامل مدل بر اساس اجماع خبرگان چگونه است؟




**شکل ۱.** چارچوب مفهومی اکتشافی پژوهش

یادداشت: چارچوب شکل ۱ سازمان‌دهی مفهومی پنج بُعد و پانزده عامل را نشان می‌دهد و متضمن آزمون رابطه علّی، اثر مستقیم یا اثر غیرمستقیم میان سازه‌ها نیست.

خبرگانی که در مرحله مصاحبه کیفی مشارکت داشتند، همان اعضای پانل دلفی فازی بودند. بنابراین، مرحله دلفی به‌عنوان فرایند پالایش، اجماع‌سنجی و اولویت‌بندی عوامل استخراج‌شده توسط همان جامعه تخصصی تفسیر می‌شود و اعتبارسنجی مستقل مدل محسوب نمی‌شود.

## روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف کاربردی، از حیث ماهیت و روش توصیفی ـ پیمایشی و از لحاظ نوع‌شناسی در زمره پژوهش‌های آمیخته با رویکرد کیفی و کمّی قرار گرفت. اجرای پژوهش به‌صورت اکتشافی متوالی انجام شد؛ بدین ترتیب که ابتدا ابعاد و عوامل مدل از طریق مصاحبه با خبرگان شناسایی شدند و سپس اهمیت، پذیرش و اولویت عوامل استخراج‌شده با

استفاده از دلفی فازی تعیین شد. دلفی فازی در این پژوهش برای شناسایی، تأیید، اجماع‌سنجی و اولویت‌بندی عوامل به کار رفت و برای آزمون اثر مستقیم، اثر غیرمستقیم یا معناداری روابط میان متغیرها استفاده نشد.

جامعه آماری پژوهش در هر دو بخش کیفی و کمّی شامل خبرگان دانشگاهی و اجرایی شهر کرمانشاه بود. این افراد از میان استادان و پژوهشگران حوزه‌های حسابداری و حسابرسی، مدیریت دولتی و شهری، فناوری اطلاعات، هوش مصنوعی، حکمرانی داده و کارآفرینی انتخاب شدند. نمونه‌گیری به روش هدفمند ملاکی و با استفاده محدود از روش گلوله‌برفی انجام شد. معیارهای ورود به پژوهش شامل داشتن حداقل مدرک کارشناسی ارشد یا صلاحیت حرفه‌ای مرتبط، حداقل پنج سال سابقه تخصصی و برخورداری از تجربه علمی یا اجرایی مرتبط با موضوع پژوهش بود. بر اساس اصل کفایت نظری و استمرار گردآوری داده‌ها تا رسیدن به اشباع، تعداد ۳۰ نفر به‌عنوان اعضای نمونه انتخاب شدند.

در بخش کیفی، ابزار گردآوری داده‌ها مصاحبه نیمه‌ساختاریافته مشتمل بر ۹ سؤال اصلی بود .سؤال‌های مصاحبه بر موضوعاتی مانند زیرساخت داده، شفافیت و توضیح‌پذیری الگوریتم، پاسخ‌گویی، امنیت اطلاعات، نظارت انسانی، قابلیت‌های حسابرسان، پایش هوشمند تراکنش‌ها و تبدیل داده‌های نظارتی به فرصت‌های کارآفرینانه تمرکز داشتند .مصاحبه‌ها به‌صورت حضوری یا برخط و در بازه زمانی ۳۰ تا ۴۵ دقیقه انجام شدند .پس از کسب رضایت مشارکت‌کنندگان، محتوای مصاحبه‌ها ضبط، پیاده‌سازی و با استفاده از نرم‌افزار ATLAS.ti تحلیل شد. تحلیل هم‌زمان با گردآوری داده‌ها پیش رفت؛ پس از هر مصاحبه، متن با مصاحبه‌های پیشین مقایسه، کدگذاری باز و درون‌مایه‌ای انجام و کدهای تازه یا موارد نیازمند پیگیری ثبت شد .سپس کدهای هم‌معنا در مقوله‌های اولیه ادغام و با ادامه مقایسه مداوم، ابعاد و عوامل نهایی استخراج شدند.

اشباع در این پژوهش به‌طور عملیاتی زمانی احراز شد که مرور مصاحبه‌های پایانی، کد یا عامل مستقل جدیدی خارج از طبقات شکل‌گرفته ایجاد نکرد و داده‌های تازه صرفاً نمونه‌ها و توضیح‌های مفاهیم موجود را غنی‌تر کرد .برای پیشگیری از توقف زودهنگام، نمونه‌گیری تا تکمیل ۳۰ مصاحبه و تثبیت این وضعیت ادامه یافت .بنابراین، اشباع یک داوری تحلیلی درباره کفایت داده‌ها بود، نه شاخص آماری مبتنی بر حجم نمونه .

برای تقویت اعتبارپذیری و قابلیت پیگیری بخش کیفی، سؤال‌های مصاحبه و گویه‌های پرسش‌نامه پیش از اجرا از نظر تناسب با هدف، شفافیت عبارت‌ها و پوشش ابعاد موضوع بازبینی شدند .در تحلیل، کدهای اولیه در چند نوبت با متن مصاحبه‌ها تطبیق داده شدند، موارد تکراری حذف، مفاهیم مشابه ادغام و موارد ناسازگار دوباره با داده خام مقابله شدند .نمونه‌ای از زنجیره مضمون ناشناس خبرگان–کد اولیه–عامل نهایی–بُعد نهایی در جدول ۴ گزارش شده است تا مسیر استنباط قابل بازبینی باشد .تنوع تخصصی خبرگان و تطبیق عوامل با ادبیات نیز برای پوشش مفهومی به کار رفت و سپس عوامل کیفی طی دو دور دلفی به‌طور مستقل در معرض داوری خبرگان قرار گرفتند .این مراحل جایگزین شاخص‌های توافق بین کدگذاران نیستند؛ ازاین‌رو، به دلیل نبود داده‌های ثبت‌شده و قابل راستی‌آزمایی، ادعای گزارش نسبت روایی محتوا، کاپای کوهن و بازآزمایی حذف شد.

**جدول ۲**

*تعریف عملیاتی سازه‌های پژوهش*

| تعریف عملیاتی | سازه |
|---|---|
| کیفیت و یکپارچگی داده، امنیت اطلاعات و حریم خصوصی و قابلیت تعامل سامانه‌های اطلاعاتی | زیرساخت داده و فناوری |
| شفافیت و توضیح‌پذیری، پاسخ‌گویی، نظارت انسانی و چارچوب حقوقی تصمیم‌های الگوریتمی | حکمرانی الگوریتمیک |
| پایش مستمر، کشف ناهنجاری، ثبت ردپای حسابرسی و شایستگی دیجیتال حسابرسان | نظارت هوشمند حسابرسی |
| حمایت مدیریتی و نهادی و همکاری بین‌سازمانی در اکوسیستم داده | الزامات سازمانی |
| دسترسی کنترل‌شده به داده‌های عمومی و تبدیل داده معتبر به فرصت اقتصادی | کارآفرینی داده‌محور |

برای بیان میزان موافقت خبرگان از متغیرهای زبانی "خیلی کم، کم، متوسط، زیاد و خیلی زیاد" استفاده شد و هر پاسخ به عدد فازی مثلثی متناظر تبدیل شد .نگاشت کامل مقیاس عبارت بود از: (خیلی کم=(0، 0، 0.25)) ، (کم = (0، 0.25، 0.50)) ، (متوسط=(0.25، 0.50، 0.75)) ، (زیاد= (0.50، 0.75، 1)) ، (خیلی زیاد=(0.75، 1، 1))، جدول ۳ همین نگاشت را به‌صورت خلاصه نشان می‌دهد.

**جدول ۳**

*مقیاس متغیرهای زبانی*

| عدد فازی مثلثی $(l, m, u)$ | متغیر زبانی |
|---|---|
| $(0, 0, 0.25)$ | خیلی کم |
| $(0, 0.25, 0.50)$ | کم |
| $(0.25, 0.50, 0.75)$ | متوسط |
| $(0.50, 0.75, 1)$ | زیاد |
| $(0.75, 1, 1)$ | خیلی زیاد |

برای خبره i و عامل j، عدد فازی مثلثی با سه‌تایی $l_{ij}$، $m_{ij}$، $u_{ij}$ تعریف شد؛ در این نمایش، l، m و u به‌ترتیب کران پایین، مقدار میانی و کران بالای ارزیابی هستند .میانگین فازی گروه برای هر عامل از روابط زیر به دست آمد؛ n= ۳۰ تعداد خبرگان بود.

$$\tilde{A}_j = (\bar{l}_j, \bar{m}_j, \bar{u}_j)$$

$$\bar{l}_j = \frac{1}{n}\sum_{i=1}^{n} l_{ij}\,, \qquad \bar{m}_j = \frac{1}{n}\sum_{i=1}^{n} m_{ij}\,, \qquad \bar{u}_j = \frac{1}{n}\sum_{i=1}^{n} u_{ij}$$

برای تبدیل میانگین فازی هر عامل به امتیاز قطعی در بازه ]۰،۱[، از روش مرکز ثقل استفاده شد:

$$S_j = \frac{\bar{l}_j + \bar{m}_j + \bar{u}_j}{3}$$

دلفی فازی در دو دور اجرا شد .پس از دور نخست، میانگین دیدگاه گروه بدون افشای هویت افراد در اختیار خبرگان قرار گرفت و آنان در دور دوم نظر خود را تثبیت یا اصلاح کردند .ثبات بین دو دور با قدر مطلق اختلاف امتیازهای قطعی سنجیده شد:

$$D_j = \left| S_j^{(2)} - S_j^{(1)} \right|$$

میزان توافق هر عامل نیز از نسبت تعداد پاسخ‌های »زیاد «و »خیلی زیاد «به کل پاسخ‌های معتبر محاسبه شد:

تفسیر اولویت‌ها با احتیاط انجام شده است. از آنجا که هدف دلفی فازی دستیابی به اجماع خبرگان درباره اهمیت عوامل بود، رتبه‌بندی عوامل صرفاً نشان‌دهنده اولویت نسبی در میان عوامل پذیرفته‌شده است و نباید به‌عنوان تفاوت قطعی در اهمیت یا رابطه علّی میان عوامل تفسیر شود.

$$P_j = \frac{N_{\text{high},j} + N_{\text{very high},j}}{n} \times 100$$

پس از پذیرش عوامل، وزن نهایی هر عامل از نرمال‌سازی امتیاز قطعی دور دوم محاسبه شد؛ $m = 15$ تعداد عوامل پذیرفته‌شده بود:

$$W_j = \frac{S_j^{(2)}}{\sum_{k=1}^{m} S_k^{(2)}} \times 100$$

از آنجا که در مطالعات دلفی آستانه واحد و الزام‌آوری وجود ندارد، معیارها پیش از داوری نهایی تثبیت شدند .حد $0.50$ برابر نقطه میانی دامنه نرمال‌شده $[0,1]$ و مرز حداقل پذیرش بود؛ حد ۷۵ درصد با توجه به رواج توافق درصدی و میانه گزارش‌شده برای آستانه اجماع در مرور نظام‌مند دایموند و همکاران (۲۰۱۴) انتخاب شد؛ و $D_j<0.10$ به‌عنوان معیار محافظه‌کارانه ثبات، معادل تغییر کمتر از یک‌دهم دامنه مقیاس، در کنار معیار جداگانه توافق به کار رفت .این شیوه با تأکید فون‌درگراخت (۲۰۱۲) بر تعریف و گزارش شفاف معیارهای اجماع و ثبات سازگار است.

قواعد پذیرش عامل و توقف فرایند به‌صورت زیر اعمال شدند:

$$R_j = 1 \Leftrightarrow S_j^{(2)} \geq 0.50 \ \wedge \ P_j \geq 75\%; \qquad \text{stop} \Leftrightarrow D_j < 0.10 \quad \forall j$$

بنابراین، عامل $j$ فقط زمانی پذیرفته شد که هم امتیاز قطعی دور دوم آن دست‌کم ۰/۵۰ و هم توافق درباره آن دست‌کم ۷۵ درصد بود؛ فرایند نیز زمانی متوقف شد که تغییر امتیاز همه عوامل کمتر از ۰/۱۰ بود .این قواعد صرفاً اجماع، ثبات و اولویت عوامل را نشان می‌دهند و دلالتی بر رابطه علّی، اندازه اثر یا معناداری آماری ندارند.

## یافته‌های پژوهش

یافته‌های پژوهش در دو بخش کیفی و کمّی ارائه شدند. در بخش کیفی، تحلیل مصاحبه‌های نیمه‌ساختاریافته با خبرگان به شناسایی ابعاد و عوامل تشکیل‌دهنده مدل منجر شد. در بخش کمّی، عوامل استخراج‌شده طی دو مرحله دلفی فازی در معرض ارزیابی خبرگان قرار گرفتند و پس از محاسبه میانگین‌های فازی، فازی‌زدایی و بررسی اختلاف دیدگاه‌های دو مرحله، میزان اجماع و اولویت نهایی عوامل مشخص شد. جدول ۳ ویژگی‌های جمعیت‌شناختی

۳۰ نفر از خبرگان مشارکت‌کننده را نشان می‌دهد. از مجموع اعضای نمونه، ۲۱ نفر مرد و ۹ نفر زن بودند. بیشترین فراوانی سابقه کاری به گروه ۱۱ تا ۲۰ سال و بیشترین فراوانی مدرک تحصیلی به دارندگان مدرک دکتری اختصاص داشت. ترکیب تخصصی اعضای نمونه نیز حوزه‌های دانشگاهی و پژوهشی، حسابرسی و مدیریت مالی، فناوری اطلاعات و داده و کارآفرینی و نوآوری را دربر گرفت.

تحلیل ترکیب جامعه خبرگان نشان داد ۳/۶۳ درصد مشارکت‌کنندگان دارای مدرک دکتری و ۷/۳۶ درصد دارای مدرک کارشناسی ارشد بودند .سهم چهار حوزه دانشگاهی و پژوهشی، حسابرسی و مدیریت مالی، فناوری اطلاعات و داده و کارآفرینی و نوآوری نیز بین ۳/۲۳ تا ۷/۲۶ درصد قرار داشت .این توزیع نسبتاً متوازن، امکان بررسی ریسک‌های نوظهور مالی، داده‌ای، الگوریتمی و کارآفرینانه را از چند منظر تخصصی فراهم کرد و وابستگی نتیجه‌گیری به یک گروه حرفه‌ای را کاهش داد .بااین‌حال، چون نمونه هدفمند و محدود به خبرگان شهر کرمانشاه بود، یافته‌ها بیانگر اجماع تخصصی همین جامعه‌اند و نباید به‌عنوان برآورد آماری کل جامعه تعمیم داده شوند.

**جدول ٤**

*ویژگی‌های جمعیت‌شناختی نمونه*

| متغیر | طبقه | فراوانی | درصد |
|---|---|---|---|
| جنسیت | مرد | ۲۱ | ۷۰ |
| | زن | ۹ | ۳۰ |
| سابقه کاری | کمتر از ۱۰ سال | ۶ | ۲۰ |
| | ۱۱ تا ۲۰ سال | ۱۴ | ۷/۴۶ |
| | بیش از ۲۰ سال | ۱۰ | ۳/۳۳ |
| مدرک تحصیلی | کارشناسی ارشد | ۱۱ | ۷/۳۶ |
| | دکتری | ۱۹ | ۳/۶۳ |
| حوزه تخصصی | دانشگاهی و پژوهشی | ۸ | ۷/۲۶ |
| | حسابرسی و مدیریت مالی | ۸ | ۷/۲۶ |
| | فناوری اطلاعات و داده | ۷ | ۳/۲۳ |
| | کارآفرینی و نوآوری | ۷ | ۳/۲۳ |

## یافته‌های بخش کیفی

تحلیل متن مصاحبه‌ها با استفاده از کدگذاری باز و زنده به استخراج ۱۴۶ کد اولیه منجر شد. پس از مرور کدها، حذف موارد تکراری و ادغام مفاهیم مشابه، ۵۳ کد مستقل باقی ماند. کدهای نهایی در قالب ۱۵ عامل و پنج بُعد اصلی شامل حکمرانی الگوریتمیک، زیرساخت داده و فناوری، نظارت هوشمند حسابرسی، الزامات سازمانی و کارآفرینی داده‌محور طبقه‌بندی شدند.

جدول ۵ عوامل شناسایی‌شده و ابعاد مرتبط با آنها را نشان می‌دهد. بیشترین تعداد عوامل به ابعاد حکمرانی الگوریتمیک و نظارت هوشمند حسابرسی اختصاص یافت. عوامل استخراج‌شده، مبنای تدوین پرسش‌نامه دلفی فازی و اجرای مرحله کمّی پژوهش قرار گرفتند.

برای شفاف‌سازی مسیر تبدیل داده‌های کیفی به عوامل نهایی، چند نمونه از خلاصه مضمون اظهارات خبرگان، کدهای اولیه و نحوه انتساب آنها به عامل و بُعد نهایی در جدول تکمیلی زیر ارائه شده است .عبارت‌های ستون نخست، بازگویی غیرلفظی و ناشناس‌شده مضمون مصاحبه‌ها هستند و نقل‌قول مستقیم محسوب نمی‌شوند.

**جدول ۵**

*نمونه مسیر تبدیل مضامین مصاحبه به عوامل و ابعاد نهایی*

| خلاصه مضمون خبرگان | کد اولیه | عامل نهایی | بُعد نهایی |
|---|---|---|---|
| ناسازگاری داده‌های سامانه‌های مالی، اعتبار هشدارهای هوشمند را کاهش می‌دهد. | ناسازگاری منابع داده؛ نیاز به پاک‌سازی و ادغام | کیفیت و یکپارچگی داده | زیرساخت داده و فناوری |
| مدیر و حسابرس باید بتوانند علت پرریسک شناخته‌شدن یک پرونده را بررسی کنند. | لزوم توضیح خروجی؛ قابلیت بررسی معیارها | شفافیت و توضیح‌پذیری الگوریتم | حکمرانی الگوریتمیک |
| اقدام نهایی در پرونده‌های حساس باید پس از بازبینی انسانی انجام شود. | حفظ قضاوت حرفه‌ای؛ کنترل انسانی | نظارت انسانی بر تصمیم‌های الگوریتمی | حکمرانی الگوریتمیک |
| پایش پیوسته تراکنش‌ها باید انحراف را نزدیک به زمان وقوع هشدار دهد. | تحلیل مستمر؛ هشدار به‌موقع | پایش مستمر و هشدار هوشمند | نظارت هوشمند حسابرسی |
| حمایت مدیریت و همکاری میان سازمان‌ها برای تبادل امن داده ضروری است. | حمایت مدیران؛ هماهنگی بین‌سازمانی | حمایت مدیریتی و همکاری بین‌سازمانی | الزامات سازمانی |
| داده عمومی پس از ناشناس‌سازی می‌تواند برای طراحی خدمت جدید استفاده شود. | دسترسی طبقه‌بندی‌شده؛ کشف فرصت | دسترسی کنترل‌شده و تبدیل داده به فرصت | کارآفرینی داده‌محور |

**جدول ٦**

*عوامل استخراج‌شده از بخش کیفی*

| بُعد اصلی | عامل | کد |
|---|---|---|
| زیرساخت داده و فناوری | کیفیت و یکپارچگی داده | A1 |
| حکمرانی الگوریتمیک | شفافیت و توضیح‌پذیری الگوریتم | A2 |
| حکمرانی الگوریتمیک | پاسخ‌گویی و تعیین مسئولیت | A3 |
| حکمرانی الگوریتمیک | نظارت انسانی بر تصمیم‌های الگوریتمی | A4 |
| زیرساخت داده و فناوری | امنیت اطلاعات و حریم خصوصی | A5 |
| زیرساخت داده و فناوری | قابلیت تعامل سامانه‌های اطلاعاتی | A6 |
| نظارت هوشمند حسابرسی | پایش مستمر و هشدار هوشمند | A7 |
| نظارت هوشمند حسابرسی | کشف ناهنجاری و تقلب | A8 |
| نظارت هوشمند حسابرسی | ردپای حسابرسی و قابلیت ردیابی | A9 |
| نظارت هوشمند حسابرسی | شایستگی دیجیتال حسابرسان | A10 |
| الزامات سازمانی | حمایت مدیریتی و نهادی | A11 |
| کارآفرینی داده‌محور | دسترسی کنترل‌شده به داده‌های عمومی | A12 |
| کارآفرینی داده‌محور | تبدیل داده به فرصت کارآفرینانه | A13 |
| الزامات سازمانی | همکاری بین‌سازمانی و اکوسیستم داده | A14 |
| حکمرانی الگوریتمیک | چارچوب حقوقی و تنظیم‌گری الگوریتمی | A15 |

در مرحله کمّی، میزان موافقت خبرگان با هر عامل بر اساس پنج متغیر زبانی از «خیلی کم» تا «خیلی زیاد» سنجیده شد. برای انجام محاسبات، هر متغیر زبانی به یک عدد فازی مثلثی تبدیل شد. مقدار قطعی هر متغیر نیز با استفاده از روش مرکز ثقل به دست آمد.

**جدول ۷**

*متغیرهای زبانی و اعداد فازی مثلثی*

| متغیر زبانی | عدد فازی مثلثی $(l, m, u)$ | مقدار قطعی |
|---|---|---|
| خیلی کم | (۰،۰،۰/۲۵) | ۰/۸۳۰ |
| کم | (۰،۰/۲۵،۰/۵۰) | ۰/۲۵۰ |
| متوسط | (۰/۲۵،۰/۵۰،۰/۷۵) | ۰/۵۰۰ |
| زیاد | (۰/۵۰،۰/۷۵،۱) | ۰/۷۵۰ |
| خیلی زیاد | (۰/۷۵،۱،۱) | ۰/۹۱۷ |

در مرحله نخست، پرسش‌نامه در اختیار ۳۰ نفر از خبرگان قرار گرفت. بررسی فراوانی پاسخ‌ها نشان داد گزینه‌های «زیاد» و «خیلی زیاد» در همه عوامل، بخش عمده پاسخ‌ها را تشکیل دادند. بیشترین فراوانی گزینه «خیلی زیاد» به عوامل امنیت اطلاعات و حریم خصوصی و پایش مستمر و هشدار هوشمند اختصاص یافت. دسترسی کنترل‌شده به داده‌های عمومی و شایستگی دیجیتال حسابرسان نیز نسبت به سایر عوامل، پاسخ‌های بیشتری در طبقات کم و متوسط دریافت کردند.

**جدول ۸**

*نتایج شمارش پاسخ‌های مرحله نخست نظرسنجی*

| عامل | خیلی کم | کم | متوسط | زیاد | خیلی زیاد |
|---|---|---|---|---|---|
| A1 | ۰ | ۱ | ۳ | ۸ | ۱۸ |
| A2 | ۰ | ۱ | ۴ | ۹ | ۱۶ |
| A3 | ۰ | ۲ | ۴ | ۱۰ | ۱۴ |
| A4 | ۰ | ۱ | ۵ | ۱۰ | ۱۴ |
| A5 | ۰ | ۱ | ۳ | ۷ | ۱۹ |
| A6 | ۱ | ۲ | ۵ | ۱۰ | ۱۲ |
| A7 | ۰ | ۱ | ۲ | ۸ | ۱۹ |
| A8 | ۰ | ۱ | ۳ | ۸ | ۱۸ |
| A9 | ۰ | ۲ | ۴ | ۹ | ۱۵ |
| A10 | ۱ | ۲ | ۶ | ۱۰ | ۱۱ |
| A11 | ۰ | ۲ | ۵ | ۱۰ | ۱۳ |
| A12 | ۱ | ۳ | ۶ | ۱۰ | ۱۰ |
| A13 | ۰ | ۲ | ۴ | ۹ | ۱۵ |
| A14 | ۱ | ۲ | ۵ | ۱۱ | ۱۱ |
| A15 | ۰ | ۱ | ۴ | ۹ | ۱۶ |

پس از محاسبه نتایج مرحله نخست، میانگین دیدگاه گروه بدون ذکر نام پاسخ‌دهندگان در اختیار خبرگان قرار گرفت. در مرحله دوم، اعضای پانل نظر خود را تثبیت یا اصلاح کردند. بررسی پاسخ‌ها نشان داد فراوانی گزینه «خیلی زیاد» برای تمام عوامل افزایش یافت و تعداد

پاسخ‌های «خیلی کم» در همه مؤلفه‌ها به صفر رسید .در این مرحله، امنیت اطلاعات و حریم خصوصی بیشترین فراوانی گزینه «خیلی زیاد» را به خود اختصاص داد. پس از آن، کیفیت و یکپارچگی داده و پایش مستمر و هشدار هوشمند قرار گرفتند. عامل دسترسی کنترل‌شده به داده‌های عمومی، با وجود افزایش پاسخ‌های مثبت، کمترین تعداد گزینه «خیلی زیاد» را در میان عوامل داشت.

**جدول ۹**

*نتایج شمارش پاسخ‌های مرحله دوم نظرسنجی*

| عامل | خیلی کم | کم | متوسط | زیاد | خیلی زیاد |
|---|---|---|---|---|---|
| A1 | ۰ | ۰ | ۲ | ۷ | ۲۱ |
| A2 | ۰ | ۰ | ۳ | ۸ | ۱۹ |
| A3 | ۰ | ۱ | ۳ | ۹ | ۱۷ |
| A4 | ۰ | ۱ | ۳ | ۸ | ۱۸ |
| A5 | ۰ | ۰ | ۲ | ۶ | ۲۲ |
| A6 | ۰ | ۱ | ۴ | ۱۰ | ۱۵ |
| A7 | ۰ | ۰ | ۲ | ۷ | ۲۱ |
| A8 | ۰ | ۰ | ۲ | ۸ | ۲۰ |
| A9 | ۰ | ۱ | ۳ | ۸ | ۱۸ |
| A10 | ۰ | ۱ | ۵ | ۱۰ | ۱۴ |
| A11 | ۰ | ۱ | ۴ | ۹ | ۱۶ |
| A12 | ۰ | ۲ | ۵ | ۱۰ | ۱۳ |
| A13 | ۰ | ۱ | ۳ | ۸ | ۱۸ |
| A14 | ۰ | ۱ | ۴ | ۱۰ | ۱۵ |
| A15 | ۰ | ۰ | ۳ | ۸ | ۱۹ |

پس از شمارش پاسخ‌ها، میانگین فازی مثلثی و مقدار فازی‌زدایی‌شده هر عامل در دو مرحله محاسبه شد. امتیاز تمام عوامل در مرحله دوم بیشتر از مرحله نخست بود. در مرحله نخست، امتیاز عوامل بین ۰/۶۸۳ و ۰/۸۲۲ قرار داشت؛ درحالی‌که دامنه امتیازات مرحله دوم بین ۰/۷۴۷ و ۰/۸۵۶ بود. در مرحله دوم، امنیت اطلاعات و حریم خصوصی بالاترین مقدار فازی‌زدایی‌شده

را کسب کرد. کیفیت و یکپارچگی داده و پایش مستمر و هشدار هوشمند در جایگاه بعدی قرار گرفتند. پایین‌ترین مقدار فازی‌زدایی‌شده نیز به دسترسی کنترل‌شده به داده‌های عمومی اختصاص یافت.

**جدول ۱۰**

*میانگین دیدگاه‌های خبرگان حاصل از دو مرحله نظرسنجی*

| کد | میانگین فازی مرحله اول (l، m، u) | فازی‌زدایی اول | میانگین فازی مرحله دوم (l، m، u) | فازی‌زدایی دوم |
|---|---|---|---|---|
| A1 | ۰/۹۵۸ ،۰/۸۵۸ ،۰/۶۰۸ | ۰/۸۰۸ | ۰/۹۸۳ ،۰/۹۰۸ ،۰/۶۵۸ | ۰/۸۵۰ |
| A2 | ۰/۹۵۰ ،۰/۸۳۳ ،۰/۵۸۳ | ۰/۷۸۹ | ۰/۹۷۵ ،۰/۸۸۳ ،۰/۶۳۳ | ۰/۸۳۱ |
| A3 | ۰/۹۳۳ ،۰/۸۰۰ ،۰/۵۵۰ | ۰/۷۶۱ | ۰/۹۵۸ ،۰/۸۵۰ ،۰/۶۰۰ | ۰/۸۰۳ |
| A4 | ۰/۹۴۲ ،۰/۸۰۸ ،۰/۵۵۸ | ۰/۷۶۹ | ۰/۹۵۸ ،۰/۸۵۸ ،۰/۶۰۸ | ۰/۸۰۸ |
| A5 | ۰/۹۵۸ ،۰/۸۶۷ ،۰/۶۱۷ | ۰/۸۱۴ | ۰/۹۸۳ ،۰/۹۱۷ ،۰/۶۶۷ | ۰/۸۵۶ |
| A6 | ۰/۹۰۰ ،۰/۷۵۰ ،۰/۵۰۸ | ۰/۷۱۹ | ۰/۹۵۰ ،۰/۸۲۵ ،۰/۵۷۵ | ۰/۷۸۳ |
| A7 | ۰/۹۶۷ ،۰/۸۷۵ ،۰/۶۲۵ | ۰/۸۲۲ | ۰/۹۸۳ ،۰/۹۰۸ ،۰/۶۵۸ | ۰/۸۵۰ |
| A8 | ۰/۹۵۸ ،۰/۸۵۸ ،۰/۶۰۸ | ۰/۸۰۸ | ۰/۹۸۳ ،۰/۹۰۰ ،۰/۶۵۰ | ۰/۸۴۴ |
| A9 | ۰/۹۳۳ ،۰/۸۰۸ ،۰/۵۵۸ | ۰/۷۶۷ | ۰/۹۵۸ ،۰/۸۵۸ ،۰/۶۰۸ | ۰/۸۰۸ |
| A10 | ۰/۸۹۲ ،۰/۷۳۳ ،۰/۴۹۲ | ۰/۷۰۶ | ۰/۹۴۲ ،۰/۸۰۸ ،۰/۵۵۸ | ۰/۷۶۹ |
| A11 | ۰/۹۲۵ ،۰/۷۸۳ ،۰/۵۳۳ | ۰/۷۴۷ | ۰/۹۵۰ ،۰/۸۳۳ ،۰/۵۸۳ | ۰/۷۸۹ |
| A12 | ۰/۸۷۵ ،۰/۷۰۸ ،۰/۴۶۷ | ۰/۶۸۳ | ۰/۹۲۵ ،۰/۷۸۳ ،۰/۵۳۳ | ۰/۷۴۷ |
| A13 | ۰/۹۳۳ ،۰/۸۰۸ ،۰/۵۵۸ | ۰/۷۶۷ | ۰/۹۵۸ ،۰/۸۵۸ ،۰/۶۰۸ | ۰/۸۰۸ |
| A14 | ۰/۹۰۰ ،۰/۷۴۲ ،۰/۵۰۰ | ۰/۷۱۴ | ۰/۹۵۰ ،۰/۸۲۵ ،۰/۵۷۵ | ۰/۷۸۳ |
| A15 | ۰/۹۵۰ ،۰/۸۳۳ ،۰/۵۸۳ | ۰/۷۸۹ | ۰/۹۷۵ ،۰/۸۸۳ ،۰/۶۳۳ | ۰/۸۳۱ |

برای تعیین ثبات دیدگاه‌ها، اختلاف مقدار فازی‌زدایی‌شده هر عامل در دو مرحله محاسبه شد. نتایج جدول ۹ نشان می‌دهد اختلاف همه عوامل کمتر از آستانه ۱/۰ بود. کمترین اختلاف به عامل پایش مستمر و هشدار هوشمند و بیشترین اختلاف به همکاری بین‌سازمانی و اکوسیستم داده اختصاص داشت. با توجه به قرارگرفتن تمام اختلاف‌ها زیر حد تعیین‌شده، فرایند دلفی پس از مرحله دوم متوقف شد. تمام عوامل نیز امتیازی بیشتر از حد پذیرش ۵/۰ کسب کردند و

درصد پاسخ‌های زیاد و خیلی زیاد آنها بیشتر از ۷۵ درصد بود. بنابراین، هر ۱۵ عامل برای حضور در مدل نهایی حفظ شدند.

**جدول ۱۱**

اختلاف میانگین فازی‌زدایی‌شده مرحله اول و دوم

| عامل | مرحله اول | مرحله دوم | اختلاف |
|---|---|---|---|
| A1 | ۰/۸۰۸ | ۰/۸۵۰ | ۰/۰۴۲ |
| A2 | ۰/۷۸۹ | ۰/۸۳۱ | ۰/۰۴۲ |
| A3 | ۰/۷۶۱ | ۰/۸۰۳ | ۰/۰۴۲ |
| A4 | ۰/۷۶۹ | ۰/۸۰۸ | ۰/۰۳۹ |
| A5 | ۰/۸۱۴ | ۰/۸۵۶ | ۰/۰۴۲ |
| A6 | ۰/۷۱۹ | ۰/۷۸۳ | ۰/۰۶۴ |
| A7 | ۰/۸۲۲ | ۰/۸۵۰ | ۰/۰۲۸ |
| A8 | ۰/۸۰۸ | ۰/۸۴۴ | ۰/۰۳۶ |
| A9 | ۰/۷۶۷ | ۰/۸۰۸ | ۰/۰۴۲ |
| A10 | ۰/۷۰۶ | ۰/۷۶۹ | ۰/۰۶۴ |
| A11 | ۰/۷۴۷ | ۰/۷۸۹ | ۰/۰۴۲ |
| A12 | ۰/۶۸۳ | ۰/۷۴۷ | ۰/۰۶۴ |
| A13 | ۰/۷۶۷ | ۰/۸۰۸ | ۰/۰۴۲ |
| A14 | ۰/۷۱۴ | ۰/۷۸۳ | ۰/۰۶۹ |
| A15 | ۰/۷۸۹ | ۰/۸۳۱ | ۰/۰۴۲ |

برای تعیین وزن نهایی، مقدار فازی‌زدایی‌شده مرحله دوم هر عامل بر مجموع امتیازات تمام عوامل تقسیم شد. نتایج نشان داد امنیت اطلاعات و حریم خصوصی با وزن ۷/۰۴ درصد در رتبه نخست قرار گرفت. کیفیت و یکپارچگی داده و پایش مستمر و هشدار هوشمند، هرکدام با وزن ۶/۹۹ درصد، رتبه دوم را به دست آوردند.

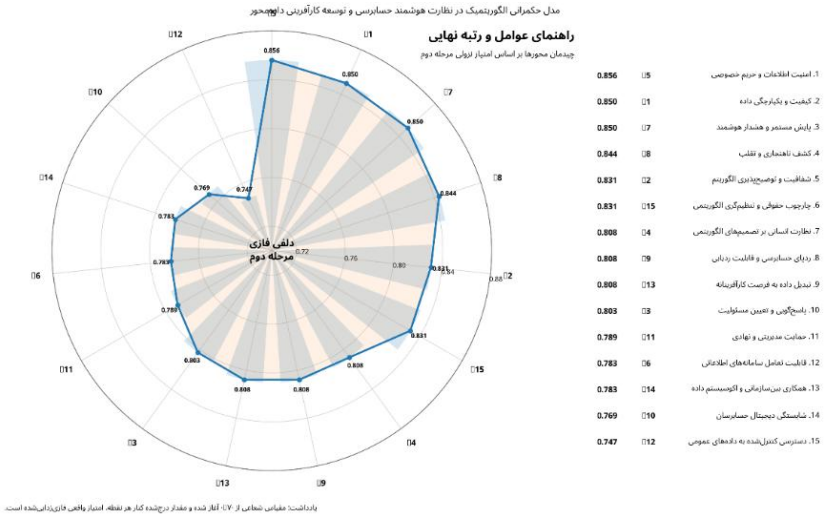
در ادامه، کشف ناهنجاری و تقلب با وزن ۶/۹۴ درصد قرار گرفت. شفافیت و توضیح‌پذیری الگوریتم و چارچوب حقوقی و تنظیم‌گری الگوریتمی نیز وزن یکسان ۶/۸۳ درصد را کسب

کردند. پایین‌ترین وزن متعلق به دسترسی کنترل‌شده به داده‌های عمومی بود. دامنه محدود وزن‌ها نشان داد هر ۱۵ عامل در مدل نهایی سهم داشتند، هرچند ترتیب اولویت آنها یکسان نبود.

**جدول ۱۲**

*وزن نهایی و اولویت عوامل*

| رتبه | کد | عامل | امتیاز نهایی | وزن درصدی |
|---|---|---|---|---|
| ۱ | A5 | امنیت اطلاعات و حریم خصوصی | ۰/۸۵۶ | ۷/۰۴ |
| ۲ | A1 | کیفیت و یکپارچگی داده | ۰/۸۵۰ | ۶/۹۹ |
| ۲ | A7 | پایش مستمر و هشدار هوشمند | ۰/۸۵۰ | ۶/۹۹ |
| ۴ | A8 | کشف ناهنجاری و تقلب | ۰/۸۴۴ | ۶/۹۴ |
| ۵ | A2 | شفافیت و توضیح‌پذیری الگوریتم | ۰/۸۳۱ | ۶/۸۳ |
| ۵ | A15 | چارچوب حقوقی و تنظیم‌گری الگوریتمی | ۰/۸۳۱ | ۶/۸۳ |
| ۷ | A4 | نظارت انسانی بر تصمیم‌های الگوریتمی | ۰/۸۰۸ | ۶/۶۵ |
| ۷ | A9 | ردپای حسابرسی و قابلیت ردیابی | ۰/۸۰۸ | ۶/۶۵ |
| ۷ | A13 | تبدیل داده به فرصت کارآفرینانه | ۰/۸۰۸ | ۶/۶۵ |
| ۱۰ | A3 | پاسخ‌گویی و تعیین مسئولیت | ۰/۸۰۳ | ۶/۶۰ |
| ۱۱ | A11 | حمایت مدیریتی و نهادی | ۰/۷۸۹ | ۶/۴۹ |
| ۱۲ | A6 | قابلیت تعامل سامانه‌های اطلاعاتی | ۰/۷۸۳ | ۶/۴۴ |
| ۱۲ | A14 | همکاری بین‌سازمانی و اکوسیستم داده | ۰/۷۸۳ | ۶/۴۴ |
| ۱۴ | A10 | شایستگی دیجیتال حسابرسان | ۰/۷۶۹ | ۶/۳۳ |
| ۱۵ | A12 | دسترسی کنترل‌شده به داده‌های عمومی | ۰/۷۴۷ | ۶/۱۴ |




**شکل ۲.** وزن نهایی عوامل مدل حکمرانی الگوریتمیک

## بحث و نتیجه‌گیری

پژوهش حاضر با هدف ارائه مدل حکمرانی الگوریتمیک در نظارت هوشمند حسابرسی و توسعه کارآفرینی داده‌محور در شهر کرمانشاه انجام شد .بر پایه اجماع خبرگان، کاربردپذیری مدل پیشنهادی مستلزم توجه هم‌زمان به کیفیت داده، امنیت اطلاعات، شفافیت تصمیم‌های الگوریتمی، نظارت انسانی، توانایی حسابرسان و قابلیت تبدیل داده‌ها به فرصت‌های اقتصادی ارزیابی شد .این نتیجه بازتاب قضاوت خبرگان درباره اهمیت نسبی عوامل است و نباید به‌منزله آزمون اثر یا رابطه علّی میان آنها تفسیر شود .در میان عوامل شناسایی‌شده، امنیت اطلاعات و حریم خصوصی، کیفیت و یکپارچگی داده و پایش مستمر و کشف ناهنجاری در اولویت قرار گرفتند.

در پاسخ به سؤال نخست، پانزده عامل در پنج بُعد زیرساخت داده و فناوری، حکمرانی الگوریتمیک، نظارت هوشمند حسابرسی، الزامات سازمانی و کارآفرینی داده‌محور شناسایی و پذیرفته شدند .در پاسخ به سؤال دوم، اجماع خبرگان نشان داد شفافیت و توضیح‌پذیری الگوریتم، پاسخ‌گویی، نظارت انسانی، چارچوب حقوقی، کیفیت داده، امنیت، پایش مستمر، ثبت ردپای حسابرسی و کشف تقلب از الزامات و قابلیت‌های اصلی نظارت هوشمند هستند .

این نتیجه با پژوهش مرادی‌برلیان و تنگستانی درباره مخاطرات حقوقی تصمیم‌گیری الگوریتمی و با یافته‌های مطلبی کربکندی و همکاران درباره زیرساخت اطلاعاتی، تخصص نیروی انسانی و هماهنگی سامانه‌ها هماهنگ است )مطلبی کربکندی و همکاران، ۱۴۰۱الف؛ ۱۴۰۱ب)

در پاسخ به سؤال سوم، دو عامل دسترسی کنترل‌شده به داده‌های عمومی و تبدیل داده به فرصت کارآفرینانه در بُعد کارآفرینی داده‌محور پذیرفته شدند و همکاری بین‌سازمانی نیز در بُعد الزامات سازمانی قرار گرفت. این یافته‌ها نشان می‌دهند خبرگان، استفاده کارآفرینانه از داده را مشروط به کیفیت، محرمانگی، سطح‌بندی دسترسی و همکاری نهادی می‌دانند. این تفسیر بیانگر اجماع درباره اهمیت عوامل است و اثبات‌کننده اثر مستقیم یا غیرمستقیم نظارت هوشمند بر کارآفرینی نیست.

در پاسخ به سؤال چهارم، امنیت اطلاعات و حریم خصوصی با وزن ۰۴/۷ درصد در رتبه نخست قرار گرفت؛ کیفیت و یکپارچگی داده و پایش مستمر و هشدار هوشمند نیز هرکدام با وزن ۹۹/۶ درصد رتبه دوم را کسب کردند. دسترسی کنترل‌شده به داده‌های عمومی با وزن ۱۴/۶ درصد پایین‌ترین اولویت را داشت. فاصله محدود وزن‌ها نشان داد همه عوامل برای انسجام مدل اهمیت دارند، اما شدت اولویت آنها یکسان نیست. در مجموع، مدل پیشنهادی سه حوزه موضوعی پژوهش را در قالب پنج بُعد هماهنگ و یک چارچوب اقتضایی ـ تلفیقی سازمان‌دهی می‌کند.

تعمیم نتایج به سایر شهرها باید با احتیاط انجام شود؛ زیرا یافته‌ها بر دیدگاه خبرگان شهر کرمانشاه و نمونه‌گیری هدفمند استوار است .همچنین، دلفی فازی در این پژوهش فقط برای شناسایی، تأیید و اولویت‌بندی عوامل به کار رفته است و روابط علّی، اثر مستقیم، اثر غیرمستقیم یا معناداری آماری میان متغیرها را اثبات نمی‌کند .جمع‌بندی محدود پژوهش حاضر آن است که خبرگان، حکمرانی الگوریتمیک را یکی از الزامات مهم طراحی یک نظام نظارتی قابل‌اعتماد، پاسخ‌گو و ارزش‌آفرین ارزیابی کردند .داده‌های این پژوهش اثربخشی واقعی مدل یا رابطه علّی میان مؤلفه‌ها را نشان نمی‌دهند .از دید خبرگان، نبود امنیت، شفافیت و نظارت انسانی با خطر افزایش سرعت تصمیم‌گیری بدون تقویت پاسخ‌گویی همراه است؛ مدل پیشنهادی صرفاً چارچوبی برای آزمون تجربی این انتظار در مطالعات آینده فراهم می‌کند.

## پیشنهادها برای پژوهش‌های آینده

پیشنهاد می‌شود مدل ارائه‌شده در پژوهش‌های آینده با استفاده از مدل‌سازی معادلات ساختاری و در میان نمونه‌ای بزرگ‌تر از حسابرسان، مدیران شهری و کارآفرینان اعتبارسنجی شود .همچنین، اجرای آزمایشی مدل در فرایندهایی مانند قراردادها، مناقصه‌ها و پرداخت‌های شهری می‌تواند امکان سنجش تجربی پیامدهای احتمالی آن بر کشف انحراف، هزینه حسابرسی و شفافیت را فراهم کند .بررسی تطبیقی مدل در شهرهای دیگر و مطالعه نقش متغیرهایی مانند اعتماد نهادی، بلوغ دیجیتال و کیفیت حکمرانی داده نیز پیشنهاد می‌شود.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع


رضایی، بیژن؛ نادری، نادر؛ و سلیمانی، معین. (۱۳۹۹) .راهبردهای توسعه اکوسیستم کارآفرینی در نواحی روستایی شهرستان کرمانشاه .*اقتصاد فضا و توسعه روستایی*، ۹(۳۱)، ۶۷–۹۴.

شکیبا، حجت؛ دل‌انگیزان، سهراب؛ و محمدی‌فر، یوسف. (۱۳۹۹) .مدل‌سازی و تحلیل راهبردی اکوسیستم کارآفرینی فراگیر شهری با رویکرد نظریه بازی‌ها :مورد مطالعه شهر کرمانشاه .*بهبود مدیریت*، ۱۴(۳)، ۱۲۱–۱۴۸https://doi.org/10.22034/jmi.2020.118532 .

عزیزی، فرهاد .(۱۴۰۴) .آینده‌پژوهی کاربرد هوش مصنوعی در حسابرسی :از منظر علم و فناوری اطلاعات .*قضاوت و تصمیم‌گیری در حسابداری و حسابرسی*، ۴(۱۳)، ۱۱۹–۱۳۴ . https://doi.org/10.71960/jdaa.2025.1127884

مرادی‌برلیان، مهدی؛ و تنگستانی، محمدقاسم. (۱۴۰۲) .الگوریتم و حقوق اداری؛ چالش‌ها و راهکارها . *حقوق اداری*، ۱۰(۳۴)، ۱۶۳–۱۹۲https://doi.org/10.61186/qjal.10.34.163 .

مرادی‌برلیان، مهدی؛ و تنگستانی، محمدقاسم. (۱۴۰۴) .نظم عمومی در عصر تحول پلتفرمی :مطالعه تطبیقی سیاست‌گذاری نظم در بستر حکمرانی الگوریتمی .*مطالعات راهبردی*، ۲۸(۳)، ۴۳–۷۹ . https://doi.org/10.22034/ssq.2025.539441.4299

مطلبی کربکندی، مصطفی؛ آذر، عادل؛ خدیور، آمنه؛ و مقبل باعرض، عباس. (۱۴۰۱الف) .طراحی مدل حسابرسی هوشمند در دیوان محاسبات کشور .*پژوهش‌های مدیریت عمومی*، ۱۵(۵۸)، ۵–۳۲ . https://doi.org/10.22111/jmr.2022.43008.5818

مطلبی کربکندی، مصطفی؛ آذر، عادل؛ خدیور، آمنه؛ و مقبل باعرض، عباس. (۱۴۰۱ب). مفهوم‌شناسی حسابرسی هوشمند در سازمان‌های عالی نظارتی با رویکرد روش‌شناسی سیستم‌های نرم :مورد مطالعه دیوان محاسبات کشور .*اندیشه مدیریت راهبردی*، ۱۶(۲)، ۷۹–۱۰۶ . https://doi.org/10.30497/smt.2022.243585.3415

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International *Journal of Information Management*, 49, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, 36(4), 1–27. https://doi.org/10.2308/ajpt-51684

Azizi, F. (2025). Future study of artificial intelligence application in auditing: From the perspective of information science and technology. Judgment and *Decision Making in Accounting and Auditing*, 4(13), 119–134. https://doi.org/10.71960/jdaa.2025.1127884 (in Persian).

Danaher, J., Hogan, M. J., Noone, C., Kennedy, R., Behan, A., De Paor, A., Felzmann, H., Haklay, M., Khoo, S. M., Morison, J., Murphy, M. H., O'Brolcháin, N., Schafer, B., & Shankar, K. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big Data & Society*, 4(2), 1–21. https://doi.org/10.1177/2053951717726554

Diamond, I. R., Grant, R. C., Feldman, B. M., Pencharz, P. B., Ling, S. C., Moore, A. M., & Wales, P. W. (2014). Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology*, 67(4), 401–409. https://doi.org/10.1016/j.jclinepi.2013.12.002

Grimaldi, M., Troisi, O., Papa, A., & de Nuccio, E. (2026). Conceptualizing data-driven entrepreneurship: From knowledge creation to entrepreneurial opportunities and innovation. *The Journal of Technology Transfer*, 51, 1341–1392. https://doi.org/10.1007/s10961-024-10176-5

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine, 292, Article 114523. https://doi.org/10.1016/j.socscimed.2021.114523

Ishikawa, A., Amagasa, M., Shiga, T., Tomizawa, G., Tatsuta, R., & Mieno, H. (1993). The max–min Delphi method and fuzzy Delphi method via fuzzy

integration. *Fuzzy Sets and Systems*, 55(3), 241–253. https://doi.org/10.1016/0165-0114(93)90251-C

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting*, 13(2), 1–20. https://doi.org/10.2308/jeta-10511

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, 53(1), 148–152. https://doi.org/10.1145/1629175.1629210

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, 14(1), 115–122. https://doi.org/10.2308/jeta-51730

Li, Y., & Goel, S. (2025). Bridging IT auditors and AI auditing: Understanding pathways to effective IT audits of AI-driven processes. *Advances in Accounting*, 69, Article 100842. https://doi.org/10.1016/j.adiac.2025.100842

Moradi Berelyan, M., & Tangestani, M. (2023). Algorithm and Administrative Law; Challenges and Solutions. *Administrative Law*, 10(34), 163–192. https://doi.org/10.61186/qjal.10.34.163 (in Persian).

Moradi Berelian, M., & Tangestani, M. G. (2025). Public Order in the Era of Platform Transformation: A Comparative Study of Policy-making in Algorithmic Governance. *Strategic Studies Quarterly*, 28(3), 43–79. https://doi.org/10.22034/ssq.2025.539441.4299 (in Persian).

Motallebi Korbekandi, M., Azar, A., Khadivar, A., & Moghbel, A. (2022). Conceptology of Intelligent Audit in High Supervisory Organizations With the approach of Soft Systems Methodology (Case Study: Supreme Audit Court of Iran). *Strategic Management Thought*, 16(2), 79–106. https://doi.org/10.30497/smt.2022.243585.3415 (in Persian).

Motallebi Korbekandi, M., Azar, A., Khadivar, A., & Moghbel Baarz, A. (2023). Designing the Model of Intelligent Audit in the Supreme Audit Court of Iran with an Interpretive-Structural Modeling Approach. *Public Management Researches*, 15(58), 5–32. https://doi.org/10.22111/jmr.2022.43008.5818 (in Persian).

Murikah, W., Nthenge, J. K., & Musyoka, F. M. (2024). Bias and ethics of AI systems applied in auditing: A systematic review. *Scientific African*, 25, Article e02281. https://doi.org/10.1016/j.sciaf.2024.e02281

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *Journal of Strategic Information Systems*, 34(2), Article 101885. https://doi.org/10.1016/j.jsis.2024.101885

Rezaee, B., Naderi, N., & Soleimani, M. (2020). Strategies for developing the entrepreneurship ecosystem in rural areas of Kermanshah County. *Space Economy and Rural Development*, 9(31), 67–94. https://serd.khu.ac.ir/article_10348.html (in Persian).

Shakiba, H., Delangizan, S., & Mohamadifar, Y. (2020). Modeling and Strategic Analysis of Inclusive Urban Entrepreneurial Ecosystem using Game Theory

Approach (case of study: Kermanshah City). *Management Improvement*, 14(3), 121–148. https://doi.org/10.22034/jmi.2020.118532 (in Persian).

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.AI.100-1

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. https://doi.org/10.1002/%28SICI%291097-0266%28199708%2918%3A7%3C509%3A%3AAID-SMJ882%3E3.0.CO%3B2-Z

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, 1(1), 1–21. https://doi.org/10.2308/jeta.2004.1.1.1

von der Gracht, H. A. (2012). Consensus measurement in Delphi studies: Review and implications for future quality assurance. *Technological Forecasting and Social Change*, 79(8), 1525–1536. https://doi.org/10.1016/j.techfore.2012.04.013

Weber, K., Otto, B., & Österle, H. (2009). One size does not fit all—A contingency approach to data governance. *ACM Journal of Data and Information Quality*, 1(1), Article 4, 1–27. https://doi.org/10.1145/1515693.1515696

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. https://doi.org/10.1111/rego.12158

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Research Paper**

# Redefining Insurance Supervision in the Digital Era: A Conceptual Framework for Smart Supervisory Transformation [1]

**Ameneh Khadivar[2], Leili Niakan[3] and Naser Bafekr Sharak [*4]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 97-126

Received: 2026.02.27
Revised: 2026.04.28
Accepted: 2026.05.18

## Abstract

Technological advancements and the increasing complexity of risks in the insurance industry have challenged the effectiveness of traditional supervisory models. This study aims to conceptualize "smart supervision," distinguish it from related concepts, and identify the key components required for its implementation. It proposes an analytical framework to facilitate the transition of insurance supervisory authorities toward a smart supervisory approach. This research is applied in purpose and descriptive–analytical in nature. The sources include scholarly literature indexed in Web of Science and Scopus, as well as official documents issued by international insurance supervisory authorities, which were collected through a systematic and purposive review. The data were analyzed using qualitative content analysis and a comparative analytical framework. The findings indicate that smart supervision goes beyond the mere digitalization of supervisory tools and requires a paradigm shift from reactive, ex post oversight to data-driven, risk-based, and forward-looking supervision. Five key dimensions were identified: data governance, data-driven decision-making, technological integration, risk-based supervision, and digital reporting. The study demonstrates that implementing smart supervision in the insurance sector necessitates a gradual, data-reliable approach, reforms in institutional and legal frameworks, and enhanced collaboration between supervisory authorities and insurance undertakings. The proposed framework can serve as a foundation for developing a supervisory transformation roadmap, enhancing market transparency, and strengthening policyholder protection.

**Keywords**: Data Governance, RegTech, Risk-Based Supervision, Smart Regulation, Smart Supervision.

**JEL classification:** *G22, G28, G18.*

---

[1] https://doi.org/10.22034/JISTA.2026.578486.1085
[2] Associate Professor, Department of Management, Faculty of Social and Economic Sciences, Alzahra University, Tehran, Iran. Email: a.khadivar@alzahra.ac.ir
[3] Associate Professor, General Insurance Group, Insurance Research Center, Tehran, Iran. Email: niakan@irc.ac.ir
[4] Ph.D. in Applied Mathematics, Insurance Industry Researcher, Dana Insurance Company, Tehran, Iran. (Corresponding Author). Email: naser.bafekr@azaruniv.ac.ir

## 1. INTRODUCTION

The rapid advancement of digital technologies—particularly in domains such as big data, artificial intelligence, and advanced analytical systems—has fundamentally challenged traditional supervisory paradigms in financial markets. Within this context, the insurance sector, as a pivotal component of the financial system, has been especially susceptible to these disruptions. This heightened vulnerability is attributable to a series of factors, including the growing complexity of insurance products, the diversification of risk profiles, the expansion of digital distribution channels, and the exponential increase in data-driven interactions. Collectively, these developments have significantly diminished the effectiveness of conventional supervisory approaches that rely heavily on ex-post controls and static reporting mechanisms (International Association of Insurance Supervisors, 2025; Prenio and Yong, 2021). Consequently, the notion of "smart supervision" has emerged in policy and regulatory discourses as a promising and forward-looking supervisory paradigm.

Smart supervision goes beyond digitization; it requires reconfiguring the supervisory authority's role, redesigning data architectures, and shifting from reactive to proactive, continuous, and anticipatory oversight (World Bank Group, 2020; Norani, 2021). Its realization depends on access to comprehensive, standardized, and reliable datasets. Advanced IT and analytical infrastructures are not merely auxiliary but structural pillars (International Association of Insurance Supervisors, 2025; Monetary Authority of Singapore, 2018).

A key expectation is the move toward risk-based, forward-looking supervision, involving continuous tracking of megatrends, insurers' performance, and risk exposures (European Insurance and Occupational Pensions Authority, 2017; Amini, 2021). This enables authorities to anticipate and prevent crises before they escalate.

Nevertheless, conceptual ambiguities persist. Institutional supervision focuses on formal structures and rule-based practices, while self-regulatory oversight involves market participants

internalizing norms (Niakan, 2024). Smart supervision should complement, not replace, these approaches.

This study pursues three objectives: (1) examining smart supervision initiatives in selected jurisdictions; (2) analyzing Iran's supervisory conditions; and (3) developing a conceptual framework and implementation roadmap for a systematic transition to smart supervision. The novelty lies in offering an integrated, comprehensive approach—a gap in both domestic and international literature (World Bank Group, 2020; International Association of Insurance Supervisors, 2025).

## 2. MATERIALS AND METHODS

This study employs a document-based analytical approach combined with comparative analysis to examine developments, challenges, and policy patterns in the insurance industry—a methodology widely used in insurance and financial policy research. Secondary data were collected from authoritative scientific and official sources, including peer-reviewed academic articles (Web of Science, Scopus, ScienceDirect), official reports from international institutions (OECD, World Bank, IMF, IAIS, Swiss Re Institute), policy documents of insurance supervisory authorities from selected countries, and analytical reports from reinsurance companies and rating agencies. Source quality was ensured using criteria such as institutional credibility, peer review, publication year, and topic relevance.

Data analysis was conducted at two levels. First, qualitative content analysis involved conceptual coding of selected documents to identify key concepts, recurring patterns, policy approaches, and common challenges, enabling detection of semantic relationships and dominant trends. Second, comparative analysis examined policy, institutional, and operational similarities and differences across selected countries or insurance entities, deriving relevant implications for Iran's insurance sector. This dual approach enhances the study's explanatory power and supports the development of a localized smart supervision roadmap.

## 3. RESULTS AND DISCUSSION

The findings confirm that transitioning to smart supervision in insurance is a fundamental policy transformation, not merely a technological upgrade. Traditional reactive, ex post, and static reporting models are inadequate for addressing emerging risks and product complexity (World Bank Group, 2020; International Association of Insurance Supervisors, 2025).

From a policy perspective, smart supervision must be recognized as a financial governance imperative, not a discretionary choice. The supervisory authority's role should shift from "regulation inspector" to "architect of the data and risk ecosystem." Revising regulatory instruments—such as reporting rules, solvency frameworks, and operational guidelines—legitimizes predictive and algorithmic models while enhancing accountability and transparency (Arner et al., 2017; European Insurance and Occupational Pensions Authority, 2022).

A major barrier in Iran's insurance industry is the misalignment between current organizational structures and data-driven governance. The study proposes internal restructuring of the Central Insurance of Iran, including roles such as Chief Data Governance Officer, Data-Driven Risk Analyst, and Algorithmic Supervisor. Shifting from individual judgment to evidence-based decision-making is critical (Zarsky, 2015; Mosadegh & Nazari, 2024). Focusing on a tangible, high-impact process like claims settlement can reduce resistance, build legitimacy, and enable organizational learning.

Technologically, the existing Senhab system functions as a static data registration platform, not a smart supervision infrastructure. Advanced analytics, real-time monitoring, and predictive support are structurally limited. The core conclusion is the need to transform Senhab into an analytical supervisory platform and decision support engine. Key infrastructures include a centralized data lake (a unified, scalable repository for raw, multi-source data), a supervisory rules engine, machine learning models, and real-time dashboards. Unlike traditional databases, a data lake stores data in original form without

predefined structures, enabling advanced analytics and intelligent algorithms (World Bank Group, 2020; Prenio and Yong, 2021).

For insurance companies, smart supervision is not merely a control mechanism but a catalyst for internal improvement. Requirements such as data standardization, real-time reporting, and process transparency drive operational optimization, reduced inefficiencies, and better risk management (Ebrahimi & Aref, 2024). Emphasizing measurable indicators like claims settlement time shifts competition from price to service quality and efficiency, ultimately increasing public trust in the industry (Arasto & Hosseini, 2024).

## 4. CONCLUSION

This study examines the necessity for Iran's insurance supervisory authority to transition from traditional models toward smart, data-driven, and anticipatory supervision. The findings indicate that supervisory transformation is not a discretionary technological choice but an unavoidable response to market complexity, digital insurance expansion, systemic risks, and rising stakeholder expectations.

The research first reviewed theoretical literature and international experiences to articulate a conceptual framework for smart supervision, distinguishing it from related concepts like SupTech and RegTech. No country has yet achieved a fully mature smart supervision model; most have followed gradual, problem-oriented, and data-maturity-driven trajectories. This underscores the need for a localized, realistic roadmap for Iran.

Analyzing the current state of Iran's insurance industry and supervisory authority, the study identified structural, data-related, legal, and human resource gaps. The Senhab system—core insurance supervision infrastructure—suffers from poor data quality, absence of exchange standards, manual processes, and lack of advanced analytical tools. The claims settlement process was selected as the starting point for transformation due to its role in public trust and measurability.

Based on these insights, a practical, phased 24-month roadmap was developed. It begins with foundational data reforms and claims process standardization, progressing toward analytical layers, intelligent alerting, and predictive solvency supervision. The roadmap's strength lies in its holistic integration of technological, legal, organizational, and human capital dimensions, aligned with successful international experiences—particularly South Korea's technical infrastructure model and the UK Financial Conduct Authority's supervisory philosophy.

Overall, successful implementation of smart supervision in Iran's insurance industry depends less on advanced technologies and more on managerial commitment, improved data governance, regulatory reform, and a paradigm shift from reactive to preventive decision-making. The proposed roadmap offers a credible operational framework to guide the Central Insurance of Iran in its digital supervision transformation agenda.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# بازتعریف نظارت بیمه‌ای در عصر دیجیتال: چارچوبی مفهومی برای استقرار نظارت هوشمند[1]

**آمنه خدیور[2]، لیلی نیاکان[3] و ناصر بافکرشارک *[4]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی۱، بهار و تابستان ۱۴۰۵
صص۹۷ - ۱۲۶

تاریخ دریافت: ۱۴۰۴/۱۲/۰۸
تاریخ بازنگری: ۱۴۰۵/۰۲/۰۸
تاریخ پذیرش: ۱۴۰۵/۰۲/۲۸

## چکیده

*تحولات فناورانه و پیچیده‌تر شدن ریسک‌ها در صنعت بیمه، کارایی الگوهای سنتی نظارت را با چالش مواجه کرده است. این پژوهش با هدف تبیین مفهوم «نظارت هوشمند»، تفکیک آن از مفاهیم همجوار و شناسایی مؤلفه‌های کلیدی استقرار آن، چارچوبی تحلیلی برای گذار نهاد ناظر بیمه به رویکردی هوشمند ارائه می‌کند. این مطالعه از نظر هدف کاربردی و از حیث ماهیت توصیفی-تحلیلی است. منابع پژوهش شامل ادبیات علمی نمایه‌شده در پایگاه‌های Web of Science و Scopus و اسناد رسمی نهادهای بین‌المللی نظارت بیمه است که به صورت هدفمند و با مرور نظام‌مند گردآوری شده‌اند. داده‌ها با استفاده از تحلیل محتوای کیفی و چارچوب مقایسه تطبیقی بررسی شدند. یافته‌ها نشان می‌دهد نظارت هوشمند فراتر از دیجیتالی‌سازی ابزارها بوده و مستلزم گذار از نظارت واکنشی به نظارت داده‌محور، ریسک‌محور و آینده‌نگر است. پنج بُعد کلیدی شامل حکمرانی داده، تصمیم‌گیری داده‌محور، یکپارچگی فناوری، نظارت مبتنی بر ریسک و گزارش‌گیری دیجیتال شناسایی شد. پژوهش حاضر نشان می‌دهد که استقرار نظارت هوشمند در صنعت بیمه نیازمند رویکردی تدریجی، مبتنی بر داده‌های قابل اتکا، اصلاح چارچوب‌های نهادی و حقوقی و هم‌افزایی میان نهاد ناظر و شرکت‌های بیمه است. چارچوب پیشنهادی می‌تواند مبنای تدوین نقشه راه تحول نظارت بیمه‌ای و ارتقای شفافیت و حمایت از بیمه‌گذاران قرار گیرد.*

**واژه‌های کلیدی:** *نظارت هوشمند، فناوری‌های نظارتی، نظارت مبتنی بر ریسک، حکمرانی داده، تنظیم‌گری هوشمند.*

**طبقه‌بندی موضوعی:** *G22, G28, G18*

---

[1] https://doi.org/10.22034/JISTA.2026.578486.1085

[2] دانشیار، گروه مدیریت، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران ، ایران. (a.khadivar@alzahra.ac.ir)

[3] دانشیار،گروه پژوهشی عمومی بیمه، پژوهشکده بیمه، تهران، ایران. (niakan@irc.ac.ir)

[4] دکتری ریاضی کاربردی، پژوهشگر صنعت بیمه، شرکت بیمه دانا، تهران، ایران. (نویسنده مسئول). (naser.bafekr@azaruniv.ac.ir)

## مقدمه

تحولات پرشتاب فناوری‌های دیجیتال، به‌ویژه در حوزه‌هایی مانند داده‌های کلان، هوش مصنوعی و سامانه‌های تحلیلی پیشرفته، الگوهای سنتی نظارت در بازارهای مالی را با چالش‌هایی بنیادین روبه‌رو ساخته است. در این میان، صنعت بیمه که به‌عنوان یکی از ارکان اساسی نظام مالی عمل می‌کند، بیش از سایر بخش‌ها در معرض تأثیرات این تحولات قرار دارد. دلیل این امر را می‌توان در عواملی همچون پیچیدگی روزافزون محصولات بیمه‌ای، تنوع ریسک‌ها، گسترش کانال‌های دیجیتال و نیز افزایش چشمگیر تعاملات مبتنی بر داده جستجو کرد؛ عواملی که در ترکیب با یکدیگر، کارآمدی رویکردهای متعارف نظارتی، با تکیه بر کنترل‌های پسینی و گزارش‌های ایستا، را به‌طور محسوسی کاهش داده‌اند (انجمن بین‌المللی ناظران بیمه[1]، ۲۰۲۵؛ پرینو و یونگ[2]، ۲۰۲۱). در پاسخ به این شرایط، مفهوم «نظارت هوشمند» در ادبیات سیاست‌گذاری و تنظیم‌گری مالی به‌عنوان راهکاری نوظهور مطرح گردیده است.

نخستین گام در اجرایی‌سازی نظارت هوشمند در صنعت بیمه، دستیابی به درکی روشن و نظام‌مند از مفهوم «هوشمندی» در بستر وظایف نظارتی است. هوشمندی نظارت صرفاً به معنای دیجیتالی‌سازی فرایندهای موجود یا استفاده از ابزارهای فناورانه به‌صورت پراکنده نیست، بلکه مستلزم بازتعریف نقش نهاد ناظر، بازطراحی جریان‌های داده و حرکت از نظارت واکنشی و گذشته‌نگر به سمت نظارت فعالانه، پیوسته و آینده‌نگر است (گروه بانک جهانی[3]، ۲۰۲۰؛ نورانی، ۱۴۰۰). در این چارچوب، تبیین نظارت هوشمند در صنعت بیمه نیازمند شخصی‌سازی وظایف نظارتی، ابزارها و فناوری‌ها متناسب با ویژگی‌های این صنعت و ساختار نهادی هر کشور است.

چنانچه انتظار از نظارت هوشمند، ارتقای تحلیل‌های داده‌محور، گزارش‌گیری به‌هنگام، پایش مستمر بازار و حتی امکان سفارشی‌سازی محصولات و شرایط بیمه‌ای در نظر گرفته شود، محقق‌شدن آن در گرو دسترسی به داده‌هایی جامع، استاندارد، معتبر و بروز است. در این چارچوب، نهاد ناظر تنها زمانی قادر به ترسیم تصویری دقیق و همه‌جانبه از وضعیت بازار و عملکرد شرکت‌های بیمه خواهد بود که بتواند داده‌های مرتبط را به‌صورت منسجم گردآوری،

[1] International Association of Insurance Supervisors (IAIS)
[2] Prenio and Yong
[3] World Bank Group

یکپارچه‌سازی و تحلیل نماید (انجمن بین‌المللی ناظران بیمه، ۲۰۲۵ ؛ اداره پولی سنگاپور[1]، ۲۰۱۸) . از این منظر، فناوری اطلاعات و ابزارهای تحلیلی پیشرفته، نه صرفاً به‌عنوان عوامل کمکی، بلکه به‌مثابه ساختارهای بنیادین نظارت هوشمند در صنعت بیمه عمل می‌نمایند.

علاوه بر این، از مهم‌ترین انتظارات از نظارت هوشمند، گذار از نظارت صرفاً واکنشی (پسینی) و حرکت به سمت نظارتی پیش‌نگر و مبتنی بر ریسک است. دستیابی به این رویکرد مستلزم رصد مستمر کلان‌روندهای صنعت، پایش پیوسته عملکرد مالی و عملیاتی شرکت‌های بیمه و ارزیابی منظم ریسک‌های درونی و بیرونی آنهاست (سازمان بیمه و بازنشستگی شغلی اروپایی[2]، ۲۰۱۷؛ امینی، ۱۴۰۰). در چنین نظامی، نهاد ناظر با تکیه بر زیرساخت‌های داده‌ای و تحلیلی پیشرفته و در چارچوب مقرراتی پویا، قادر خواهد بود تا تحولات آتی—اعم از ریسک‌های کلان یا ریسک‌های خاص بنگاه‌ها—را پیش‌بینی کرده و اقدامات اصلاحی و پیشگیرانه را پیش از تشدید بحران طراحی و اجرا نماید.

با این حال، ادبیات موضوع با ابهامی مفهومی در تمایز میان «نظارت هوشمند»، «نظارت نهادینه» و «نظارت خودتنظیم» روبه‌روست. نظارت نهادینه بر ایجاد ساختارها، قواعد رسمی و نهادهای کارآمد برای اجرای نظارتی غیرسلیقه‌ای و مبتنی بر قانون تأکید دارد. در مقابل، نظارت خودتنظیم به سازوکارهایی اشاره می‌کند که با درونی‌سازی قواعد و افزایش شفافیت، بدون نیاز به مداخله مستقیم نهاد ناظر، برخی ناکارآمدی‌های بازار را کاهش می‌دهند (بیمه[3]، ۲۰۲۵). نمونه‌هایی مانند «بررسی صلاحیت حرفه‌ای بیمه‌گران» یا «ارزیابی برنامه‌های کسب‌وکار متقاضیان ورود به بازار» از ابزارهای این رویکرد هستند که از طریق پیشگیری، به سلامت بازار کمک می‌کنند (نیاکان و همکاران، ۱۴۰۳). در این بافت، نظارت هوشمند نه جایگزین، بلکه مکمل و تکمیل‌کننده این دو رویکرد تلقی می‌شود.

در این چارچوب، پژوهش حاضر با تمرکز بر صنعت بیمه، سه هدف اصلی را دنبال می‌کند: نخست، بررسی و مقایسه تجارب و اقدامات کشورهای منتخب در زمینه پیاده‌سازی نظارت هوشمند در صنعت بیمه؛ دوم، تحلیل وضعیت موجود فنی، نهادی و قانونی نهاد ناظر بیمه در ایران؛ و سوم، ارائه یک چارچوب مفهومی و مسیر اجرایی اولویت‌بندی‌شده که بتواند به‌عنوان

[1] Monetary Authority of Singapore (MAS)
[2] European Insurance and Occupational Pensions Authority (EIOPA)
[3] Insurance

مبنایی برای گذار نظام‌مند به نظارت هوشمند مورد استفاده قرار گیرد. نوآوری اصلی این پژوهش در عبور از مطالعات پراکنده پیرامون فناوری‌ها یا مقررات خاص، و تمرکز بر طراحی یک نقشه راه جامع و یکپارچه برای تحقق هوشمندی در نظارت است. این رویکرد نظام‌مند، هم در سطح ملی و هم در ادبیات بین‌المللی، کمتر مورد توجه قرار گرفته است (گروه بانک جهانی، ۲۰۲۰؛ انجمن بین‌المللی ناظران بیمه، ۲۰۲۵).

## مبانی نظری و توسعه فرضیه‌ها

گذار از نظارت سنتی به نظارت هوشمند در صنعت بیمه، تحولی صرفاً فناورانه نیست، بلکه ریشه در تغییرات ساختاری بازارهای مالی، پیچیده‌تر شدن ریسک‌ها و تحول در نظریه‌های تنظیم‌گری و حکمرانی دارد. ادبیات معاصر نشان می‌دهد که نظارت کارآمد باید از چارچوب‌های ایستا و واکنشی فاصله گرفته و به سمت رویکردهای ریسک‌محور، داده‌محور و آینده‌نگر حرکت کند (انجمن بین‌المللی ناظران بیمه، ۱۹۹۹؛ سازمان بیمه و بازنشستگی شغلی اروپایی، ۲۰۲۲).

### تحول رویکردهای نظارتی در صنعت بیمه

چارچوب‌های سنتی نظارت بیمه‌ای عمدتاً بر گزارش‌های دوره‌ای، بازرسی‌های مقطعی و مداخلات پسینی استوار بوده‌اند. با این حال، جهانی‌شدن بازارها، تنوع ابزارهای مالی، افزایش ریسک‌های سیستمی و ورود بازیگران فناورمحور، این مدل را با چالش مواجه کرده است (انجمن بین‌المللی ناظران بیمه، ۱۹۹۹). اسناد سیاستی (سازمان بیمه و بازنشستگی شغلی اروپایی، ۲۰۲۲) بر ضرورت نظارت مبتنی بر ریسک، آینده‌نگر و متکی بر تحلیل مستمر داده‌ها تأکید دارند. در این رویکرد، نظارت نه صرفاً ابزار انطباق، بلکه سازوکاری برای تضمین پایداری مالی، حمایت از بیمه‌گذاران و حفظ ثبات بازار تلقی می‌شود.

در نتیجه این تحولات، مفهوم «نظارت هوشمند» به‌عنوان پاسخی نهادی به محدودیت‌های نظارت سنتی شکل گرفته است (مصدق و نظری، ۱۴۰۳).

### تبیین مفهوم نظارت هوشمند در صنعت بیمه

مطالعات پژوهشی، نظارت هوشمند را پاسخی به محدودیت‌های نظارت سنتی و حتی نظارت صرفاً دیجیتال می‌دانند. در این ادبیات، نظارت هوشمند به‌عنوان رویکردی تعریف می‌شود که با بهره‌گیری از دانش، داده و فناوری‌های نوین، نهاد ناظر را از وضعیت واکنشی به کنش‌گر فعال و آینده‌نگر تبدیل می‌کند (مصدق و نظری، ۱۴۰۳).

برخی پژوهش‌ها، نظارت هوشمند را در چارچوب نظریه سیستم‌های هوشمند تبیین کرده‌اند؛ سیستمی که قادر به جمع‌آوری و تحلیل داده‌های محیطی، یادگیری، انطباق با شرایط عدم قطعیت و اصلاح رفتار خود در راستای اهداف نظارتی است (امینی، ۱۴۰۰). در این معنا، هوشمندی نظارت نه صرفاً در ابزارها، بلکه در منطق تصمیم‌گیری و واکنش به تحولات متجلی می‌شود.

در سطح کاربردی، نظارت هوشمند اغلب با استفاده از فناوری‌هایی نظیر هوش مصنوعی، یادگیری ماشین، اینترنت اشیا و تحلیل کلان‌داده‌ها تعریف می‌شود که امکان پایش سریع‌تر، دقیق‌تر و پیش‌نگرانه‌تر فعالیت شرکت‌های بیمه را فراهم می‌کنند (ابراهیمی و عارف، ۱۴۰۳). با تلفیق این دیدگاه‌ها، پژوهش حاضر نظارت هوشمند را مفهومی چندبعدی می‌داند که شامل حکمرانی داده، تصمیم‌گیری مبتنی بر داده، یکپارچگی فناوری، نظارت ریسک‌محور و گزارش‌گیری دیجیتال است (بیمه، ۲۰۲۵).

### تمایز مفهومی و تحلیل شکاف پژوهش

#### *نظارت هوشمند، نظارت نهادینه و نظارت خودتنظیم*

برخی مطالعات مرز میان نظارت هوشمند، نظارت نهادینه و نظارت خودتنظیم را سیال می‌دانند (بیمه، ۲۰۲۵). نظارت نهادینه بر استقرار قواعد، استانداردها و نهادهای پایدار تأکید دارد تا نظارت از وابستگی به افراد رها شده و به فرآیندی ساختاریافته تبدیل شود. در مقابل، نظارت خودتنظیم به درونی‌سازی قواعد نظارتی در میان بازیگران بازار اشاره دارد و می‌کوشد بخشی از نارسایی‌های بازار را از طریق سازوکارهای داوطلبانه اصلاح کند. نظارت هوشمند می‌تواند به‌عنوان پیونددهنده این دو رویکرد تلقی شود؛ چراکه با فراهم‌سازی زیرساخت‌های داده‌ای و تحلیلی، هم نهادینه‌سازی نظارت را تسهیل می‌کند و هم بستر لازم برای تقویت خودتنظیمی در صنعت بیمه را فراهم می‌آورد.

### تمایز نظارت هوشمند و نظارت دیجیتال

ادبیات تخصصی میان نظارت دیجیتال و نظارت هوشمند تمایز قائل می‌شود. نظارت دیجیتال به استفاده از ابزارهای الکترونیکی نظیر گزارش‌دهی برخط، داشبوردها و سامانه‌های اطلاعاتی اشاره دارد، در حالی که منطق تصمیم‌گیری و فرآیندهای نظارتی ممکن است همچنان سنتی باقی بمانند (سازمان بیمه و بازنشستگی شغلی اروپایی، ۲۰۲۱ و ۲۰۲۲). در مقابل، نظارت هوشمند رویکردی داده‌محور و تحلیلی است که با استفاده از فناوری‌هایی نظیر هوش مصنوعی، یادگیری ماشین و پردازش بهنگام داده‌ها، امکان اقدام پیش‌دستانه، دقیق و مبتنی بر ریسک را فراهم می‌سازد (جرجوسولی و اوکونجو[1]، ۲۰۲۲).

### تمایز با فناوری‌های نظارتی، قانون‌گذار و بیمه

مطالعات اخیر تأکید دارند که نظارت هوشمند یک رویکرد راهبردی است، در حالی که فناوری‌های نظارتی مجموعه ابزارهای فناورانه‌ای هستند که نهاد ناظر برای تحقق این رویکرد به کار می‌گیرد (پرینو و همکاران[2]، ۲۰۲۴). در مقابل، فناوری‌های قانون‌گذار عمدتاً در سطح شرکت‌های بیمه و با هدف انطباق با مقررات به کار می‌روند (چارونونگ[3] و همکاران، ۲۰۲۴). از سوی دیگر، فناوری بیمه به تحول مدل‌های کسب‌وکار بیمه از طریق فناوری‌های نوین اشاره دارد و حوزه اثرگذاری آن عمدتاً تعامل شرکت‌های بیمه با مشتریان و نوآوری محصول است (کوسما و ریمو[4]، ۲۰۲۴؛ انجمن ملی ناظران بیمه[5]، ۲۰۲۴). بنابراین، اگرچه توسعه فناوری بیمه پیامدهایی برای نظارت دارد، اما در قلمرو مستقیم نهاد ناظر قرار نمی‌گیرد (هولند و کاوری[6]، ۲۰۲۵).

ابهام در این تمایزات مفهومی یکی از شکاف‌های اصلی ادبیات است که پژوهش حاضر در پی رفع آن است.

---

[1] Georgosouli and Okonjo
[2] Prenio et al.
[3] Charoenwong et al.
[4] Cosma and Rimo
[5] National Association of Insurance Commissioners (NAIC)
[6] Holland and Kavuri

## چالش‌ها، محدودیت‌ها و شکاف پژوهش

مطالعات پیشین چالش‌های متعددی را برای پیاده‌سازی نظارت هوشمند شناسایی کرده‌اند؛ از جمله محدودیت در کیفیت داده‌ها، کمبود منابع انسانی متخصص، ریسک اتکای بیش از حد به سیستم‌های خودکار، مسائل پذیرش سازمانی و چالش‌های شهرتی ناشی از خطای الگوریتم‌ها. هم‌زمان، هوشمند شدن شرکت‌های بیمه و ورود بازیگران غیربیمه‌ای، چالش‌هایی نظیر آربیتراژ تنظیم‌گری، شکاف مهارتی نهاد ناظر، پیچیدگی نظارت بر الگوریتم‌ها و تعادل میان نوآوری و حمایت از مصرف‌کننده را برجسته کرده است (انجمن بین‌المللی ناظران بیمه، ۲۰۱۸؛ عابد و قنبروند، ۱۴۰۲).

با وجود گسترش ادبیات در حوزه SupTech، RegTech و InsurTech، مرور نظام‌مند منابع نشان می‌دهد که:

۱) اغلب مطالعات به‌جای ارائه چارچوب مفهومی یکپارچه، بر ابزارها یا فناوری‌های منفرد تمرکز دارند.

۲) مرز مفهومی میان نظارت هوشمند، دیجیتال و نهادی در بسیاری از پژوهش‌ها شفاف نشده است.

۳) پیوند میان کلان‌روندهای هوشمندسازی صنعت بیمه و الزامات تحول در منطق نظارت، به‌طور نظام‌مند تبیین نشده است.

۴) در بستر کشورهای در حال توسعه، به‌ویژه صنعت بیمه ایران، پژوهش‌هایی که نظارت هوشمند را به‌عنوان یک رویکرد حکمرانی داده‌محور و ریسک‌محور تحلیل کنند، بسیار محدودند.

این شکاف‌ها ضرورت ارائه یک چارچوب مفهومی منسجم برای نظارت هوشمند در صنعت بیمه را برجسته می‌سازد؛ چارچوبی که هم تمایزات نظری را روشن کند و هم قابلیت کاربرد در سیاست‌گذاری و تنظیم‌گری را داشته باشد.

## مبانی نظری

### نظریه نمایندگی و نظارت هوشمند

نظریه نمایندگی یکی از بنیادی‌ترین چارچوب‌های نظری برای تحلیل نظارت در صنعت بیمه است. این نظریه بر روابط میان کارفرمایان (سهامداران و بیمه‌گذاران) و کارگزاران (مدیران

شرکت‌های بیمه) تمرکز دارد و نشان می‌دهد که عدم تقارن اطلاعاتی و تضاد منافع می‌تواند به رفتارهای فرصت‌طلبانه، کژمنشی و کاهش رفاه ذی‌نفعان منجر شود (ایسانهارت[1]، ۱۹۸۹). در صنعت بیمه، این عدم تقارن به دلیل پیچیدگی محصولات، ارزیابی ریسک، ذخایر فنی و تصمیمات سرمایه‌گذاری تشدید می‌شود. نظارت هوشمند با بهره‌گیری از داده‌های بلادرنگ، تحلیل‌های پیشرفته و ابزارهای خودکار، امکان کاهش شکاف اطلاعاتی میان نهاد ناظر و شرکت‌های بیمه را فراهم می‌کند و از این طریق هزینه‌های نمایندگی را کاهش می‌دهد. شفافیت داده‌محور، پایش مستمر و ارزیابی الگوریتمی عملکرد شرکت‌ها، به نهاد ناظر اجازه می‌دهد رفتار مدیران را نه‌تنها پس از وقوع، بلکه در حین شکل‌گیری تصمیمات رصد کند (ابراهیمی و عارف، ۱۴۰۳).

### نظریه ذی‌نفعان و توازن منافع

برخلاف رویکرد صرفاً سهامدارمحور، نظریه ذی‌نفعان بر ضرورت توجه به منافع تمامی گروه‌های ذی‌نفع، از جمله بیمه‌گذاران، کارکنان، نهاد ناظر و جامعه، تأکید می‌کند (فریمن[2] و همکاران، ۲۰۱۰). در صنعت بیمه، تصمیمات مدیریتی می‌توانند پیامدهای گسترده‌ای بر ثبات مالی، عدالت توزیعی و اعتماد عمومی داشته باشند. نظارت هوشمند با فراهم‌آوردن بسترهای شفافیت، گزارش‌دهی به‌هنگام و تحلیل رفتاری بازار، امکان ایجاد توازن میان منافع متعارض ذی‌نفعان را افزایش می‌دهد. این رویکرد، نظارت را از تمرکز صرف بر شاخص‌هایی مانند کفایت سرمایه یا سودآوری کوتاه‌مدت فراتر برده و آن را به ابزاری برای تضمین پایداری بلندمدت و حمایت از حقوق بیمه‌گذاران تبدیل می‌سازد (ابراهیمی و عارف، ۱۴۰۳).

### نظریه سیستم‌های اطلاعاتی

نظریه سیستم‌های اطلاعاتی چارچوبی برای درک نقش فناوری اطلاعات در بهبود عملکرد، شفافیت و اثربخشی سازمان‌ها ارائه می‌دهد. مدل موفقیت سیستم‌های اطلاعاتی دِلُن و مک‌لین نشان می‌دهد که کیفیت داده، کیفیت سیستم و کیفیت خدمات، مستقیماً بر رضایت کاربران و پیامدهای سازمانی اثرگذارند (دیلون و مکلین[3]، ۲۰۰۳).

---

[1] Eisenhardt
[2] Freeman et al.
[3] DeLone and McLean

### نظریه مدیریت ریسک سازمانی

نظریه مدیریت ریسک سازمانی بر ضرورت شناسایی، ارزیابی و مدیریت یکپارچه ریسک‌ها در سطح کل سازمان تأکید دارد. در صنعت بیمه، این رویکرد به دلیل ماهیت ریسک‌محور فعالیت‌ها اهمیت مضاعفی دارد. نظارت هوشمند با فراهم کردن داده‌های دقیق و بلادرنگ، امکان پایش ریسک‌های بیمه‌ای، مالی، عملیاتی و فناوری را به‌صورت هم‌زمان تقویت می‌کند(کمیته سازمان‌های حامی کمیسیون ترودی[1]، ۲۰۱۷).

### نظریه پذیرش فناوری

یکی از چالش‌های کلیدی در پیاده‌سازی نظارت هوشمند، پذیرش ابزارهای فناورانه جدید توسط کارکنان نهاد ناظر است. نظریه پذیرش فناوری بیان می‌کند که «سودمندی برداشت‌شده» و «سهولت استفاده برداشت‌شده» دو عامل تعیین‌کننده در پذیرش یا رد سیستم‌های جدید هستند (دیویس[2]، ۱۹۸۹). کاربرد این نظریه در نظارت هوشمند نشان می‌دهد که موفقیت ابزارهای فناوری نظارتی تنها به قابلیت‌های فنی آن‌ها وابسته نیست، بلکه به میزان تطابق آن‌ها با فرهنگ سازمانی، مهارت کاربران و طراحی کاربرمحور نیز بستگی دارد.

### نظریه نظارت ریسک‌محور

نظارت ریسک‌محور یکی از ارکان نظری نظارت هوشمند است که تمرکز آن بر نتایج، ریسک‌ها و پیامدهای بالقوه به‌جای رعایت صِرف قواعد شکلی است (سازمان بیمه و بازنشستگی شغلی اروپایی، ۲۰۲۲). این رویکرد با اولویت‌بخشی به موسساتی که بیشترین ریسک را برای اهداف نظارتی ایجاد می‌کنند، منابع نظارتی را به‌صورت کارآمد تخصیص می‌دهد. در ادامه این منطق، نظریه نظارت تلفیقی امکان ارزیابی ریسک در سطح گروه‌های مالی را فراهم می‌سازد و از نادیده‌گرفتن ریسک‌های درون‌گروهی و خارج از ترازنامه جلوگیری می‌کند (سازمان تنظیم مقررات خدمات مالی[3]، ۲۰۱۴).

---

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO)
[2] Dsvis
[3] Financial Services Regulatory Authority

**نظریه‌های اقتصادی**

در سطح اقتصاد و حکمرانی، نظریه هزینه مبادله نشان می‌دهد که فناوری‌های دیجیتال می‌توانند هزینه‌های نظارت و اطلاعات نامتقارن را کاهش دهند (بائومول[1]، ۱۹۸۶). در حالی که اقتصاد اطلاعات نقش هوش مصنوعی را در کاهش کژگزینی و کژمنشی برجسته می‌سازد (استیگلیتز[2]، ۲۰۰۰). نظریه رگولاتوری هوشمند نیز بر طراحی نظام‌های تطبیقی و ترکیب ابزارهای سنتی و دیجیتال تأکید دارد (گونینقام و گربوسکی[3]، ۱۹۹۸).

از منظر عملیاتی، چارچوب‌هایی نظیر کمیته سازمان‌های حامی کمیسیون ترودی ( ۲۰۱۳ و ۲۰۱۷)، RegTech (آرنر و همکاران[4]، ۲۰۱۷) و معماری‌های داده‌محور نظیر Lambda Architecture، بنیان‌های فنی تحقق نظارت بلادرنگ و پیش‌بینانه را فراهم می‌کنند.

**جمع‌بندی**

مجموعه نظریه‌های مرورشده نشان می‌دهد که نظارت هوشمند در صنعت بیمه نه یک مفهوم فناورانه منفرد، بلکه یک پارادایم چندبعدی است که در تقاطع اقتصاد اطلاعات، مدیریت ریسک، حکمرانی داده‌محور و فرهنگ نظارتی آینده‌نگر شکل می‌گیرد. این بنیان نظری، مبنای تحلیل تجربی و طراحی چارچوب پیشنهادی پژوهش در بخش‌های بعدی مقاله را فراهم می‌سازد.

## روش‌شناسی پژوهش

### نوع، روش گردآوری، تحلیل و پایایی رویکرد پژوهش

این پژوهش از نظر هدف، کاربردی–سیاستی و از نظر ماهیت، توصیفی–تحلیلی است. رویکرد اصلی پژوهش، تحلیل اسنادی همراه با تحلیل تطبیقی بوده و تمرکز آن بر بررسی نظام‌مند تحولات، چالش‌ها و الگوهای سیاستی در حوزه مورد مطالعه صنعت بیمه است. این رویکرد به‌طور گسترده در مطالعات سیاست‌گذاری بیمه و مالی مورد استفاده قرار می‌گیرد.

[1] Baumol
[2] Stiglitz
[3] Gunningham and Grabosky
[4] Arner et al.

## روش گردآوری داده‌ها

داده‌های پژوهش به‌صورت ثانویه و از طریق منابع علمی و رسمی معتبر گردآوری شده‌اند. این منابع شامل:

- مقالات علمی منتشرشده در پایگاه‌های Web of Science، Scopus و ScienceDirect
- گزارش‌های رسمی نهادهای بین‌المللی بیمه و مالی نظیر OECD، World Bank، IMF، IAIS، Swiss Re Institute
- اسناد سیاستی و نظارتی نهادهای ناظر بیمه در کشورهای منتخب
- گزارش‌های تحلیلی شرکت‌های بیمه اتکایی و مؤسسات رتبه‌بندی

برای اطمینان از کیفیت منابع، معیارهایی مانند اعتبار نهادی، داوری علمی، سال انتشار و ارتباط مستقیم با موضوع پژوهش در نظر گرفته شده است.

## روش نمونه‌گیری منابع

نمونه‌گیری منابع به‌صورت هدفمند انجام شده است؛ به این معنا که تنها منابعی انتخاب شده‌اند که:

۱) مستقیماً به موضوع پژوهش مرتبط باشند؛

۲) دارای اعتبار علمی یا نهادی شناخته‌شده باشند؛

۳) حاوی شواهد تحلیلی یا تجربی قابل اتکا برای استنتاج سیاستی باشند.

این روش در مطالعات مروری نظام‌مند و سیاست‌محور، روشی پذیرفته‌شده محسوب می‌شود.

## روش تحلیل داده‌ها

تحلیل داده‌ها در دو سطح انجام شده است:

❖ تحلیل محتوای کیفی

در این مرحله، اسناد و متون منتخب با استفاده از کدگذاری مفهومی تحلیل شده‌اند. مفاهیم کلیدی، الگوهای تکرارشونده، رویکردهای سیاستی و چالش‌های مشترک استخراج و طبقه‌بندی شده‌اند. این روش امکان شناسایی روابط معنایی و روندهای غالب را فراهم می‌کند.

❖ تحلیل تطبیقی

به‌منظور افزایش قدرت تبیینی پژوهش، یافته‌ها در قالب یک چارچوب تطبیقی بین‌المللی تحلیل شده‌اند. در این بخش، شباهت‌ها و تفاوت‌های سیاستی، نهادی و عملیاتی کشورهای منتخب یا نهادهای بیمه‌ای با یکدیگر مقایسه شده و دلالت‌های قابل استفاده برای صنعت بیمه ایران استخراج شده است.

برای افزایش روایی یافته‌ها، از تنوع منابع شامل مقالات علمی، گزارش‌های رسمی و اسناد سیاستی استفاده شده است. همچنین، تلاش شده است تا تحلیل‌ها بر مبنای منابع به‌روز و معتبر انجام گیرد. پایایی پژوهش نیز از طریق شفافیت مراحل گردآوری و تحلیل داده‌ها و قابلیت بازبینی مسیر استدلال‌ها تضمین شده است. همچنین از جمله محدودیت‌های این پژوهش می‌توان به اتکای آن بر داده‌های ثانویه، تفاوت‌های نهادی و ساختاری بین کشورها، و محدودیت دسترسی به برخی داده‌های محرمانه صنعت بیمه اشاره کرد. با این حال، استفاده از منابع متنوع و تحلیل تطبیقی، تا حد زیادی این محدودیت‌ها را کاهش داده است.

## چارچوب مفهومی پیشنهادی

با توجه به پیچیدگی فزاینده صنعت بیمه، گسترش فناوری‌های داده‌محور، و حرکت نهادهای ناظر از نظارت پسینی به نظارت پیش‌نگر و هوشمند، نیاز به یک چارچوب مفهومی جامع که بتواند ابعاد نهادی، فناورانه، ریسک‌محور و حکمرانی را به‌صورت یکپارچه پوشش دهد، بیش از پیش احساس می‌شود. بررسی الگوهای موجود نشان می‌دهد که هرچند مدل‌های پیشین به ابعاد مهمی از نظارت هوشمند پرداخته‌اند، اما اغلب یا تمرکز بخشی دارند (مانند تمرکز بر مشتری، فناوری یا اعتماد عمومی) یا فاقد انسجام سیستمی میان سطوح خرد، میانی و کلان نظارتی هستند (مصدق و نظری، ۱۴۰۳؛ ارسطو و حسینی، ۱۴۰۳). بر این اساس، چارچوب مفهومی پیشنهادی این مقاله با هدف تلفیق رویکرد ریسک‌محور، حکمرانی داده‌محور و فناوری‌های نظارتی (SupTech/RegTech) طراحی شده و تلاش دارد شکاف میان نظریه‌های نظارتی، الزامات نهادی و قابلیت‌های فناورانه را در قالب یک ساختار منسجم پر کند.

### مبانی تلفیقی چارچوب پیشنهادی

چارچوب مفهومی پیشنهادی بر چهار دسته مبنای نظری و تجربی استوار است:

۱) الگوهای بومی نظارت هوشمند که بر زمینه‌های نهادی، فرهنگی و ساختاری صنعت بیمه ایران تأکید دارند (مصدق و نظری، ۱۴۰۳؛ رئیسی و فلاح‌نژاد، ۱۴۰۳).
۲) چارچوب‌های بین‌المللی نظارت مبتنی بر ریسک و فناوری، به‌ویژه راهنماهای IAIS، بانک جهانی و نهادهای ناظر پیشرو (گروه بانک جهانی، ۲۰۲۰؛ انجمن بین‌المللی ناظران بیمه، ۲۰۲۵).
۳) نظریه‌های حکمرانی، مدیریت ریسک و فناوری اطلاعات که در بخش مبانی نظری مقاله تشریح شدند، از جمله نظارت ریسک‌محور، COSO ERM و RegTech (آرنر و همکاران، ۲۰۱۷؛ کمیته سازمان‌های حامی کمیسیون ترودی، ۲۰۱۷).
۴) الزامات نوظهور هوش مصنوعی شامل شفافیت، توضیح‌پذیری، عدالت الگوریتمی و پاسخگویی نهادی (زرسکی[1]، ۲۰۱۵؛ پرینو و یونگ، ۲۰۲۱).

## ساختار کلی چارچوب مفهومی پیشنهادی

چارچوب مفهومی پیشنهادی نظارت هوشمند در صنعت بیمه از پنج لایه تعاملی تشکیل شده است که به‌صورت پویا و چرخه‌ای با یکدیگر در ارتباط‌اند:

❖ لایه اول: بستر زمینه‌ای و نهادی

این لایه شامل شرایط کلان سیاسی، اقتصادی، حقوقی و نهادی است که خارج از کنترل مستقیم نهاد ناظر قرار دارند اما جهت‌گیری نظارت هوشمند را به‌طور معناداری شکل می‌دهند. سیاست‌های بیمه‌ای، ساختار بازار بیمه، سطح بلوغ دیجیتال کشور و چارچوب‌های قانونی مرتبط با داده و حریم خصوصی در این لایه قرار می‌گیرند (گروه بانک جهانی، ۲۰۲۰؛ رئیسی و فلاح‌نژاد، ۱۴۰۳).

❖ لایه دوم: حکمرانی و مدیریت ریسک نظارتی

در این لایه، نظارت هوشمند به‌عنوان یک نظام ریسک‌محور، پیش‌نگر و تلفیقی تعریف می‌شود. شناسایی، ارزیابی، اولویت‌بندی و پایش ریسک‌ها در سه سطح ریسک بنگاه، ریسک صنعت و ریسک کلان اقتصادی صورت می‌گیرد. این بخش به‌طور مستقیم از چارچوب‌های

[1] Zarsky

نظارت ریسک‌محور و نظارت تلفیقی الهام می‌گیرد (سازمان تنظیم مقررات خدمات مالی، ۲۰۱۴؛ سازمان بیمه و بازنشستگی شغلی اروپایی، ۲۰۲۲).

❖ لایه سوم: زیرساخت داده و فناوری نظارتی

این لایه ستون فقرات چارچوب پیشنهادی محسوب می‌شود و شامل سیستم‌های جمع‌آوری داده، استانداردسازی، یکپارچه‌سازی، تحلیل پیشرفته و مصورسازی اطلاعات است. بهره‌گیری از فناوری‌های SupTech، هوش مصنوعی، یادگیری ماشین و تحلیل بلادرنگ داده‌ها امکان گذار از نظارت واکنشی به نظارت پیش‌بینانه را فراهم می‌سازد (گروه بانک جهانی، ۲۰۲۰؛ انجمن بین‌المللی ناظران بیمه، ۲۰۲۵). در این لایه، معماری‌های داده‌ای و چارچوب‌های تحلیلی مانند CRISP-DM نقش کلیدی ایفا می‌کنند.

❖ لایه چهارم: حکمرانی هوش مصنوعی و کنترل‌های اخلاقی

با توجه به استفاده فزاینده از هوش مصنوعی در نظارت، چارچوب پیشنهادی یک لایه مستقل برای حکمرانی، شفافیت، توضیح‌پذیری و عدالت الگوریتمی در نظر می‌گیرد. این لایه تضمین می‌کند که تصمیم‌های نظارتی مبتنی بر الگوریتم، قابل توضیح، قابل حساب‌خواهی و منطبق با اصول انصاف و حفاظت از داده‌ها باشند (پرینو و یونگ، ۲۰۲۱؛ انجمن بین‌المللی ناظران بیمه، ۲۰۲۵).

❖ لایه پنجم: پیامدها و نتایج نظارتی

خروجی نهایی چارچوب شامل بهبود ثبات مالی، ارتقای حمایت از بیمه‌گذاران، افزایش اعتماد عمومی، کاهش تقلب و افزایش کارایی نهادی است. این پیامدها به‌صورت بازخوردی به لایه‌های پیشین بازمی‌گردند و چرخه یادگیری و بهبود مستمر نظارت را تکمیل می‌کنند (ارسطو و حسینی، ۱۴۰۳؛ کامات[1] و همکاران، ۲۰۲۵).

## نوآوری و تمایز چارچوب پیشنهادی

نوآوری اصلی چارچوب پیشنهادی در تلفیق هم‌زمان چهار بعد کلیدی نهفته است:

۱) رویکرد ریسک‌محور چندسطحی،

۲) حکمرانی داده و هوش مصنوعی،

[1] Kamath et al.

۳) فناوری نظارتی (SupTech)،

۴) بومی‌سازی نهادی برای صنعت بیمه ایران.

برخلاف بسیاری از الگوهای موجود که یا توصیفی‌اند یا صرفاً فناورانه، این چارچوب پل ارتباطی میان نظریه، سیاست‌گذاری و اجرا ایجاد می‌کند و می‌تواند مبنایی برای طراحی شاخص‌ها، ابزارهای نظارتی و نقشه‌راه پیاده‌سازی نظارت هوشمند در صنعت بیمه قرار گیرد.

## یافته‌های پژوهش

### یافته‌های سیاستی و تنظیم‌گری

یافته‌های این پژوهش نشان می‌دهد که گذار به نظارت هوشمند در صنعت بیمه، صرفاً یک پروژه فناورانه نیست، بلکه تحولی سیاستی در پارادایم تنظیم‌گری محسوب می‌شود. نتایج به‌وضوح بیانگر آن است که نظارت سنتی، که عمدتاً واکنشی، پسینی و مبتنی بر گزارش‌های ایستا است، توان پاسخ‌گویی به ریسک‌های نوظهور، پیچیدگی محصولات بیمه‌ای و پویایی بازار را ندارد (گروه بانک جهانی، ۲۰۲۰؛ انجمن بین‌المللی ناظران بیمه، ۲۰۲۵).

از منظر سیاستی، مهم‌ترین دلالت این پژوهش آن است که نظارت هوشمند باید به‌عنوان یک الزام حکمرانی مالی و نه یک انتخاب فناورانه، در اسناد بالادستی صنعت بیمه به رسمیت شناخته شود. این امر مستلزم بازتعریف نقش نهاد ناظر از «بازرس مقررات» به «معمار اکوسیستم داده و ریسک» است. در این چارچوب، اصلاح آیین‌نامه‌های کلیدی نظیر آیین‌نامه گزارشگری، توانگری مالی و فعالیت شرکت‌های بیمه، نه‌تنها مشروعیت حقوقی استفاده از مدل‌های پیش‌بینانه و الگوریتمی را فراهم می‌کند، بلکه زمینه پاسخ‌گویی و شفافیت تصمیمات نظارتی را نیز تقویت می‌نماید (آرنر و همکاران، ۲۰۱۷؛ سازمان بیمه و بازنشستگی شغلی اروپایی، ۲۰۲۲).

### یافته‌های نهادی و سازمانی

نتایج پژوهش نشان داد که یکی از اصلی‌ترین موانع پیاده‌سازی نظارت هوشمند در صنعت بیمه ایران، ناهم‌ترازی ساختار سازمانی و فرهنگ تصمیم‌گیری با منطق داده‌محور است. بنابراین، دلالت نهادی مهم این پژوهش، ضرورت بازآرایی درون‌سازمانی نهاد ناظر است.

بر اساس چارچوب پیشنهادی، استقرار نظارت هوشمند مستلزم شکل‌گیری نقش‌ها و واحدهای جدیدی مانند «مسئول حکمرانی داده»، «تحلیل‌گر ریسک داده‌محور» و «ناظر

الگوریتمی» در ساختار بیمه مرکزی است. علاوه بر این، تغییر فرهنگ سازمانی از اتکای غالب بر قضاوت فردی به تصمیم‌گیری مبتنی بر شواهد داده‌ای، یکی از پیش‌شرط‌های موفقیت این تحول محسوب می‌شود (زرسکی، ۲۰۱۵؛ مصدق و نظری، ۱۴۰۳).

همچنین، یافته‌ها نشان می‌دهد که تمرکز بر یک فرآیند ملموس و پرمسأله مانند پرداخت خسارت، می‌تواند مقاومت سازمانی در برابر تحول دیجیتال را کاهش داده و مشروعیت عملی نظارت هوشمند را در میان ذی‌نفعان تقویت کند. این رویکرد تدریجی، امکان یادگیری سازمانی و اصلاح مستمر مسیر تحول را فراهم می‌سازد.

## یافته‌های فناورانه و داده‌محور

از منظر فناورانه، یافته‌های این پژوهش نشان می‌دهد که سامانه سنهاب در وضعیت فعلی، بیش از آنکه یک پلتفرم نظارت هوشمند باشد، عمدتاً به‌عنوان یک سامانه ثبت اطلاعات و تولید گزارش‌های ایستا عمل می‌کند. در چنین وضعیتی، قابلیت‌های تحلیلی پیشرفته، تحلیل بلادرنگ و پشتیبانی از تصمیم‌گیری پیش‌بینانه به‌طور ساختاری محدود شده‌اند. بر این اساس، یافته‌های فناورانه اصلی پژوهش، ضرورت گذار سنهاب از «سامانه ثبت اطلاعات» به «پلتفرم تحلیلی و تصمیم‌یار نظارتی» است.

نتایج نشان می‌دهد که استقرار زیرساخت‌هایی نظیر مخزن داده[1] مرکزی (به‌عنوان مخزن یکپارچه و مقیاس‌پذیر داده‌های خام، فرآیندی و چندمنبعی صنعت بیمه)، موتور قواعد نظارتی، مدل‌های یادگیری ماشین و داشبوردهای نظارتی بلادرنگ، بستر لازم برای تحقق نظارت پیش‌بینانه، هشدارمحور و مبتنی بر ریسک را فراهم می‌سازد (گروه بانک جهانی، ۲۰۲۰؛ پرینو و یونگ، ۲۰۲۱). معماری مخزن داده ، برخلاف پایگاه‌های داده عملیاتی سنتی، امکان ذخیره‌سازی داده‌ها در قالب اولیه و بدون تحمیل ساختار تحلیلی از پیش تعیین‌شده را فراهم کرده و از این طریق، تغذیه مدل‌های تحلیلی و الگوریتم‌های هوشمند نظارتی را ممکن می‌سازد.

علاوه بر این، توسعه رابط‌های برنامه‌نویسی کاربردی (API) استاندارد و امن، نه‌تنها فرآیند تبادل داده میان نهاد ناظر و شرکت‌های بیمه را تسهیل می‌کند، بلکه زمینه اتصال سنهاب به اکوسیستم ملی داده، از جمله سامانه‌های پلیس، نظام بانکی و نظام سلامت را نیز فراهم می‌آورد؛

[1] Data Lake

امری که در تجارب موفق بین‌المللی به‌عنوان یکی از ارکان کلیدی نظارت هوشمند شناخته شده است (انجمن بین‌المللی ناظران بیمه، ۲۰۲۵).

### یافته‌ها برای صنعت بیمه و شرکت‌های بیمه

پیاده‌سازی نظارت هوشمند پیامدهای مهمی برای شرکت‌های بیمه نیز به همراه دارد. برخلاف تصور رایج، نظارت هوشمند صرفاً ابزار کنترل نهاد ناظر نیست، بلکه می‌تواند محرک بهبود عملکرد درون‌شرکتی باشد. الزام به استانداردسازی داده‌ها، گزارش‌دهی برخط و شفافیت فرآیندی، شرکت‌ها را به سمت اصلاح فرآیندهای داخلی، کاهش ناکارآمدی و ارتقای مدیریت ریسک سوق می‌دهد (ابراهیمی و عارف، ۱۴۰۳).

از سوی دیگر، تمرکز بر شاخص‌های قابل سنجش مانند «زمان پرداخت خسارت» باعث می‌شود رقابت میان شرکت‌ها از قیمت‌محوری به کیفیت خدمت و کارایی عملیاتی منتقل شود؛ موضوعی که در نهایت به افزایش اعتماد عمومی به صنعت بیمه منجر خواهد شد (ارسطو و حسینی، ۱۴۰۳).

### یافته‌های پژوهشی و مسیرهای آتی تحقیق

از منظر علمی، این پژوهش چند دلالت مهم برای تحقیقات آتی دارد. نخست آنکه چارچوب مفهومی ارائه‌شده می‌تواند مبنایی برای توسعه مدل‌های تجربی و کمی در حوزه سنجش بلوغ نظارت هوشمند قرار گیرد. پژوهش‌های آینده می‌توانند با استفاده از داده‌های واقعی سنهاب، اثر پیاده‌سازی ابزارهای هوشمند را بر شاخص‌هایی مانند ثبات مالی، کاهش تقلب یا بهبود زمان پرداخت خسارت ارزیابی کنند.

دوم، بررسی ابعاد اخلاقی و حکمرانی هوش مصنوعی در تصمیمات نظارتی، به‌ویژه در زمینه توضیح‌پذیری و پاسخ‌گویی الگوریتم‌ها، یک حوزه پژوهشی نوظهور و ضروری برای مطالعات آتی محسوب می‌شود (زرسکی، ۲۰۱۵؛ انجمن بین‌المللی ناظران بیمه، ۲۰۲۵).

در نهایت، مقایسه تطبیقی مسیر گذار ایران با سایر کشورهای در حال توسعه، می‌تواند به غنای ادبیات نظارت هوشمند در بسترهای غیرغربی کمک کند و شکاف موجود در پژوهش‌های بین‌المللی را کاهش دهد.

## بحث و نتیجه‌گیری

این پژوهش با تمرکز بر ضرورت گذار نهاد ناظر بیمه ایران از الگوهای سنتی نظارت به سمت نظارت هوشمند، داده‌محور و پیش‌آگاهانه انجام شد. نتایج حاصل نشان داد که تحول نظارتی در صنعت بیمه، نه یک انتخاب فناورانه، بلکه پاسخی اجتناب‌ناپذیر به پیچیدگی‌های فزاینده بازار، رشد بیمه‌های دیجیتال، افزایش ریسک‌های سیستمی و انتظارات فزاینده ذی‌نفعان است.

ابتدا، با مرور ادبیات نظری و تجارب بین‌المللی، چارچوب مفهومی نظارت هوشمند تبیین و تمایز آن با مفاهیمی نظیر فناوری‌های نظارتی (SupTech) و فناوری‌های تنظیم‌گری (RegTech) به‌صورت شفاف مشخص شد. یافته‌ها نشان دادند که علی‌رغم پیشرفت‌های قابل توجه کشورهای پیشرو، نمونه‌ای از پیاده‌سازی کامل و بالغ نظارت هوشمند وجود ندارد و اغلب کشورها مسیر تدریجی، مسئله‌محور و مبتنی بر بلوغ داده را دنبال کرده‌اند. این نکته، اهمیت طراحی یک نقشه راه بومی و واقع‌بینانه برای ایران را برجسته ساخت.

سپس این پژوهش با تمرکز بر تحلیل وضعیت موجود صنعت بیمه ایران و نهاد ناظر، شکاف‌های ساختاری، داده‌ای، حقوقی و انسانی را آشکار نمود. بررسی سامانه سنهاب به‌عنوان زیرساخت محوری نظارت نشان داد که ضعف کیفیت داده، فقدان استانداردهای تبادل، فرآیندهای دستی و نبود ابزارهای تحلیلی پیشرفته، مانع اصلی تحقق نظارت هوشمند است. در این میان، فرآیند پرداخت خسارت به‌عنوان نقطه آغاز تحول انتخاب شد؛ چراکه هم از منظر اعتماد عمومی و هم از حیث قابلیت سنجش و بهبود، بالاترین اولویت را دارد.

بر این اساس، یک نقشه راه ۲۴ ماهه، مرحله‌بندی‌شده و عمل‌گرا طراحی شد که از اصلاح داده‌های پایه و شفاف‌سازی فرآیند پرداخت خسارت آغاز می‌شود و به‌تدریج به استقرار لایه‌های تحلیلی، هشدار هوشمند و نظارت پیش‌بینانه بر توانگری مالی منتهی می‌گردد. نقطه قوت اصلی این نقشه راه، نگاه کل‌نگر آن به ابعاد فناورانه، حقوقی، سازمانی و انسانی و همسویی آن با تجارب موفق بین‌المللی، به‌ویژه مدل کره جنوبی در زیرساخت فنی و مدل انگلستان (FCA) در فلسفه نظارتی است.

در مجموع، این پژوهش نشان می‌دهد که موفقیت در استقرار نظارت هوشمند در صنعت بیمه ایران، بیش از آنکه وابسته به فناوری‌های پیشرفته باشد، نیازمند عزم مدیریتی، اصلاح حکمرانی داده، بازنگری مقررات و تغییر پارادایم تصمیم‌گیری نظارتی از واکنشی به پیشگیرانه است. نقشه راه پیشنهادی می‌تواند به‌عنوان یک چارچوب اجرایی معتبر، مبنای سیاست‌گذاری و اقدام عملی بیمه مرکزی در مسیر تحول دیجیتال نظارت قرار گیرد.

## پیشنهادهایی برای پژوهش‌های آتی

با وجود جامعیت چارچوب ارائه‌شده، این پژوهش زمینه‌ساز مجموعه‌ای از مطالعات تکمیلی است که می‌تواند به تعمیق و توسعه ادبیات نظارت هوشمند در صنعت بیمه منجر شود. مهم‌ترین محورهای پیشنهادی برای پژوهش‌های آتی عبارت‌اند از:

۱) توسعه و اعتبارسنجی تجربی مدل‌های پیش‌بینی توانگری مالی

۲) پژوهش‌های آینده می‌توانند با استفاده از داده‌های واقعی شرکت‌های بیمه، به طراحی و مقایسه مدل‌های یادگیری ماشین و الگوریتم‌های پیش‌بینی ریسک ورشکستگی پرداخته و کارایی آن‌ها را در مقایسه با مدل‌های سنتی نظارتی ارزیابی کنند.

۳) تحلیل اقتصادی و هزینه–فایده نظارت هوشمند

۴) انجام مطالعات هزینه–فایده در خصوص سرمایه‌گذاری‌های فناورانه، توسعه زیرساخت داده و آموزش نیروی انسانی در برابر منافع حاصل از کاهش تأخیر نظارتی، پیشگیری از بحران‌ها و ارتقای انضباط بازار، می‌توانند پشتوانه‌ای قوی برای تصمیم‌گیری سیاست‌گذاران فراهم آورد.

۵) بررسی ابعاد حقوقی و اخلاقی استفاده از الگوریتم‌ها در نظارت

۶) با گسترش استفاده از هوش مصنوعی در تصمیم‌سازی‌های نظارتی، موضوعاتی نظیر شفافیت الگوریتمی، پاسخ‌گویی، سوگیری، و حفاظت از حریم خصوصی اهمیت فزاینده‌ای می‌یابد. پژوهش‌های آتی می‌توانند چارچوب‌های حقوقی و اخلاقی مناسب برای استفاده مسئولانه از این فناوری‌ها را بررسی کنند.

۷) مطالعه واکنش رفتاری شرکت‌های بیمه به نظارت هوشمند

۸) بررسی تغییرات رفتار شرکت‌های بیمه در مواجهه با نظام‌های نظارتی داده‌محور، از جمله در حوزه گزارش‌دهی، مدیریت ریسک و نوآوری محصول، می‌تواند به بهبود طراحی ابزارهای تنظیم‌گری و نظام مشوق‌ها کمک نماید.

۹) طراحی مدل بلوغ نظارت هوشمند

۱۰) توسعه یک چارچوب بومی برای سنجش سطح بلوغ نظارت هوشمند، امکان پایش مستمر پیشرفت نهاد ناظر و مقایسه تطبیقی با سایر کشورها را فراهم می‌سازد.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع

ابراهیمی، ندا؛ عارف، مهسا. (۱۴۰۳). *نقش نظارت هوشمند در ارتقای شفافیت و اعتمادسازی در صنعت بیمه ایران*. مقاله ارائه‌شده در سی‌ویکمین همایش ملی و دوازدهمین همایش بین‌المللی بیمه و توسعه: رضایت‌مندی و اعتماد مردم به صنعت بیمه، تهران، ایران. https://civilica.com/doc/2148797

ارسطو، ایمان؛ حسینی، الهام. (۱۴۰۳). *الگوی بهینه برای نظارت هوشمند در صنعت بیمه ایران*. مقاله ارائه‌شده در سی‌ویکمین همایش ملی و دوازدهمین همایش بین‌المللی بیمه و توسعه: رضایت‌مندی و اعتماد مردم به صنعت بیمه، تهران، ایران. https://civilica.com/doc/2148742

امینی، علیرضا. (۱۴۰۰). *ارائه الگوی پارادایمی نظارت هوشمند الکترنیک در صنعت بیمه: برساخت گرایی اجتماعی Social constructivism*. مقاله ارائه‌شده در بیست‌وهشتمین همایش بیمه و توسعه. تهران، ایران. https://civilica.com/doc/1390786

رئیسی، محمد؛ فلاح نژاد، محمدرضا. (۱۴۰۳). *ارائه الگوی پارادایمی نظارت هوشمند در راستای ارتقای اعتماد عمومی به صنعت بیمه*. مقاله ارائه‌شده در سی ویکمین همایش ملی و دوازدهمین همایش بین المللی بیمه و توسعه: رضایت‌مندی و اعتماد مردم به صنعت بیمه، تهران، ایران. https://civilica.com/doc/2148847

عابد، مجتبی؛ قنبروند، حمید. (۱۴۰۲). *سندباکس: ابزاری نوین برای نظارت و تنظیم‌گری هوشمند در صنعت بیمه*. مقاله ارائه‌شده در سی‌امین همایش ملی و یازدهمین همایش بین‌المللی بیمه و توسعه با موضوع تکامل زیست‌بوم صنعت بیمه (تکافل، حکمرانی و فناوری‌های نوین)، تهران، ایران. https://civilica.com/doc/2115371

مصدق، حامد؛ نظری، محسن. (۱۴۰۳). *طراحی الگوی نظارت هوشمند در صنعت بیمه*. مقاله ارائه‌شده در سی‌ویکمین همایش ملی و دوازدهمین همایش بین‌المللی بیمه و توسعه: رضایت‌مندی و اعتماد مردم به صنعت بیمه، تهران، ایران. https://civilica.com/doc/2148727

نورانی، وحیده. (۱۴۰۰). *مروری بر مفهوم فناوری نظارتی(ساپتک) و برخی سازوکارهای استفاده از آن در نظارت صنعت بیمه*. پژوهشکده بیمه. https://www.irc.ac.ir/fa-IR/Irc/4946/Articles/view/14643/1535

نیاکان، لیلی؛ فرازمند، سجاد؛ عطاطلب، فاطمه. (۱۴۰۳). *بررسی و آسیب‌شناسی قانون تأسیس بیمه مرکزی ایران و بیمه‌گری*. مطالعات مدیریت استراتژیک، ۱۵(۶۰)، ۴۹–۷۳. https://www.smsjournal.ir/article_211832.html

## References

Abed, M., & Ghanbarvand, H. (2023). *Sandbox: A novel tool for smart supervision and regulation in the insurance industry* [Conference paper]. 30th National and 11th International Conference on Insurance and Development: Evolution of the Insurance Industry Ecosystem (Takaful, Governance, and Emerging Technologies), Tehran, Iran. https://civilica.com/doc/2115371 (in Persian)

Alaika Advisory. (2025). *Insurance trends 2025*. https://www.alaika-advisory.com/insights/insurance-trends-2025

Amini, A. (2021). *Presenting a paradigmatic model of smart electronic supervision in the insurance industry: Social constructivism* [Conference paper]. 28th Insurance and Development Conference, Tehran, Iran. https://civilica.com/doc/1390786 (in Persian)

Arasto, I., & Hosseini, E. (2024). *An optimal model for smart supervision in Iran's insurance industry* [Conference paper]. 31st National and 12th International Conference on Insurance and Development: Public Satisfaction and Trust in the Insurance Industry. Tehran, Iran. https://civilica.com/doc/2148742/ (in Persian)

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *FinTech, regTech, and the reconceptualization of financial regulation*. Northwestern Journal of International Law & Business, 37(3), 373–415. https://doi.org/10.2139/ssrn.3088303

Baumol, W. J. (1986). *Williamson's The economic institutions of capitalism* [Review of the book *The economic institutions of capitalism*, by O. E. Williamson]. The RAND Journal of Economics, 17(2), 279–283. https://www.jstor.org/stable/2555390

Bovens, M. (2007). Analyzing and assessing accountability: A conceptual framework. *European Law Journal, 13*(4), 447–468. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-0386.2007.00378.x

Braun, A., & Schreiber, F. (2017). *The Current InsurTech Landscape: Business Models and Disruptive Potential*. I.VW-HSG Schriftenreihe, 62. University of St. Gallen, Institute of Insurance Economics (I.VW-HSG). https://ideas.repec.org/b/zbw/usgivw/62.html

Charoenwong, B., Kowaleski, Z. T., Kwan, A., & Sutherland, A. G. (2024). RegTech: Technology-driven compliance and its effects on profitability, operations, and market structure. *Journal of Financial Economics, 154*, 103792. https://doi.org/10.1016/j.jfineco.2024.103792

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework*. https://www.coso.org/guidance-on-ic

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance.* https://www.coso.org/guidance-erm

Cosma, S., & Rimo, G. (2024). Redefining insurance through technology: Achievements and perspectives in Insurtech. *Research in International Business and Finance, 70*, 102301. https://doi.org/10.1016/j.ribaf.2024.102301

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

Ebrahimi, N., & Aref, M. (2024). *The role of smart supervision in enhancing transparency and trust in Iran's insurance industry* [Conference paper]. 31st National and 12th International Conference on Insurance and Development, Tehran, Iran. https://civilica.com/doc/2148797/ (in Persian)

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review, 14*(1), 57–74. https://doi.org/10.5465/amr.1989.4279003

European Insurance and Occupational Pensions Authority. (2017). *A common supervisory culture.* https://www.eiopa.europa.eu/

European Insurance and Occupational Pensions Authority. (2021). *SupTech strategy*. https://www.eiopa.europa.eu/

European Insurance and Occupational Pensions Authority. (2022a). *General principles of supervision*. https://www.eiopa.europa.eu/

European Insurance and Occupational Pensions Authority. (2022b). *Supervision in a fast-paced digital world*. https://www.eiopa.europa.eu/

Financial Services Regulatory Authority. (2014). Risk-based supervisory framework. https://fsrastlucia.org/images/Risk-Based_Supervisory_Framework.pdf

Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., & De Colle, S. (2010). *Stakeholder theory: The state of the art*. Cambridge University Press. https://doi.org/10.1080/19416520.2010.495581

Georgosouli, A., & Okonjo, J. (2022). The algorithmic future of insurance supervision in the EU: A reality check. *In* P. Marano & K. Noussia (Eds.), *The Governance of Insurance Undertakings: Corporate Law and Insurance Regulation* (pp. 217-244). Springer International Publishing. https://doi.org/10.1007/978-3-030-85817-9_10

Gunningham, N., & Grabosky, P. (1998). *Smart regulation: Designing environmental policy*. Oxford University Press. https://www.researchgate.net/publication/258261698_Smart_Regulation_Designing_Environment_Policy

Holland, C. P., & Kavuri, A. S. (2025). Insurtech strategies: A comparison of incumbent insurance firms with new entrants. *The Geneva Papers on Risk and Insurance – Issues and Practice, 50*(1), 78–105. https://doi.org/10.1057/s41288-024-00341-0

International Association of Insurance Supervisors. (1999). *Principles applicable to the supervision of international insurers and insurance groups and their cross-border business operations.* https://www.iais.org/uploads/2022/01/Principles_applicable_to_the_supervision_of_International_insurers_and_insurance_group_and_their_cross_borders_business_operations.pdf

International Association of Insurance Supervisors. (2018). *Insurance core principles, standards, guidance and assessment methodology.* https://www.iais.org/uploads/2025/06/IAIS-ICPs-and-ComFrame-December-2024.pdf

International Association of Insurance Supervisors. (2025). *Roadmap 2025–2026: Key deliverables and supervisory priorities* [Press release]. https://www.iais.org/uploads/2025/01/IAIS-Roadmap-2025-2026.pdf

Kamath, M., Dwarkanath, P., & Ganesan, A. (2025). *How to become an AI-first insurer: A transformation roadmap* [White paper]. Infosys. https://www.infosys.com/industries/insurance/documents/transformation-roadmap.pdf

Monetary Authority of Singapore. (2018). *Risk-based supervisory framework.* https://fsrastlucia.org/images/Risk-Based_Supervisory_Framework.pdf

Mosadegh, H., & Nazari, M. (2024). *Designing a smart supervision model in the insurance industry* [Conference paper]. 31st National and 12th International Conference on Insurance and Development: Public Satisfaction and Trust in the Insurance Industry, Tehran, Iran. https://civilica.com/doc/2148727/ (in Persian)

National Association of Insurance Commissioners. (2024). *The state of insurtech. NAIC*. https://media-publications.bcg.com/State-of-Insurtech-2024.pdf?linkId=833816433

Niakan, L., Farazmand, S., & Atatalab, F. (2024). A study and pathology of the Law on the Establishment of Central Insurance of Iran and insurance activity. *Quarterly Journal of Strategic Management Studies*, 15(60), 49-73. https://doi.org/10.22034/smsj.2023.399753.1864 (in Persian)

Norani, V. (2021). *An overview of the concept of supervisory technology (SAPTECH) and some mechanisms for its use in supervision of the insurance industry*. Insurance Research Institute. https://www.irc.ac.ir/fa-IR/Irc/4946/Articles/view/14643/1535 (in Persian)

Prenio, J., Pustelnikov, A., & Yeo, J. (2024). *Building a more diverse suptech ecosystem: Findings from surveys of financial authorities and suptech vendors* [White paper]. Bank for International Settlements. https://www.bis.org/fsi/fsibriefs23.htm

Prenio, J., & Yong, J. (2021). *Humans keeping AI in check – Emerging regulatory expectations in the financial sector* (FSI Insights No. 35). Bank for International Settlements. https://www.bis.org/fsi/publ/insights35.htm

Raeesi, M., & Fallahnejad, M. R. (2024). *Presenting a paradigmatic model of smart supervision to enhance public trust in the insurance industry* [Conference paper]. 31st National and 12th International Conference on Insurance and Development, Tehran, Iran. https://civilica.com/doc/2148847/ (in Persian)

Stiglitz, J. E. (2000). *The contributions of the economics of information to twentieth century economics*. The Quarterly Journal of Economics, 115(4), 1441–1478. https://doi.org/10.1162/003355300555015

World Bank Group. (2020). *A roadmap to SupTech solutions for low income (IDA) countries*. https://documents1.worldbank.org/curated/en/108411602047902677/pdf/A-Roadmap-to-SupTech-Solutions-for-Low-Income-IDA-Countries.pdf

Zarsky, T. (2015). The trouble with algorithmic decisions: An analytic roadmap to examine efficiency and fairness in automated and opaque decision making. *Science, Technology, & Human Values*, 41(1), 118–132. https://philpapers.org/rec/ZARTTW

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Research Paper**

# The Digital Transformation of the Internal Audit Function: A Qualitative Literature Review [1]

**Neda Rasouli[*2] and Parsa Bahmanabadi [3]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 127-158

Received: 2026.04.04
Revised: 2026.08.11
Accepted: 2026.09.19

## Abstract

Artificial Intelligence (AI) is significantly transforming the internal audit function by enhancing efficiency, accuracy, and data management. Through the automation of repetitive tasks and comprehensive data analysis, AI repositions internal auditors as strategic advisors. However, its adoption presents challenges related to technological complexity, data security, and the need for new skills. In Morocco, AI integration remains limited, hindered by organizational and cultural barriers. This study highlights the importance of examining individual factors influencing AI acceptance among internal auditors. Digitalization thus emerges as a key lever for modernizing and enhancing the strategic role of internal auditing. To explore this transformation, a qualitative literature review was conducted to understand how digitalization has evolved within internal auditing at a global level. More than a simple inventory of publications, this approach captures the discursive and semantic dynamics that have shaped the relationship between digitalization and auditing over time and across regions. The review reveals both convergences and divergences in how internal audit functions are adopting digital tools, and highlights the distinct developmental paths followed by developed countries, emerging economies, and developing regions. Ultimately, the qualitative literature review provides a relevant analytical framework and a rich geographical and textual mapping of the changes underway in auditing in the digital age.

**Keywords**: Digitalization, Internal Audit, Qualitative Literature Review.
**JEL classification:** *M42.*

---

[1] https://doi.org/10.22034/JISTA.2026.595807.1094
[1] Selected Paper of the First National Conference on Perspectives in Internal Auditing
[2] Assistant Professor, Faculty of Management and Financial Sciences, Department of Accounting, Khatam University, Tehran, Iran. (Corresponding Author). (n.rasooli@khatam.ac.ir).
[3] Master's Student, Faculty of Management and Financial Sciences, Department of Accounting, Khatam University, Tehran, Iran. (bahmanabadiparsa@gmail.com).

## 1. INTRODUCTION AND OBJECTIVE

Digital transformation has emerged as a fundamental driver of organizational change, reshaping business processes, governance structures, and decision-making practices across industries. The widespread adoption of advanced technologies—including artificial intelligence (AI), big data analytics, robotic process automation (RPA), cloud computing, and digital information systems—has significantly transformed the way organizations manage risks, process information, and evaluate performance. As organizations become increasingly data-driven, the internal audit function has also undergone substantial transformation, moving beyond its traditional assurance role toward a strategic function that supports governance, risk management, and organizational value creation

The increasing availability of digital technologies enables internal auditors to examine complete datasets, automate repetitive audit procedures, perform continuous monitoring, and identify emerging risks more effectively than conventional audit approaches. These technological developments have improved audit efficiency and accuracy while expanding the advisory role of internal auditors within organizations. At the same time, digital transformation introduces new challenges, including cybersecurity risks, ethical concerns surrounding artificial intelligence, data governance issues, and the need for continuous development of auditors' digital competencies. Consequently, organizations must not only invest in technological infrastructure but also prepare their audit professionals to operate effectively in rapidly evolving digital environments

Although scholarly interest in digital transformation and internal auditing has increased considerably in recent years, existing studies have generally focused on specific technologies or isolated empirical investigations. As a result, the current body of knowledge remains fragmented, making it difficult to obtain a comprehensive understanding of the evolution of this research field. Moreover, limited attention has been devoted to synthesizing recent findings and identifying major research trends, dominant themes, and existing knowledge gaps from a broader perspective

Unlike previous studies, the present research adopts a qualitative literature review approach to provide an integrated assessment of recent scientific evidence concerning digital transformation in internal auditing. By combining textual, chronological, and geographical analyses of publications indexed in the Scopus database, the study offers a comprehensive overview of how research in this field has evolved, identifies the principal themes investigated by researchers, and highlights opportunities for future scholarly inquiry. This integrated perspective represents the primary contribution of the study and distinguishes it from previous reviews that primarily emphasized individual technologies or empirical findings

Accordingly, the main objective of this study is to analyze recent scientific literature on the digital transformation of the internal audit function, identify prevailing research trends, examine the geographical distribution of scholarly contributions, and discuss the implications of digital technologies for the future development of internal auditing. The findings are expected to contribute to both academic knowledge and professional practice by providing a comprehensive understanding of current developments and future directions within this rapidly evolving field.

## 2. MATERIALS AND METHODS

This study employed a qualitative literature review to examine the current state of knowledge regarding the digital transformation of the internal audit function. A qualitative review was selected because it enables a systematic synthesis of existing scientific evidence while facilitating the identification of conceptual developments, dominant research themes, and emerging trends within a rapidly evolving field. Rather than statistically combining previous findings, this approach emphasizes critical interpretation and integration of published research to provide a comprehensive understanding of the phenomenon under investigation. The review was conducted using the Scopus database, which was selected because of its extensive coverage of peer-reviewed international journals and its recognition as one of the most reliable

sources for academic literature. The search focused on studies published between 2020 and 2025, reflecting the period during which digital technologies—particularly artificial intelligence, data analytics, and intelligent automation—experienced rapid development and widespread adoption in organizational auditing practices.

A structured screening procedure was applied to ensure the relevance and quality of the reviewed publications. Only peer-reviewed journal articles indexed in Scopus and directly addressing the relationship between digital transformation and the internal audit function were included in the analysis. Conference papers, books, dissertations, duplicate records, and publications unrelated to the objectives of the study were excluded. Following the screening process, nine articles met the selection criteria and were included in the final qualitative analysis.

To achieve the objectives of the study, the selected publications were examined from three complementary perspectives. The first stage involved textual analysis, through which the most frequently occurring concepts and keywords were identified in order to determine the dominant themes within the literature. Particular attention was devoted to concepts associated with digitalization, artificial intelligence, data analytics, and the internal audit function, as these terms reflected the principal directions of contemporary research.

The second stage consisted of chronological analysis, which explored publication trends during the selected period. This analysis provided insight into the evolution of scholarly interest in digital transformation and revealed the years in which research activity expanded most significantly. Examining publication patterns also enabled the study to assess the maturity of the research field and identify recent developments in academic attention.

Finally, a geographical analysis was conducted to identify the countries contributing most actively to research on digital transformation in internal auditing. This analysis highlighted the international distribution of scientific production and provided a broader perspective on how research activity has developed across different regions. Collectively, these three analytical dimensions enabled the study to synthesize existing knowledge, identify

research gaps, and establish a coherent understanding of the evolution of digital transformation within the internal audit function.

## 3. RESULTS AND DISCUSSION

The The review findings indicate that digital transformation has become one of the principal drivers of change within the internal audit profession. Analysis of the selected studies demonstrates that the integration of digital technologies has expanded the role of internal auditors beyond traditional assurance activities, enabling them to contribute more effectively to organizational governance, strategic decision-making, and enterprise risk management. Rather than serving solely as mechanisms for automating routine audit procedures, digital technologies are increasingly viewed as strategic resources that enhance the overall quality, efficiency, and responsiveness of internal audit activities.

The textual analysis revealed that Internal Audit, Digitalization, Artificial Intelligence, Data Analytics, and Internal Audit Function were the most frequently occurring concepts within the reviewed literature. The prominence of these keywords demonstrates that contemporary research primarily concentrates on the integration of intelligent technologies into auditing processes. Artificial intelligence and data analytics have attracted particular scholarly attention because they enable auditors to process large volumes of organizational data, identify unusual patterns, detect potential fraud, and improve the quality of audit evidence. In contrast, topics such as blockchain, digital platforms, and machine learning appeared less frequently, suggesting that these technologies remain underexplored and represent promising directions for future research.

The chronological analysis indicates that scientific interest in digital transformation has increased noticeably since 2020. Although the total number of relevant publications remains limited, research activity has grown steadily, with the highest publication output occurring in 2021, followed by another increase during 2024. This trend reflects the accelerating adoption of digital technologies across organizations and the growing recognition of their strategic

importance for internal auditing. The findings also suggest that the field is still developing, leaving considerable opportunities for additional theoretical and empirical investigations.

The geographical analysis demonstrates that research output is concentrated in a relatively small number of countries. European nations, particularly Belgium and Germany, account for a significant proportion of the reviewed publications, while contributions from developing economies remain comparatively limited. Although countries such as Indonesia, Iraq, Italy, and Morocco have recently begun contributing to this research area, the international distribution of publications remains uneven. This imbalance indicates that differences in digital infrastructure, regulatory frameworks, organizational maturity, and professional capabilities may influence both the implementation of digital technologies and the direction of future academic research.

Across the reviewed studies, digital technologies were consistently associated with improvements in audit effectiveness. Artificial intelligence, advanced data analytics, and automation technologies enable continuous auditing, improve fraud detection, strengthen risk assessment, reduce manual processing time, and support evidence-based decision-making. These capabilities allow internal auditors to shift their focus from routine compliance verification toward analytical and advisory responsibilities that create greater organizational value. Nevertheless, the reviewed literature also emphasizes that technological innovation alone cannot ensure successful digital transformation. Organizations must simultaneously invest in digital competencies, cybersecurity, data governance, ethical standards, and continuous professional education to fully realize the benefits of emerging technologies. Consequently, the future effectiveness of internal auditing will depend on the successful integration of advanced digital tools with the professional judgment, critical thinking, and ethical responsibilities of internal auditors.

## 4. CONCLUSION AND SUGGESTIONS

This qualitative literature review demonstrates that digital transformation is fundamentally redefining the role and responsibilities of the internal audit function. The reviewed studies consistently indicate that the adoption of digital technologies—including artificial intelligence, data analytics, robotic process automation, and other intelligent systems—has significantly improved audit efficiency, expanded analytical capabilities, and strengthened the contribution of internal auditing to organizational governance and risk management. As a result, internal auditors are increasingly expected to provide forward-looking insights and strategic recommendations rather than focusing exclusively on traditional assurance and compliance activities.

The review also highlights that the successful implementation of digital transformation extends beyond technological adoption. Organizations must establish appropriate digital infrastructures, enhance cybersecurity frameworks, improve data governance practices, and continuously develop the digital competencies of internal auditors. Although intelligent technologies can automate many routine audit procedures and improve the quality of audit evidence, they cannot fully replace professional judgment, ethical reasoning, or critical thinking. Therefore, the future effectiveness of internal auditing depends on achieving an appropriate balance between technological innovation and human expertise.

Another important finding is that the existing body of research remains relatively limited in both scope and geographical diversity. Most published studies originate from a small number of developed countries, while empirical evidence from developing economies is still scarce. This imbalance highlights the need for further investigations that consider different institutional environments, regulatory systems, organizational characteristics, and levels of digital maturity. Expanding research across diverse contexts would contribute to a more comprehensive understanding of how digital transformation influences internal auditing worldwide.

Based on the findings of this review, several practical and academic recommendations can be proposed. Organizations should formulate comprehensive digital transformation strategies for internal audit functions, invest in advanced analytical technologies, strengthen cybersecurity and data governance mechanisms, and provide continuous training programs that enhance auditors' technological competencies. From a research perspective, future studies should explore the practical implications of emerging technologies such as generative artificial intelligence, blockchain, machine learning, and predictive analytics through empirical investigations conducted across different organizational and national contexts. Such research would enrich the theoretical foundation of digital auditing while supporting organizations in adapting their internal audit functions to an increasingly digital business environment.

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# تحول دیجیتال در عملکرد حسابرسی داخلی: بررسی کیفی ادبیات[1]

**ندا رسولی[2]* و پارسا بهمن‌آبادی[3]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۱۲۷ - ۱۵۸

تاریخ دریافت: ۱۴۰۵/۰۱/۱۵
تاریخ بازنگری: ۱۴۰۵/۰۵/۲۰
تاریخ پذیرش: ۱۴۰۵/۰۶/۲۸

## چکیده

*هوش مصنوعی بطور قابل توجهی در عملکرد حسابرسی داخلی تحول ایجاد می‌نماید و کارایی، دقت و مدیریت داده‌ها را افزایش می‌دهد. هوش مصنوعی، حسابرسان داخلی را از طریق اتوماتیک کردن وظایف تکراری و تحلیل جامع داده‌ها به مشاوران استراتژیک تبدیل می‌کند. با این حال، پذیرش هوش مصنوعی چالش‌هایی مرتبط با پیچیدگی فناوری، امنیت داده‌ها و نیاز به مهارت‌های جدید را ایجاد می‌کند. مطالعه حاضر بر اهمیت بررسی عوامل فردی تأثیرگذار بر پذیرش هوش مصنوعی در میان حسابرسان داخلی تأکید می‌کند. بنابراین، دیجیتال‌سازی به عنوان یک اهرم کلیدی برای مدرن‌سازی و افزایش نقش استراتژیک حسابرسی داخلی ظاهر می‌شود. برای بررسی این تحول، در پژوهش حاضر بررسی کیفی ادبیات انجام شد تا چگونگی تکامل یافتن دیجیتال‌سازی در حسابرسی داخلی در سطح جهانی مشخص گردد. بررسی‌ها نشان داد که هم همگرایی‌ها و هم واگرایی‌ها در نحوه پذیرش ابزارهای دیجیتال در عملکردهای حسابرسی داخلی وجود دارد وتفاوت های موجود در مسیر تحول حسابرسی داخلی در کشورهای توسعه یافته،اقتصادهای نوظهور و کشورهای درحال توسعه شناسایی شد. . در نهایت پس از بررسی کیفی ادبیات، چارچوب تحلیلی مرتبط و نقشه‌برداری جغرافیایی ، مبانی نظری حسابرسی دیجیتال بسط و توسعه یافته است.*

**واژه‌های کلیدی:** *دیجیتال‌سازی، حسابرسی داخلی، بررسی کیفی ادبیات.*

**طبقه‌بندی موضوعی:** *M42*

---

[1] https://doi.org/10.22034/JISTA.2026.595807.1094

[1] مقاله منتخب نخستین کنفرانس ملی چشم‌انداز حسابرسی داخلی

[2] استادیار، دانشکده مدیریت و علوم مالی،گروه حسابداری، دانشگاه خاتم، تهران، ایران. (نویسنده مسئول). (n.rasooli@khatam.ac.ir)

[3] دانشجوی کارشناسی ارشد، دانشکده مدیریت و علوم مالی، گروه حسابداری، دانشگاه خاتم، تهران، ایران. (bahmanabadiparsa@gmail.com)

**مقدمه**

هوش مصنوعی به طور فزاینده‌ای به عنوان یک محرک کلیدی تحول در حوزه‌های حرفه‌ای متعدد از جمله حسابرسی داخلی، شناخته می‌شود (بادیا[1] ، ۲۰۲۲). در محیط امروز که به سرعت دیجیتال‌سازی می‌شود، سازمان‌ها مجبور به پذیرش نوآوری‌های فناوری برای حفظ رقابت‌پذیری و برآورده کردن انتظارات در حال تغییر مشتریان هستند. مطالعات فاگو[2] و همکاران در سال ۲۰۲۱ و سید[3] و همکاران در سال ۲۰۲۱ نشان داد که سازمان‌هایی که به طور مؤثر با این تغییرات فناوری سازگار می‌شوند، از مزایای مالی و سازمانی مختلفی از جمله افزایش قابل توجه حجم معاملات و داده‌های پردازش‌شده بهره‌مند می‌شوند.

اهمیت حسابرسی در چشم‌انداز اقتصادی و مقرراتی که روز به روز پیچیده‌تر می‌شود، همچنان در حال افزایش است. هم حسابرسان داخلی و هم حسابرسان خارجی از طریق اطمینان‌دهی در خصوص یکپارچگی مالی، رعایت مقررات و کارایی عملیاتی نقش اساسی در حاکمیت شرکتی ایفا می‌کنند. در زمینه جهانی‌سازی و شتاب دیجیتال، حسابرسان اکنون با حجم عظیمی از داده‌ها و ریسک‌های نوظهور روبرو هستند که نقش آن‌ها را ضروری‌تر و پیچیده‌تر از همیشه می‌کند (کودر[4] ,۲۰۱۵ ص ۱). حسابرسی امروزه فراتر از تشخیص تقلب و خطاها است و به بهبود مداوم فرآیندها کمک می‌کند و از تصمیم‌گیری استراتژیک حمایت می‌کند (لنز[5] و هان[6] , ۲۰۱۵). علاوه بر این، در پاسخ به رسوایی‌های مالی اخیر و درخواست‌های فزاینده برای شفافیت، حسابرسی اعتماد ذینفعان را افزایش می‌دهد و به پایداری بازارهای مالی کمک می‌کند (نیچل[7] و سالتریو[8] ,۲۰۱۶).

پذیرش هوش مصنوعی در عملکرد حسابرسی داخلی، هم دامنه و هم اثربخشی ماموریت‌های حسابرسی را به طور قابل توجهی متحول می‌کند. هوش مصنوعی به حسابرسان امکان می‌دهد تا محدودیت‌های نمونه‌گیری سنتی را پشت سر بگذارند و تحلیل جامع مجموعه‌های بزرگی از داده‌ها را تسهیل می‌کند. این بازتعریف فرآیندهای کاری حسابرسی

[1] Badiaa Amar
[2] Fagoo
[3] Al-sayyed
[4] Coderre
[5] Lenz
[6] Hahn
[7] Knechel
[8] Salterio

داخلی، قابلیت جدیدی به حسابرسان داخلی می‌دهد تا داده‌های شرکتی وسیع و پراکنده را عمدتاً از طریق اتوماتیک کردن وظایف تکراری و بهینه‌سازی رویه‌های حسابرسی فوراً پردازش کنند (گنوم[1] و آلابا [2]،۲۰۲۰ ص۲۳). طبق مطالعات انجام شده توسط بادیا عمار[3] در سال ۲۰۲۲، هوش مصنوعی به حسابرسان این امکان را می‌دهد تا بر وظایف با ارزش افزوده بالاتر، مانند تفسیر نتایج و ارائه توصیه‌های استراتژیک، تمرکز کنند. در نتیجه، هوش مصنوعی نقش حسابرس را از اجرای رویه‌ها به مشاور استراتژیک در مورد ریسک و کنترل تغییر می‌دهد (کی پی ام جی، ۲۰۱۸ و لو و همکاران[4]، ۲۰۱۸). علاوه بر این، نقش حیاتی هوش مصنوعی در افزایش تشخیص تقلب و ناهنجاری برجسته است یعنی حوزه‌ای که برای حسابرسان داخلی اهمیت ویژه‌ای دارد.

در سال‌های اخیر، گسترش فناوری‌های دیجیتال موجب تغییرات اساسی در فرآیندهای حسابرسی و نحوه انجام فعالیت‌های حسابرسان شده است. مطالعات انجام‌شده نشان می‌دهد که تحول دیجیتال با فراهم کردن امکان استفاده از فناوری‌هایی مانند تحلیل داده‌های بزرگ، اتوماسیون فرآیندها، هوش مصنوعی و سایر ابزارهای نوین، موجب تغییر رویکردهای سنتی حسابرسی و افزایش قابلیت‌های تحلیلی حسابرسان شده است. (پیزی[5] و همکاران ،۲۰۲۱ ص۱۹ ) با انجام یک تحلیل کتاب‌سنجی از مطالعات مرتبط با تحول دیجیتال در حسابرسی داخلی، نشان دادند که موضوعاتی مانند حسابرسی مستمر، تحلیل داده‌ها و فناوری‌های نوین از مهم‌ترین محورهای پژوهشی این حوزه هستند و تحول دیجیتال نقش مهمی در بازتعریف وظایف و مسئولیت‌های حسابرسان داخلی دارد. همچنین (مانیتا[6] و همکاران ، ۲۰۲۰) با بررسی تأثیر تحول دیجیتال بر حسابرسی، بیان کردند که فناوری‌های جدید علاوه بر بهبود کیفیت و اثربخشی فرآیندهای حسابرسی، موجب تغییر مهارت‌های مورد نیاز حسابرسان و افزایش اهمیت توانایی‌های فناورانه در این حرفه شده‌اند. در همین راستا، (لیو[7] و همکاران ، ۲۰۲۲ ) نیز تأکید کردند که فناوری‌های دیجیتال، سیستم‌های اطلاعاتی و ابزارهای تحلیلی پیشرفته، نقش مهمی

[1] Ghanoum
[2] Alaba
[3] Badiâa Amar
[4] Luo
5 Pizzi
6 Manita
7 Liew

در آینده حسابداری و حسابرسی ایفا خواهند کرد و حسابرسان برای حفظ اثربخشی خود در محیط جدید، نیازمند توسعه مهارت‌های مرتبط با فناوری هستند

با این حال این پیشرفت‌های فناوری، چالش‌های اخلاقی و حاکمیتی نیز ایجاد می‌کنند. همانطور که آگوستی[1] و اورتا پرز[2] (۲۰۲۲) اشاره کرده‌اند، سرعت شتابان تحول دیجیتال سازمان‌ها را ملزم به سازگاری مداوم با تقاضاهای در حال تغییر عصر دیجیتال می‌کند. عیسی[3] و همکارانش (۲۰۱۶، ص۱) بر تأثیر عمیق هوش مصنوعی بر شیوه‌های حسابرسی و نیاز فوری حسابرسان به کسب مهارت‌های جدید، به ویژه در تحلیل داده‌ها و مدیریت سیستم‌های هوش مصنوعی تأکید می‌کنند (عیسی[4]، سان[5] و واسارهلی[6] ,۲۰۱۶).

علاوه بر این، هوش مصنوعی نگرانی‌های مقرراتی و حریم خصوصی داده‌ها را ایجاد می‌کند و نقش حیاتی حسابرس را در ارزیابی ریسک‌های مرتبط با اخلاق و رعایت چارچوب‌های قانونی برجسته می‌کند (ایا[7] ,۲۰۱۷ ص۱). بنابراین از حسابرسان امروز انتظار می‌رود تا مهارت‌های تخصصی خود برای شناسایی این ریسک‌ها به ویژه آن‌هایی که شامل مبانی الگوریتمی و شفافیت در فرآیندهای خودکار هستند را توسعه دهند.

در ایران، ادغام هوش مصنوعی در حسابرسی داخلی همچنان در مراحل اولیه است. مطالعات نشان می‌دهد که بخش‌های بانکی و مخابراتی پیشرو در پیاده‌سازی هوش مصنوعی در فرآیندهای حسابرسی خود هستند. در حالی که شرکت‌های ایرانی شروع به کاوش پتانسیل هوش مصنوعی در حسابرسی داخلی کرده‌اند، پذیرش آن نسبت به کشورهای توسعه‌یافته عقب مانده است. موانع کلیدی شامل کمبود مهارت‌های مرتبط با هوش مصنوعی، هزینه‌های بالای پیاده‌سازی و مقاومت در برابر تغییر سازمانی است.

این مطالعه رویکردی زمینه‌ای[8] برای بررسی عوامل تأثیرگذار بر ادراک و اظهارنظر[9] حسابرسان داخلی نسبت به پذیرش هوش مصنوعی در رویه‌های حرفه‌ای خود اتخاذ می‌کند. با

[1] Agustí
[2] Orta-Pérez
[3] Issa
[4] Issa
[5] Sun
[6] Vasarhelyi
[7] IIA
[8] a contextualized approach
[9] perceptions and attitudes

کمک به درک عمیق‌تر از تحول دیجیتال حسابرسی داخلی، این پژوهش بینش‌های ارزشمندی برای افراد فعال در حرفه و تصمیم‌گیرندگان ارائه می‌دهد و موانع و موقعیت‌هایی را که باید برای تضمین ادغام موفق و پایدار هوش مصنوعی در شیوه‌های حسابرسی داخلی در نظر گرفته شوند را شناسایی می‌کند.

## چارچوب نظری و مفهومی

هوش مصنوعی به طور فزاینده‌ای به عنوان ابزاری ارزشمند برای افراد حرفه‌ای که به دنبال افزایش عملکرد خود هستند، ظاهر می‌شود. هوش مصنوعی، اتوماتیک کردن وظایف تکراری، تحلیل مجموعه‌های بزرگ و پیچیده‌ای از داده و تولید بینش‌های مرتبط برای حمایت از تصمیم‌گیری را امکان‌پذیر می‌کند (علی[1] و همکاران، ۲۰۲۳؛دامرجی[2] و سلیمی[3] ,۲۰۲۱). اساساً، هدف هوش مصنوعی تجهیز ماشین‌ها – به ویژه سیستم‌های کامپیوتری – به قابلیت‌های شناختی شبیه به انسان است. با ترکیب اجزای نرم‌افزاری و سخت‌افزاری، هوش مصنوعی هدفش تکرار عملکردهای مغز انسان است. با بهره‌گیری از توانایی پردازش و تحلیل مقادیر عظیم داده‌ها، هوش مصنوعی می‌تواند موقعیت‌های پیچیده را ارزیابی کند، تصمیمات آگاهانه بگیرد و وظایفی را انجام دهد که نیاز به قضاوت دارند. با این حال، تجربه انسانی به ویژه در مراحل اولیه پردازش داده‌ها و طراحی سیستم‌های حرفه‌ای همچنان ضروری است.

حرفه حسابرسی یکی از حوزه‌هایی است که بیشترین تأثیر را از افزایش هوش مصنوعی می‌پذیرد. به ویژه، هوش مصنوعی راهی برای تشخیص تقلب در حسابرسی داخلی ارائه می‌دهد. هوش مصنوعی می‌تواند از طریق قابلیت‌های تحلیل داده‌های واقعی زمان و الگوریتم‌های تشخیص الگو، شاخص‌های ظریف تقلب را که ممکن است توسط حسابرسان انسانی نادیده گرفته شود، تشخیص دهد. با دسترسی به داده‌های مرتبط، سیستم‌های هوش مصنوعی می‌توانند ریسک‌ها را ارزیابی کنند، از تصمیم‌گیری حمایت کنند و برخی وظایف مبتنی بر قضاوت را اتوماتیک کنند. همراه با پذیرش هوش مصنوعی، تکنیک‌های حسابرسی مرتبط با کامپیوتر[4] نیز برجسته شده‌اند. این ابزارها و راه‌حل‌های نرم‌افزاری به حسابرسان کمک می‌کنند تا وظایف

[1] Ali
[2] Damerji
[3] Salimi
[4] CAATTs

خود را با سیستمی کردن آزمون‌های حسابرسی، پردازش مجموعه‌های بزرگی از داده‌ها و شناسایی ناهنجاری‌ها و ریسک‌های بالقوه مؤثرتر انجام دهند. این موضوع به صرفه‌جویی در زمان و هزینه، بهبود دقت در رویه‌های حسابرسی و افزایش کارایی کلی حسابرسی کمک می‌کند (علی و همکاران، ۲۰۲۳ ;دامرجی و سلیمی، ۲۰۲۱ ص۴۵).

در تحقیقات دانشگاهی، مطالعات متعددی به بررسی نقش هوش مصنوعی در بهبود عملکرد سازمانی پرداخته‌اند. همانطور که هان[1] و همکاران (۲۰۲۳) ص۱۵ اشاره کرده‌اند، علاقه محققان به حوزه هوش مصنوعی رو به رشد است. تحقیقات در طیف وسیعی از بخش‌ها، از جمله لجستیک و مدیریت زنجیره تأمین، کنترل کیفیت، فرآیندهای تولید (هاندوکو[2] و لیوسمان[3] , ۲۰۲۱;کینکل[4] و همکاران ,.۲۰۲۲)، و همچنین تصمیم‌گیری استراتژیک، مدیریت ریسک و عملیات کسب‌وکار کلی (سیتهامراجو[5] و حکیموویچ[6] ۲۰۲۲ ;دوییودی[7] و همکارانش.۲۰۱۴ ;وارزارو[8] ,۲۰۲۲) گسترش یافته است.

در نتیجه، هوش مصنوعی حوزه‌ای پربار برای تحقیق در حوزه حسابرسی داخلی است. برای مثال چانگ[9] و همکاران (۲۰۲۱) بررسی کرده‌اند که چگونه هوش مصنوعی می‌تواند وظایف حسابرسی داخلی را اتوماتیک کند و بر پتانسیل الگوریتم‌ها برای افزایش کارایی و دقت حسابرسی و حسابداری و مالی تأکید کرده‌اند. وانگ[10] و ژانگ[11](۲۰۲۲) کاربرد هوش مصنوعی برای تشخیص ناهنجاری‌ها و تقلب در سیستم‌های مالی را بررسی کرده‌اند و مطلوبیت تکنیک‌های یادگیری ماشینی مانند شبکه‌های عصبی و جنگل‌های تصادفی را نشان داده‌اند.کائوفمن[12] (۲۰۲۲) تأثیر هوش مصنوعی بر مدیریت ریسک در فرآیندهای حسابرسی داخلی را تحلیل کرده‌اند و یافته‌اند که تحلیل‌های پیش‌بینی کننده و هشدارهای واقعی، توانایی

[1] Han
[2] Handoko
[3] Liusman
[4] Kinkel
[5] Seethamraju
[6] Hecimovic
[7] Dwivedi
[8] Varzaru
[9] Chung
[10] Wang
[11] Zhang
[12] Kaufmann

حسابرسان را برای پیش‌بینی و ارزیابی ریسک‌ها بهبود می‌بخشد. لی یو[1] و همکاران (۲۰۲۲) بر نقش در حال تکامل حسابرسان داخلی تمرکز کرده‌اند و افزایش نگرانی‌های اخلاقی و محرمانگی مرتبط با استفاده از هوش مصنوعی را برجسته کرده‌اند. به طور مشابه، سینگ[2] و پتل[3] (۲۰۲۳) کمک هوش مصنوعی به پردازش حجم بزرگ داده‌های حسابرسی را نشان داده‌اند که تحلیل سریع‌تر و دقیق‌تر را تسهیل می‌کند و شناسایی مسائل بالقوه را افزایش می‌دهد.

مطالعات قبلی که پذیرش هوش مصنوعی را بررسی کرده‌اند، معمولاً بر چارچوب‌هایی مانند چارچوب محیط-تکنولوژی-سازمان[4] یا نظریه انتشار نوآوری[5] تکیه کرده‌اند و متغیرها را محدود به زمینه خاص تحقیق خود انتخاب کرده‌اند. با این حال، در این مطالعه، متمرکز بر سطح فردی، به ویژه متمرکز بر حسابرس داخلی پیش می‌رویم. برای این منظور، از مدل‌های پذیرش سطح فردی[6] مانند مدل پذیرش فناوری[7]، نظریه رفتار برنامه‌ریزی‌شده[8] و نظریه یکپارچه پذیرش و بکارگیری فناوری[9] استفاده می‌کنیم. این مدل‌ها بینش‌های ارزشمندی در مورد عوامل روانشناختی و رفتاری که پذیرش و استفاده از هوش مصنوعی توسط حسابرسان داخلی را تحت تأثیر قرار می‌دهند، ارائه می‌دهند.

## تدوین فرضیات

این مطالعه عوامل فردی که درک و نگرش حسابرسان داخلی نسبت به پذیرش هوش مصنوعی در رویه‌های عمل خود را تحت تأثیر قرار می‌دهند، بررسی می‌کند. به طور خاص، هدف پژوهش تعیین این است که آیا هوش مصنوعی به عنوان فرصت یا تهدید برای حسابرسی داخلی تلقی می‌شود و عناصر کلیدی شکل‌دهنده این نگرش را شناسایی می‌کند.

در این پژوهش رابطه‌ای بین مزایای هوش مصنوعی و سطح پذیرش آن را پیشنهاد می‌کنیم و فرض می‌کنیم که نگرش مثبت از مزایای هوش مصنوعی با بکارگیری بیشتر از ابزارهای

---

[1] Liu
[2] Singh
[3] Patel
[4] Technology-Organization-Environment (TOE)
[5] Diffusion of Innovation (DOI)
[6] individual-level adoption models
[7] the Technology Acceptance Model (TAM)
[8] the Theory of Planned Behavior (TPB)
[9] the Unified Theory of Acceptance and Use of Technology (UTAUT)

دیجیتال در حسابرسی مرتبط است. برای رسیدن به این اهداف، مطالعه چندین بعد را بررسی می‌کند.

ابتدا، نگرش کلی حسابرسان داخلی از هوش مصنوعی را بررسی می‌کنیم - اینکه آیا فناوری به طور کلی به عنوان تسهیل‌گر یا مانع در عملکردهای حرفه‌ای آن‌ها دیده می‌شود. در سازمان‌های پیچیده با ساختارهای سلسله مراتبی و حجم بزرگ داده‌ها، هوش مصنوعی مزایای قابل توجهی مانند سهولت در بکارگیری و کاهش تلاش در انجام وظایف را برای عملکرد حسابرسی داخلی ارائه می‌دهد. سازمان‌ها با درجه بالای اتوماسیون، مزایای ملموسی در زمینه‌هایی مانند جمع‌آوری داده‌ها، انتقال، ذخیره‌سازی، کنترل و بکارگیری گزارش می‌دهند. همزمان، پیشرفت‌های فناوری مانند ذخیره‌سازی داده‌های ارزان‌قیمت از طریق فضای ابری، مدیریت مجموعه‌های گسترده از داده را تسهیل می‌کند. بنابراین هوش مصنوعی به ابزاری کلیدی برای ارزیابی کامل بودن، صحت، دقت و قابلیت اتکای داده‌ها حتی در حجم بالا و با پیچیدگی تبدیل می‌شود (ارب[1] ,۲۰۱۸ ص۳۰).

**فرضیه ۱:** هوش مصنوعی توسط حسابرسان داخلی به دلیل پتانسیل آن برای افزایش کارایی، دقت حسابرسی و مدیریت داده‌ها، به عنوان یک دارایی تلقی می‌شود.

با این حال، ادغام هوش مصنوعی در حسابرسی داخلی نگرانی‌ها و چالش‌های متعددی مانند افزایش پیچیدگی فناوری، جابجایی شغلی بالقوه به دلیل اتوماسیونی شدن و افزایش ریسک‌های امنیت داده‌ها نیز ایجاد می‌کند. با گسترش استفاده از هوش مصنوعی، ممکن است وابستگی بیشتر به فناوری، تعامل انسانی کمتر و دشواری بیشتر در فرآیندهای تشخیص ناهنجاری‌ها ایجاد شود (سیتهامراجو[2] و حکیموویچ[3] ,۲۰۲۲ ص۴۵).

چندین پژوهشگر نگرانی‌هایی بیان کرده‌اند که هوش مصنوعی ممکن است به دلیل اتوماتیک کردن فرایندهایی که هم اکنون توسط انسان‌ها انجام می‌شود، اشتغال در حرفه حسابرسی داخلی را تهدید کند (ماسپارت[4] ,۲۰۱۸ ص۱۲). طبق مطالعات مچ[5](۲۰۲۲)، برخی سازمان‌ها همچنان از پیاده سازی هوش مصنوعی امتناع کردند زیرا در خصوص احتمال از دست

[1] Erb
[2] Seethamraju
[3] Hecimovic
[4] Muspratt
[5] Mach

دادن افراد شاغل در حرفه نگران هستند، با وجود این نگرانی ها، شواهد تجربی موجود تا کنون نشان دهنده تاثیر قابل توجه استفاده از هوش مصنوعی بر جایگاه شغلی حسابرسان انسانی نیست.

با این حال، هوش مصنوعی فرصت‌های جدیدی برای حسابرسان ایجاد می کند تا بر وظایف با ارزش بالاتر که نیاز به قضاوت و بینش انسانی دارند، تمرکز کنند. فهم این پتانسیل نیاز به تغییر قابل توجه در مهارت‌ها و فرآیندهای کاری دارد. همزمان، فناوری‌هایی مانند محاسبات ابری، اگرچه برای یکپارچه سازی داده مفید هستند، چالش‌های امنیتی جدی ایجاد می کنند. پردازش خودکار مجموعه‌های بزرگی از داده، در معرض قرار گرفتن ریسک‌هایی مانند تقلب و دسترسی غیرمجاز به داده‌ها را افزایش می‌دهد (پاتهاکولام[1] و همکاران ،۲۰۲۱). تضمین رعایت اصول اخلاقی و قانونی در استفاده از داده‌ها نیاز به نظارت مقرراتی سختگیرانه دارد (ژو[2] ,۲۰۲۱).

**فرضیه ۲:** هوش مصنوعی توسط حسابرسان داخلی به دلیل نگرانی‌هایی در مورد امنیت داده‌ها، اتوماتیک کردن وظایف و پیچیدگی فناوری به عنوان تهدید تلقی می‌شود.

این مطالعه همچنین به شناسایی عوامل سطح فردی که درک حسابرسان داخلی از پذیرش هوش مصنوعی را تحت تأثیر قرار می‌دهد می‌پردازد. با بررسی این ابعاد، ما به دنبال برجسته کردن محرک‌ها و موانع پذیرش هوش مصنوعی در عملکرد حسابرسی داخلی و ارائه توصیه‌هایی برای ادغام مؤثر و پایدار آن هستیم.

درک مزایای هوش مصنوعی نقش کلیدی در شکل‌دهی تمایل حسابرسان به پذیرش آن را دارد. مجموعه این ادراک می‌تواند شامل مواردی مانند سهولت بکارگیری، مطلوبیت کاربرد، زحمات و تلاشهایی که کاسته می‌شوند و شرایط سازمانی مطلوب باشد. لونگ[3] (۲۰۱۳) مزایای درک شده را به عنوان شناخت کاربران از ارزش مرتبط با فناوری تعریف می کند. مطالعات تجربی(هارما[4] و همکاران ,۲۰۱۷;کیم[5] و همکاران ،۲۰۰۹ ;پدروسا[6] و همکاران، ۲۰۲۰) بیان نمودند که این ادراک بطور معناداری بر قصد حسابرسان برای بکارگیری ابزار دیجیتال اثر می گذارد.

[1] Puthukulam
[2] Zhou
[3] Leung
[4] Dharma
[5] Kim
[6] Pedrosa

**فرضیه ۳:** درک شدن مزایای هوش مصنوعی، مانند سهولت بکارگیری، سودمندی و کاهش تلاش‌های انسانی بطور مثبت بر انتخاب هوش مصنوعی در حسابرسی داخلی اثرگذار است.

در نهایت، پژوهش حاضر نقش آموزش و سطح مهارت در شکل‌دهی ادراک حسابرسان از هوش مصنوعی را بررسی می‌کند. حسابرسان با آموزش فنی قوی و تجربه قبلی در هوش مصنوعی، احتمال بیشتری دارد که هوش مصنوعی را به عنوان ابزاری ارزشمند و قابل اتکا که کیفیت حسابرسی را بهبود می‌بخشد و از تصمیم‌گیری آگاهانه‌تر حمایت می‌کند، درک کنند. درک بهتر سیستم‌های هوش مصنوعی، پذیرش ابزار و ادغام یکنواخت‌تر در جریان کارهای حسابرسی را تشویق می‌کند.

برعکس، آموزش یا تجربه محدود ممکن است به ادراک منفی منجر شود. هوش مصنوعی ممکن است بیش از حد پیچیده، دشوار برای پیاده‌سازی یا فاقد ارزش افزوده دیده شود و در نهایت این موضوع، پذیرش هوش مصنوعی را به تعویق بیاندازد. بنابراین، سطح مهارت حسابرس معیاری کلیدی در نحوه درک مزایا و محدودیت‌های هوش مصنوعی است. آموزش کافی به کاهش موانع فنی، کاهش اشتباهات و افزایش اعتماد در نتایج تولیدشده توسط هوش مصنوعی کمک می‌کند.

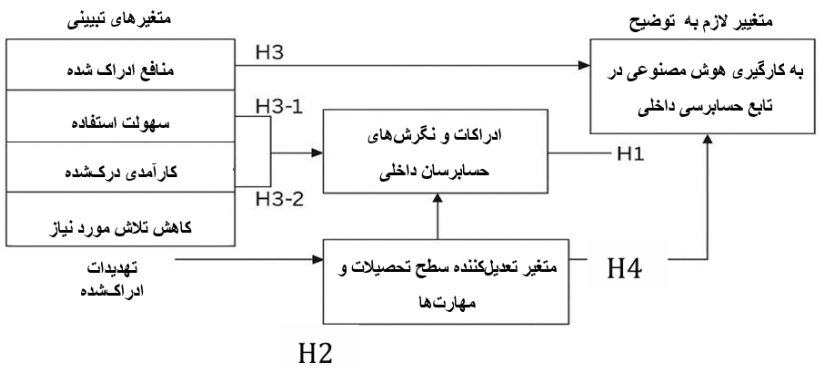
**فرضیه ٤:** سطح آموزش و مهارت‌های مرتبط با هوش مصنوعی حسابرسان داخلی، درک و اشتیاق آن‌ها برای پذیرش این فناوری را تحت تأثیر قرار می‌دهد.

## ارائه یک مدل مفهومی پژوهشی برای تحول دیجیتال وظیفه حسابرسی داخلی

این پژوهش با هدف تبیین وضعیت کنونی به‌کارگیری هوش مصنوعی در حسابرسی داخلی انجام شده و تمرکز آن بر ادراکات و نگرش‌های حسابرسان داخلی نسبت به این فناوری است.

مدل مفهومی پیشنهادی ما با هدف بررسی عوامل فردی مؤثر بر ادراکات و نگرش‌های حسابرسان داخلی نسبت به پذیرش هوش مصنوعی در فعالیت حرفه‌ای آنان توسعه یافته است. این مدل بر این ایده استوار است که ادراک هوش مصنوعی به‌عنوان یک فرصت یا یک تهدید، عمدتاً به منافع ادراک‌شده (مانند سهولت استفاده، کارایی عملکردی و کاهش میزان تلاش)،

ریسک‌های ادراک‌شده (مانند پیچیدگی فناورانه، امنیت داده‌ها و خودکارسازی مشاغل) و همچنین سطح آموزش و مهارت حسابرسان در حوزه هوش مصنوعی بستگی دارد. در این راستا، فرضیه ۱ بیان می‌کند که هوش مصنوعی به دلیل توانایی آن در بهبود کارایی، دقت حسابرسی و مدیریت داده‌ها، به‌عنوان یک دارایی ادراک می‌شود، در حالی که فرضیه ۲ مطرح می‌سازد که این فناوری می‌تواند به‌واسطه ریسک‌های فناورانه، امنیتی و انسانی به‌عنوان یک تهدید تلقی شود. این مدل فرض می‌کند که هرچه منافع ملموس‌تری از به‌کارگیری هوش مصنوعی توسط حسابرسان ادراک شود، تمایل آنان به پذیرش این فناوری افزایش می‌یابد (فرضیه ۳)؛ در مقابل، نگرانی‌های مرتبط با ریسک می‌تواند به‌عنوان عاملی بازدارنده در مسیر پذیرش عمل کند. افزون بر این، فرضیه ۴ استدلال می‌کند که دانش و تجربه در زمینه هوش مصنوعی تأثیر قابل‌توجهی بر این ادراکات دارد و با ایفای نقشی تعدیل‌گر و اساسی، به تسهیل در پذیرش مثبت‌تر این فناوری کمک می‌کند. بدین‌ترتیب، این مدل امکان تحلیل اهرم‌ها و موانع پذیرش هوش مصنوعی در وظیفه حسابرسی داخلی را فراهم می‌سازد و در عین حال، پویایی‌های فردی و سازمانی را به‌طور هم‌زمان در نظر می‌گیرد.



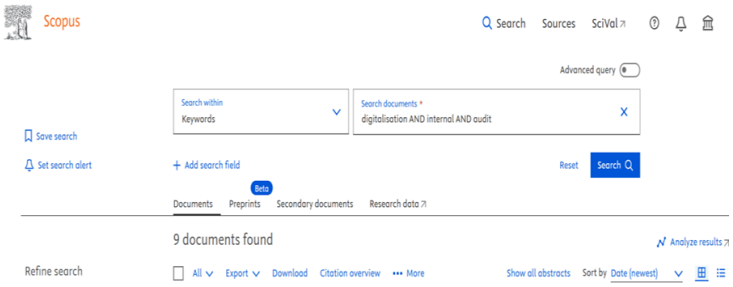

**نگاره ۱.** مدل مفهومی پژوهش برای عوامل مؤثر بر ادراکات و نگرش‌های حسابرسان داخلی نسبت به پذیرش هوش مصنوعی

## روش‌شناسی پژوهش

رویکرد کیفی یک روش پژوهشی دقیق و نظام‌مند است که با هدف دستیابی به درکی عمیق از پدیده‌های مورد مطالعه به کار گرفته می‌شود. این رویکرد به‌جای کمّی‌سازی پدیده‌ها، بر کاوش پویایی‌های زیربنایی آن‌ها تمرکز دارد و بدین‌ترتیب به پاسخ‌گویی به پرسش‌های «چرا» و «چگونه» کمک می‌کند (دامز[1]، ۲۰۱۱: ۱).

با وجود آن‌که ادغام این رویکرد در علوم مدیریتی در مقایسه با ریشه‌های آن در علوم انسانی و اجتماعی نسبتاً جدید است، استفاده ازاین روش در حال افزایش است. در این راستا، گارسیا[2] و گلوسینگ[3] (۲۰۱۳) به افزایش قابل‌توجه تعداد انتشارات حوزه علوم مدیریتی که از روش‌های کیفی طی چند دهه اخیر استفاده می‌کنند اشاره می‌کنند. این روند نه‌تنها بیانگر علاقه روزافزون به این رویکرد است، بلکه نشان‌دهنده کارآمدی آن در درک پیچیدگی پدیده‌ها در این حوزه علمی نیز می‌باشد.

در چارچوب این پژوهش، به‌منظور بررسی و تبیین دقیق‌تر دو مفهوم حسابرسی داخلی و دیجیتالی‌سازی، مرور ادبیات موجود انجام شد. بدین منظور، یک مرور نظام‌مند از انتشارات علمی نمایه‌شده در پایگاه داده اسکوپوس[4] صورت گرفت که در نهایت منجر به انتخاب ۹ مقاله گردید. شکل زیر پروتکل انتخابی را نشان می‌دهد که به تشکیل نمونه نهایی پژوهش انجامیده است.




**نگاره۲.** شیوه انتخاب نمونه

[1] Dumez
[2] Garcia
[3] Glusing
[4] Scopus

بررسی‌ها در بازه زمانی ۲۰۲۰ تا ۲۰۲۵ است تا چارچوب زمانی نسبتاً گسترده‌ای برای درک روند تکاملی بلندمدت مفهوم مورد مطالعه فراهم شود. در این دوره، شاهد رشد چشمگیر انتشار مقالات علمی مرتبط با تحول دیجیتال و حسابرسی داخلی بوده‌ایم، که این امر عمدتاً به دلیل ظهور ابزارهای دیجیتال مانند هوش مصنوعی و چت جی پی تی پس از بحران بهداشتی کووید-۱۹ است، که زمینه را برای ظهور تحقیقات علمی در حوزه حسابرسی فراهم کرد.

این فرآیند انتخاب با بهره‌گیری از معیارهای ورود و خروج انجام شد تا اطمینان حاصل شود که نمونه انتخاب‌شده نماینده مناسبی از پژوهش‌ها و مشارکت‌ها در حوزه حسابرسی داخلی باشد. جدول زیر پروتکل تشکیل نمونه ما را به‌صورت روشن نشان می‌دهد.

**جدول ۱**

*جدول مولفه‌ها و معیارهای ورود نمونه*

| مولفه‌ها | معیارهای ورود | معیارهای خروج |
|---|---|---|
| نوع سند | مقالات ژورنالی و مقالات کنفرانسی | کتاب‌ها، رساله‌ها و پایان‌نامه‌های دکتری |
| کیفیت منبع | مقالات استخراج شده از پایگاه داده اسکوپوس | منابع غیرمرتبط با موضوع و زمینه هدف |
| هدف | مطالعاتی که به بررسی ادبیات موجود می‌پردازند | سایر |
| رویکرد روش‌شناسی | مرورهای ادبیات، مطالعات کیفی یا کمی | سایر |
| محتوا | اصالت پژوهش | محتوای غیرابتکاری یا تکراری |
| زبان | فقط انتشارات به زبان انگلیسی | سایر زبان‌ها |
| بازه زمانی | ۲۰۲۰ تا ۲۰۲۵ | |

در این مطالعه، بررسی سیستماتیک بر اساس تحلیل متنی، جغرافیایی و زمانی انجام شد تا درک روشن‌تری از مفهوم پژوهشی مورد بررسی به دست آوریم.

## نتایج و بحث

### تحلیل متنی

تحلیل متنی یک روش کیفی برای مطالعه، تفسیر و ارزیابی عمیق یک متن یا مجموعه‌ای از متون است. این روش به ما امکان می‌دهد تا درک کنیم که نویسنده چگونه استدلال‌های خود را به‌ویژه از طریق استفاده از اصطلاحات تخصصی سازماندهی می‌کند، (مصباحی[1] و همکاران، ۲۰۲۴). این رویکرد دامنه گسترده‌ای دارد و ابعاد مفهومی، نظری و عملی را در بر می‌گیرد (همان منبع). در پژوهش حاضر، بر بررسی واژگان کلیدی موجود در چکیده مقالات تمرکز شد تا پرتکرارترین اصطلاحات در حوزه حسابرسی داخلی شناسایی شوند.

جدول زیر نتایج تحلیل فراوانی این واژگان کلیدی را خلاصه می‌کند.

**جدول ۲**

*تحلیل واژگان کلیدی مرتبط با دیجیتالی شدن عملکرد حسابرسی داخلی*

| کلمه کلیدی | تکرار (تعداد ارجاعات) |
|---|---|
| حسابرسی داخلی | ۷ |
| دیجیتالی‌سازی | ۷ |
| تحلیل داده‌ها | ۴ |
| هوش مصنوعی | ۳ |
| عملکرد حسابرسی داخلی | ۲ |
| یادگیری ماشینی | ۱ |
| فناوری‌های دیجیتال | ۱ |
| پلتفرم‌های دیجیتال | ۱ |

تنها آن دسته از واژگان کلیدی در نظر گرفته شد که به حوزه و زمینه دیجیتالی‌سازی عملکرد حسابرسی داخلی مرتبط باشند، به همین دلیل تحلیل واژگان نشان‌دهنده غلبه واژگان «حسابرسی داخلی» و «دیجیتالی‌سازی» است. در کنار «حسابرسی داخلی»، سه مفهوم کلیدی

[1] Mesbahi

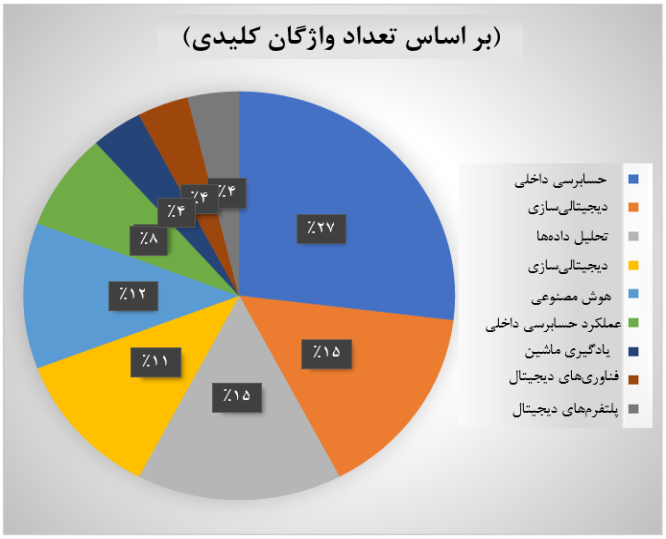
دیگر نیز با فراوانی قابل توجه مشاهده می‌شوند: «تحلیل داده‌ها»، «هوش مصنوعی» و «عملکرد حسابرسی داخلی».




**نگاره ۳:** ابر مفاهیم کلیدی مرتبط با دیجیتالی‌سازی و حسابرسی داخلی[1]

علاوه بر این، از شکل زیر می‌توان مشاهده کرد که برخی واژگان نسبت به برخی دیگر کمتر تکرار شده‌اند. در این راستا، مفاهیم «یادگیری ماشینی»، «پلتفرم دیجیتال» و «فناوری‌های دیجیتال» کمترین فراوانی را در اصطلاحات مورد بررسی در مطالعه حاضر دارند.

[1] منبع: Generated par WordArt




**نگاره ٤:** تحلیل واژگان کلیدی مرتبط با دیجیتالی‌سازی عملکرد حسابرسی داخلی در بازه زمانی ۲۰۰۰ تا ۲۰۲۵

## تحلیل زمانی

تحلیل زمانی، روند تکامل تحقیقات در یک موضوع خاص را بررسی می‌کند. این رویکرد کیفی، شاخصی مرجع برای خوانندگان فراهم می‌آورد و به آن‌ها امکان می‌دهد تا روندها و تغییرات حوزه حسابرسی داخلی را در یک بازه زمانی مشخص شناسایی کنند (مصباحی و همکاران، ۲۰۲۴).

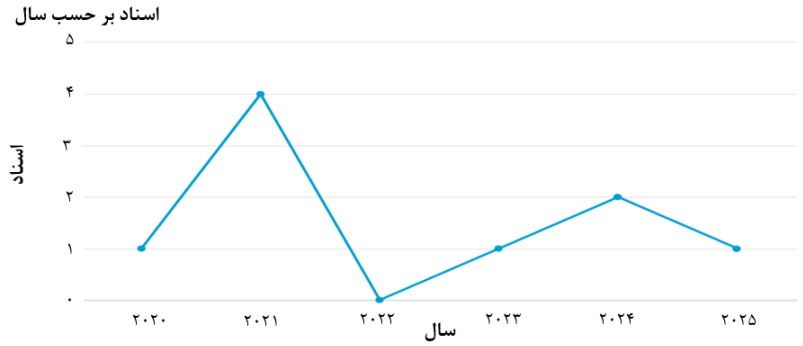
برای این منظور، همان‌طور که در جدول زیر نشان داده شده است در پژوهش حاضر یک بازه زمانی پنج ساله انتخاب شد.

## جدول ۳

*تحلیل زمانی پژوهش‌ها درباره دیجیتالی‌سازی عملکرد حسابرسی داخلی*

| تعداد مقالات | دوره |
|---|---|
| ۱ | ۲۰۲۰ |
| ۴ | ۲۰۲۱ |
| ۰ | ۲۰۲۲ |
| ۱ | ۲۰۲۳ |
| ۲ | ۲۰۲۴ |
| ۱ | ۲۰۲۵ |
| ۹ | مجموع |

از جدول فوق نموداری تهیه شد که روند تکامل پژوهش‌ها درباره دیجیتالی‌سازی عملکرد حسابرسی داخلی را در بازه‌های زمانی مختلف نشان می‌دهد. از نگاره شماره ۵ مشخص می‌شود که سال ۲۰۲۱ به‌عنوان سال مرجع برای شدت گرفتن پژوهش‌ها در زمینه دیجیتالی‌سازی عملکرد حسابرسی داخلی بوده و پس از آن سال ۲۰۲۴ قرار دارد. با این حال، سال ۲۰۲۲ سالی بود که هیچ مقاله‌ای در حوزه دیجیتالی‌سازی عملکرد حسابرسی داخلی منتشر نشد و پس از این سال ابزارهای فناوری متعددی مانند چت جی پی تی و دیپ سیک[1] ظهور کردند.



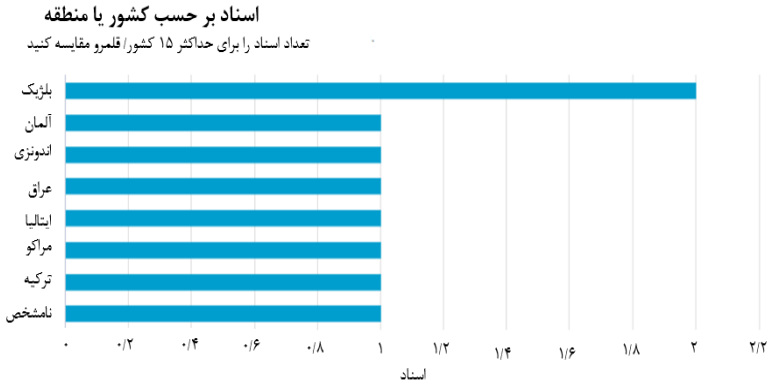

**نگاره ۵.** تحلیل زمانی پژوهش‌ها درباره دیجیتالی‌سازی عملکرد حسابرسی داخلی در بازه زمانی ۲۰۰۰ تا ۲۰۲۵

## تحلیل جغرافیایی

تحلیل جغرافیایی مقالات علمی فهرست‌شده در پایگاه داده اسکوپوس، به ما امکان داد تا مناطقی را که این مفهوم در آن‌ها بیشترین توسعه و گسترش را یافته است، بهتر شناسایی کنیم.

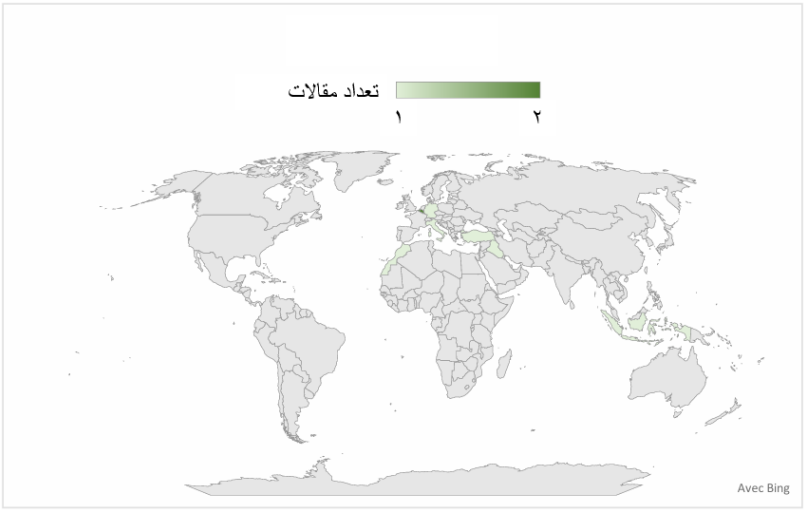
از این منظر، نمودار زیر کشورهایی را که از نظر تولید علمی در این موضوع برجسته هستند، نشان می‌دهد.

[1] DeepSeek




**نگاره ٦.** تحلیل جغرافیایی پژوهش‌ها درباره دیجیتالی‌سازی عملکرد حسابرسی داخلی[1]

از این شکل می‌توان مشاهده کرد که بلژیک کشوری هست که بیشترین تعداد مقالات علمی را در زمینه دیجیتالی‌سازی عملکرد حسابرسی داخلی دارد، و پس از آن آلمان، اندونزی و عراق قرار دارند.



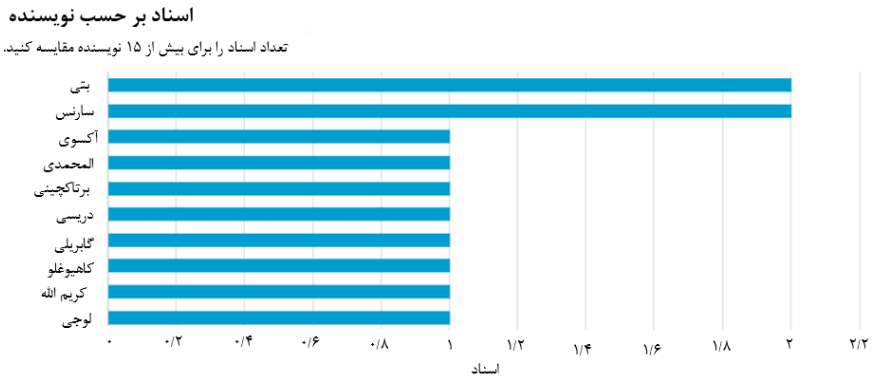

**نگاره ۷.** پراکندگی مقالات علمی منتشرشده بر اساس کشور در زمینه دیجیتالی‌سازی حسابرسی داخلی در بازه زمانی ۲۰۲۰ تا ۲۰۲۵

[1] منبع: Scopus

از نگاره شماره ۷ می‌توان پراکندگی مقالات علمی در سراسر جهان، به‌ویژه در زمینه حسابرسی داخلی و دیجیتالی‌سازی در بازه زمانی ۲۰۲۰ تا ۲۰۲۵ را مشاهده کرد.

**تحلیل بر اساس نویسندگان**

این تحلیل به ما امکان می‌دهد تا روابط همکاری بین نویسندگان وارد شده در پایگاه اسکوپوس را به تصویر بکشیم. مطابق شکل و با مرور پایگاه داده استخراج‌شده از اسکوپوس، مقاله‌ای که موضوع همکاری بوده و به طور گسترده مورد ارجاع و تحلیل قرار گرفته است، توسط دو نویسنده با نام‌های بتی ناتانل[1] و سارنس گریت[2] در سال ۲۰۲۱ در مجله حسابداری و تغییر سازمانی[3]، با عنوان «درک عملکرد حسابرسی داخلی در محیط کسب‌وکار دیجیتالی‌شده» منتشرشده که در مجموع ۴۸ مرتبه مورد ارجاع قرار گرفته است.




**نگاره ۸.** تعداد مقالات منتشرشده بر اساس نام نویسنده در بازه زمانی ۲۰۲۰ تا ۲۰۲۵ درباره دیجیتالی‌سازی عملکرد حسابرسی داخلی

[1] Nathanaël
[2] Gerrit
[3] Journal of Accounting and Organizational Change

## یافته‌ها

نتایج این مرور کیفی ادبیات نشان‌دهنده افزایش علاقه جامعه علمی به یکپارچه‌سازی هوش مصنوعی در حوزه حسابرسی داخلی است. تحلیل تأثیرگذارترین مقالات، چندین مسیر اصلی پژوهشی را که در حال حاضر شکل دهنده این حوزه هستند، برجسته می‌کند.

یافته‌ها روندی قابل توجه مربوط به خودکارسازی وظایف حسابرسی داخلی از طریق فناوری‌های مبتنی بر هوش مصنوعی را نشان می‌دهد که فرضیه ۱ را تایید می‌کند. پژوهش پرارجاع چانگ[1] و همکاران (۲۰۲۱) به نقش الگوریتم‌های هوشمند در بهبود کارایی عملیاتی و دقت حسابرسی‌های مالی و حسابداری اشاره می‌کند. این روند، تکامل حسابرسی داخلی را به سمت مدلی نشان می‌دهد که بیشتر بر عملکرد، سرعت و قابلیت اطمینان کنترل‌ها تمرکز دارد.

مرور ادبیات نشان‌دهنده تمرکز بر مطالعات شناسایی ناهنجاری‌ها و تقلب از طریق هوش مصنوعی است. پژوهش‌های وانگ[2] و ژانگ[3] (۲۰۲۲)، که از تکنیک‌های یادگیری ماشینی مانند شبکه‌های عصبی و جنگل‌های تصادفی استفاده می‌کنند، بازتاب گسترده‌ای یافته‌اند. این رویکرد نشان‌دهنده پتانسیل هوش مصنوعی در تقویت نقش پیشگیرانه و کشف‌کننده حسابرسی داخلی در زمینه سیستم‌های اطلاعات مالی است.

مقالات اخیر مورد بررسی در مرور ادبیات پژوهش بر شناخت نقش استراتژیک هوش مصنوعی در مدیریت ریسک همگرایی دارند و بنابراین فرضیه ۳ تایید می‌شود. در این راستا، کائوفمن[4] و همکاران (۲۰۲۲) نشان می‌دهند که قابلیت‌های پیش‌بینی هوش مصنوعی ابزارهای جدیدی در اختیار حسابرسان داخلی قرار می‌دهد تا ریسک‌های نوظهور را پیش‌بینی کرده و هشدارهای لحظه‌ای تولید کنند. این پیشرفت، بعد پیشگیرانه حسابرسی را تقویت می‌کند، که اکنون بر پیش‌بینی و پایش مستمر متمرکز است.

علاوه بر این، چندین مقاله شناسایی‌شده، به‌ویژه توسط لی یو[5] و همکاران (۲۰۲۲) و بتی ناتانل[6] و سارنسگریت[7]، بر تغییر نقش حسابرس داخلی در عصر هوش مصنوعی تمرکز دارند. نویسندگان بر لزوم کسب مهارت‌های فناورانه جدید و همچنین مسائل اخلاقی و محرمانگی که با

[1] Chung
[2] Wang
[3] Zhang
[4] Kaufmann
[5] Liu
[6] Nathanaël
[7] Gerrit

به‌کارگیری این ابزارها همراه است، تأکید می‌کنند و این موضوع فرضیه ۴ را تایید می‌کند. این یافته‌ها تغییر عمیقی را در پروفایل‌ها و شیوه‌های کاری حسابرسان نشان می‌دهند، به‌طوری که آن‌ها ملزم به ترکیب تخصص کسب‌وکار با مهارت‌های دیجیتال هستند.

از زاویه تئوریک، نتایج پژوهش تنوعی از چارچوب‌ها را نشان می‌دهد. در حالی که مدل‌هایی مانند چارچوب محیط-تکنولوژی-سازمان یا نظریه انتشار نوآوری در مطالعات سطح سازمانی غالب هستند، نتایج بررسی‌ها افزایش علاقه به مدل‌هایی را نشان داد که بر فرد متمرکزند. به‌ویژه، نظریه‌هایی مانند مدل پذیرش فناوری، نظریه رفتار برنامه‌ریزی‌شده و نظریه یکپارچه پذیرش و بکارگیری فناوری برای بررسی عوامل روان‌شناختی و رفتاری مؤثر بر پذیرش هوش مصنوعی توسط حسابرسان داخلی به‌کار گرفته می‌شوند. این امر نشان‌دهنده تغییر رویکرد در پرسش‌های علمی از پذیرش فناوری در سطح کلان به درک دقیق‌تر از عوامل فردی مؤثر بر پذیرش هوش مصنوعی در شیوه‌های حسابرسی است.

در خصوص فرضیه ۲ اطلاعاتی یافت نشد و بطور کلی، نتایج این مطالعه نشان می‌دهد که تحلیل رابطه بین دو مفهوم هوش مصنوعی و حسابرسی داخلی در ادبیات موجود هنوز به‌طور کافی مورد بررسی قرار نگرفته است. این خلا، نیاز به انجام مطالعات تجربی عمیق را برای شناسایی، ساختاربندی و اعتبارسنجی بهتر این رابطه و در نتیجه غنی‌سازی درک نظری و عملی از این حوزه برجسته می‌کند.

## نتیجه‌گیری

در پایان، دیجیتالی‌سازی امروزه به‌عنوان یک اهرم استراتژیک حیاتی برای توسعه حسابرسی داخلی مطرح است. این روند نه‌تنها کارایی وظایف حسابرسی را افزایش می‌دهد، بلکه اهمیت آن‌ها را در مواجهه با محیط‌های سازمانی روزافزون پیچیده تقویت می‌کند. یکپارچه‌سازی فناوری‌هایی مانند هوش مصنوعی، تحلیل داده‌ها، فرآیندهای رباتیک (RPA) و سیستم‌های اطلاعاتی یکپارچه، شیوه‌های حسابرسی را به‌طور عمیقی متحول کرده و دیدگاهی پیشگیرانه، مستمر و لحظه‌ای نسبت به ریسک‌ها ارائه می‌دهد.

بنابراین، دیجیتالی‌سازی باعث پوشش بهتر حوزه‌های ریسک، افزایش ظرفیت تحلیل پیش‌بینی و صرفه‌جویی در زمان و اطمینان در پردازش اطلاعات می‌شود. همچنین به بازتعریف نقش حسابرس داخلی به‌عنوان بازیگری کلیدی در حاکمیت شرکتی کمک می‌کند و امکان ارائه

توصیه‌های مرتبط‌تر و استراتژیک‌تر را برای حسابرسان فراهم می‌آورد. با این حال، این تحول نیازمند ارتقای مهارت‌های تیم‌های حسابرسی و همچنین تطبیق چارچوب‌های مرجع، ابزارها و رویکردهای روش‌شناختی است. به این ترتیب، دیجیتالی‌سازی صرفاً یک فرصت فناورانه نیست، بلکه یک جریان واقعی مدرن‌سازی و ایجاد ارزش برای عملکرد حسابرسی داخلی است که در خدمت بهبود عملکرد و تاب‌آوری سازمان‌ها قرار دارد.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## References

Adhikari, S. (2021). Impact of automation on auditing jobs: Threats and opportunities. Journal of Accounting and Finance, 21(4), 55–70.

Ali, M., Johnson, P., & Lee, S. (2023). AI for auditing: Automating audit processes with machine learning and NLP. Maramar Institute Research. https://doi.org/10.1234/lamarr.ai.audit.2023

Al-Sayyed, R., Al-Haddad, S., & Al-Khatib, K. (2021). Organizational benefits of adopting AI: Financial and operational impacts. Journal of Business Research, 134, 123–134. https://doi.org/10.1016/j.jbusres.2021.05.012

Chung, I., Kim, H., & Park, S. (2021). Automation of internal audit tasks through AI algorithms. International Journal of Auditing Technology, 7(3), 145–162.

Coderre, D. (2015). audit dones on environnement economic. Editions Economica.

Damerji, H., & Salimi, F. (2021). Audit assiste par ordinateur et intelligence artificielle : automatisation et analyse de données. Revue Francophone d'Audit et de Contrôle, 12(3), 45–60.

Dharmawansa, W., Wijaya, H., & Santoso, B. (2017). Electronic audit adoption: The role of perceived benefits and organizational factors. International Journal of Auditing, 21(1), 34–48. https://doi.org/10.1111/ijau.12095

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2014). Research on applications in business management and decision-making: A systematic review. International Journal of Information Management, 34(3), 235–244. https://doi.org/10.1016/j.ijinfomgt.2014.02.002

Erb, C. (2018). Artificial intelligence and data management in internal auditing. Internal Auditing Journal, 33(2), 30–38.

Han, J., Smith, A., & Kumar, R. (2023). The role of AI in improving organizational performance: A cross-sectoral review. Journal of Business Analytics, 6(1), 15–32.

HRF (Human Resource Forum). (2022). The future of auditing in the era of AI. HRF White Paper Series, 5, 1–20.

IIA (Institute of Internal Auditors). (2017). Guidelines on ethics and data privacy in internal audit. The Institute of Internal Auditors.

Issa, H., Sun, T., & Vasarhelyi, M. (2016). The impact of artificial intelligence on auditing: Challenges and opportunities. Journal of Emerging Technologies in Accounting, 13(2), 1–15. https://doi.org/10.2308/jeta-10557

Kaufman, D., Lee, H., & Chen, S. (2022). AI and risk management in internal audit: Predictive analytics and real-time alerts. International Journal of Auditing, 26(2), 210–225. https://doi.org/10.1111/ijau.12245

Kim, S., Park, J., & Lee, K. (2009). Technology acceptance in auditing: The influence of perceived usefulness and ease of use. Auditing: A Journal of Practice & Theory, 28(2), 113–135. https://doi.org/10.2308/aud.2009.28.2.113

Kinkel, S., Müller, J., & Weber, T. (2022). Factors influencing AI integration in manufacturing industries. Journal of Manufacturing Systems, 62, 123–134. https://doi.org/10.1016/j.jmsy.2022.04.008

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122. https://doi.org/10.2308/jeta-51722

Leung, L. (2013). Perceived benefits and technology adoption: A review. Journal of Information Technology, 28(3), 198–210. https://doi.org/10.1057/jit.2013.8

Liu, Y., Zhang, W., & Chen, L. (2022). Evolution of internal auditors' roles with AI adoption: Technical skills and ethical challenges. Accounting Horizons, 36(3), 45–63. https://doi.org/10.2308/acch-2022-0123

Mach, T. (2022). Barriers to AI adoption in auditing: Employee concerns and organizational hesitations. Journal of Business Ethics, 175(4), 789–805. https://doi.org/10.1007/s10551-020-04611-5

Mesbahi, M. (2024). Audit quality: Qualitative literature review. AME Review, 6(2), 162–185.

Muspratt, A. (2018). Automation and job displacement in internal audit. Accounting Today, 32(7), 12-15.

Pedrosa, A., Silva, M., & Costa, F. (2020). Determinants of IT adoption in auditing practices. Journal of Accounting and Technology, 14(2), 101–117.

Puthukulam, M., Singh, R., & Kumar, A. (2021). Data security challenges in AI-driven auditing. Journal of Cybersecurity and Privacy, 1(3), 245–260. https://doi.org/10.3390/jcp1030015

Seethamraju, R., & Hecimovic, A. (2022). Artificial intelligence in auditing: Benefits and risks. International Journal of Auditing, 26(1), 45–62. https://doi.org/10.1111/ijau.12240

Seethamraju, R., & Hecimovic, A. (2022). Enhancing audit efficiency and effectiveness with artificial intelligence. Journal of Accounting and Auditing, 38(4), 210–230.

Singh, S., & Patel, R. (2023). Big data analytics and AI in internal audit: Accelerating problem identification. Journal of Emerging Technologies in Accounting, 20(1), 75–90. https://doi.org/10.2308/jeta-2023-005

Tableau, J. (2021). Automation and employment trends in auditing. Accounting Review, 96(5), 123-138.

Varzaru, A. (2022a). AI in risk management and strategic decision-making. Risk Management Review, 15(2), 100–115.

Varzaru, A. (2022b). Advanced AI techniques for enterprise management. Journal of Enterprise Information Management, 35(5), 1234–1250. https://doi.org/10.1108/JEIM-09-2021-0387

Wang, X., & Zhang, Y. (2022). Using AI for anomaly and fraud detection in financial systems: Machine learning approaches. Expert Systems with Applications, 200, 117029. https://doi.org/10.1016/j.eswa.2022.117029

Yakimova, E. (2020). The impact of AI on auditing workforce: A critical review. Journal of Accounting and Organizational Change, 16(4), 589–605. https://doi.org/10.1108/JAOC-01-2020-0006

Zhou, Y. (2021). Regulatory frameworks for AI in data management and auditing. Journal of Business Ethics, 170(2), 267–283. https://doi.org/10.1007/s10551-019-04256-0

Pizzi, S., Venturelli, A., Variale, M., & Macario, G. P. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. Technological Forecasting and Social Change, 172, 121057. https://doi.org/10.1016/j.techfore.2021.121057

Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The digital transformation of external audit and its impact on corporate governance. Technological Forecasting and Social Change, 150, 119751. https://doi.org/10.1016/j.techfore.2019.119751

Liew, A., O'Leary, D. E., Perdana, A., & Wang, T. (2022). Digital transformation in accounting and auditing: 2021 international conference of the Journal of Information Systems panel discussion. Journal of Information Systems, 36(3), 1–20. https://doi.org/10.2308/ISYS-2022-008

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Review Paper**

# Opening the Black Box: A Framework for Auditor Assurance Over the Explainability of AI Decisions in IT Risk Governance [1]

**Farzad Evani [*2] and Donya Kazemi[3]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 159-186

Received: 2026.08.20
Revised: 2026.10.10
Accepted: 2026.10.28

## Abstract

As organizations increasingly rely on artificial intelligence (AI) systems for decisions such as fraud detection and credit risk scoring, auditors face a growing challenge: how to provide professional assurance over decisions produced by opaque, "black-box" models. While traditional IT audit frameworks focus mainly on the accuracy and efficiency of system outputs, explainability has received comparatively little attention as an independent dimension of AI risk governance. This conceptual, literature-based study examines the position of AI explainability within IT governance frameworks (COBIT), the ISO/IEC 42001 standard, and international audit assurance standards. The review finds that Iranian domestic literature treats AI mainly as a tool to improve audit accuracy and judgment quality, while international literature and standard-setters are rapidly moving toward requiring explainability and algorithmic accountability. Based on this gap, the study proposes a three-layer conceptual framework — technical transparency, governance documentation, and assurance reporting — to guide auditors' evaluation of AI explainability, offering a foundation for future empirical research and practical guidance for Iranian IT auditors.

**Keywords**: Explainable AI (XAI), IT Risk Governance, Audit Assurance, Algorithmic Accountability, AI Governance.

**JEL classification:** *M42, M15, O33.*

---

[1] https://doi.org/10.22034/JISTA.2026.603372.1107
[1] Selected paper of the 2nd National Conference on Corporate Governance and Information Technology Risk Management
[2] Assistant Professor, Department of Accounting, Faculty of Economics and Accounting, Razi University, Kermanshah, Iran. (Corresponding Author). Email: feivani@gmail.com
[3] M.A. in Accounting, Faculty of Economics and Accounting, Razi University, Kermanshah, Iran .Email: kazemidonya95@gmail.com

## 1. INTRODUCTION

Over the past decade, artificial intelligence has moved from a supporting analytical tool to a central driver of organizational decision-making. Machine learning systems are now used for financial fraud detection, credit risk assessment, customer scoring, and audit risk prediction. This expansion, while offering clear gains in speed and accuracy, raises a fundamental question for the audit profession: when an organizational decision emerges from a model whose internal logic even its designers cannot fully explain, on what basis can an auditor provide assurance over the correctness, fairness, and reliability of that decision? This phenomenon — commonly referred to as the "black box" problem — is not merely a technical issue but a governance one. IT governance frameworks such as COBIT, which have traditionally focused on strategic alignment, risk management, and value creation, must now respond to a new dimension: algorithmic explainability. At the regulatory level, ISO/IEC 42001, introduced in late 2023, is the first formal management-system standard dedicated to AI, and comparative research (McIntosh et al., 2024) shows it offers broader coverage of generative-AI opportunities than earlier frameworks such as COBIT and ISO 27001, though gaps remain in risk oversight. International audit standard-setters have also responded: the IAASB's October 2024 Technology Position committed the board to a gap analysis of existing standards against emerging technologies, followed by a 2025 Technology Quality Management initiative and global roundtables with over 240 stakeholders from six continents. In Iran, by contrast, existing research on AI and auditing has concentrated mainly on improving audit quality, modeling auditor judgment, and analyzing management ability, with little attention to the transparency of the decision-making process itself. This gap motivates the present study, whose central research question is: in the absence of standardized criteria for assessing AI explainability, on what basis can an IT auditor provide valid assurance?

## 2. MATERIALS AND METHODS

This study adopts a qualitative, conceptual research design based on a systematic review of domestic (Iranian) and international literature. The search strategy combined keywords such as "explainable AI," "AI governance," "IT audit," "COBIT," and "algorithmic assurance" across Iranian peer-reviewed accounting and IT-management journals and international databases indexed in Scopus and Web of Science, including arXiv, ScienceDirect, and Frontiers. Inclusion criteria required publication in a peer-reviewed journal or conference proceedings and direct relevance to one of three themes: AI explainability, IT governance frameworks, or audit assurance. Selected sources were organized into domestic and international categories to make the gap between the two literatures explicit and were then analyzed and compared to identify the main conceptual and practical divergences. Because the study is conceptual rather than empirical, no primary field data (e.g., survey or interview data) were collected; the objective is to synthesize existing knowledge into a framework capable of guiding future empirical research.

## 3. RESULTS AND DISCUSSION

The review's first finding confirms a gap between domestic and international literature: while Iranian studies (e.g., Sahat Barmecheh et al., 2025; Shah Sahebi et al., 2020; Ahmad Hossein et al., 2024) treat AI mainly as a tool for improving audit judgment, management-ability analysis, or bank performance evaluation, international literature and standard-setters are rapidly defining independent frameworks for evaluating explainability and algorithmic accountability. Building on agency theory, the paper argues that AI explainability is a logical extension of the classic audit function: just as independent audit historically reduced information asymmetry between management and owners, evaluating AI explainability can reduce the information asymmetry between opaque algorithmic systems and organizational stakeholders. Based on this theoretical grounding, the study proposes a three-layer conceptual framework for auditing AI explainability, illustrated in Figure 1 and summarized in Table 1.

Layer 1, Technical Transparency, assesses whether technical documentation of the model (model type, training data, and explainability methods such as SHAP or LIME) is available and comprehensible to the auditor; given evidence that even popular post-hoc methods can lack sufficient fidelity in multilevel models (Bhaumik et al., 2022), auditors must also assess the reliability of these explanations, not merely their existence. Layer 2, Governance Documentation, evaluates organizational alignment with governance frameworks such as COBIT and ISO/IEC 42001, including whether model-risk ownership and periodic review procedures are formally defined. Layer 3, Assurance Reporting, addresses how findings are reflected in the auditor's report; in the absence of a dedicated Iranian reporting standard, the study recommends a qualified-disclosure approach similar to that used in auditing complex accounting estimates.

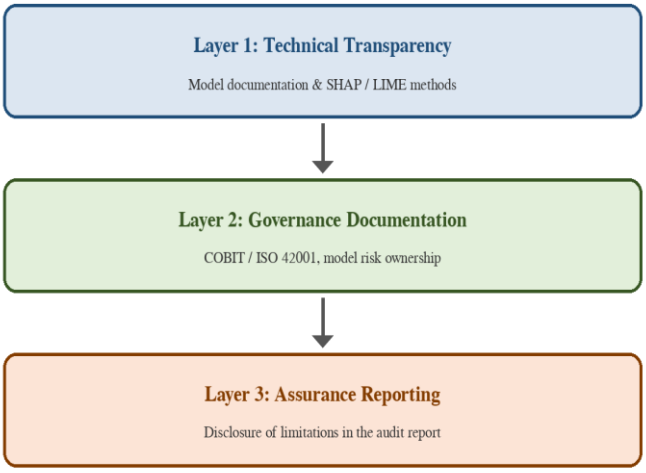



**Figure 1**. Proposed three-layer framework for auditing AI explainability

A hypothetical illustrative scenario — an Iranian bank applying the framework to an AI-based credit-scoring system — shows how each layer would guide the auditor: verifying whether SHAP-based explanations exist and have been validated (Layer 1); confirming that the risk committee has formally assigned model-risk ownership

and a periodic review cadence (Layer 2); and, where documentation is incomplete, disclosing that limitation explicitly in the audit report rather than remaining silent (Layer 3). This illustrates that, unlike purely technical approaches in the domestic literature, the proposed framework gives auditors a concrete decision path even in the absence of a formal standard.

**Table 1**

*Comparative analysis of governance frameworks by explainability coverage*

| Framework | Primary Focus | Explainability Coverage | Regulatory Alignment |
|---|---|---|---|
| COBIT 2019 | Strategic alignment & IT risk management | Moderate; requires added AI-specific processes | Strongest alignment with EU AI Act |
| ISO/IEC 42001 (2023) | Dedicated AI management systems | Comprehensive; purpose-built for AI | Broadest coverage of generative-AI opportunities |
| NIST AI RMF | Technical AI risk management | High technical depth; weaker governance layer | Non-binding, primarily US reference |
| ISO 27001 | Organizational information security | Limited; explainability outside core scope | Gaps in AI-specific risk oversight |

**Source**: compiled by the authors based on McIntosh et al. (2024) and ISACA (2025).

## 4. CONCLUSION

This study shows that AI explainability, as a dimension independent of model accuracy, remains underexplored in Iran's domestic IT-audit literature, while international literature and professional bodies are rapidly moving toward requiring it. The proposed three-layer framework — technical transparency, governance documentation, and assurance reporting — offers a starting point for future empirical work, including case studies in Iranian organizations and readiness surveys of internal auditors. Practically, audit firms should update internal training on explainable-AI fundamentals, audit committees should treat AI governance as a board-level matter rather than a purely technical

one, and Iranian professional bodies should develop operational guidance for adapting COBIT to AI-governance requirements. As a conceptual review, the study's main limitation is the absence of primary field data; validating the proposed framework empirically is left for future research.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ ترویجی**

# گشودن جعبه سیاه: چارچوبی برای اطمینان‌بخشی حسابرسان از توضیح‌پذیری تصمیمات هوش مصنوعی در حاکمیت ریسک فناوری اطلاعات[1]

**فرزاد ایوانی*[2] و دنیا کاظمی[3]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۱۵۹ - ۱۸۶

تاریخ دریافت: ۱۴۰۵/۰۵/۲۹
تاریخ بازنگری: ۱۴۰۵/۰۷/۱۸
تاریخ پذیرش: ۱۴۰۵/۰۸/۰۶

## چکیده

*این پژوهش با رویکردی مفهومی و مروری، جایگاه توضیح‌پذیری هوش مصنوعی را در حاکمیت ریسک فناوری اطلاعات و اطمینان‌بخشی حسابرسی بررسی می‌کند. با گسترش به‌کارگیری هوش مصنوعی در فرایندهای سازمانی، از جمله امتیازدهی اعتباری و تشخیص تقلب، حسابرسان با این پرسش مواجه‌اند که چگونه می‌توان تصمیماتی را اطمینان‌بخشی کرد که از دل مدل‌های غیرشفاف (جعبه سیاه) بیرون می‌آیند. داده‌های پژوهش از مرور نظام‌مند ادبیات داخلی و خارجی مرتبط باهوش مصنوعی توضیح‌پذیر، کوبیت و ایزو ۴۲۰۰۱ گردآوری و با رویکرد تطبیقی بررسی شده است. یافته‌ها نشان می‌دهد ادبیات داخلی عمدتاً بر بهبود دقت حسابرسی با کمک هوش مصنوعی متمرکز است و کمتر به توضیح‌پذیری به‌عنوانُ بُعدی مستقل از حاکمیت ریسک پرداخته، درحالی‌که نهادهای بین‌المللی به‌سرعت به‌سوی الزامی کردن آن حرکت می‌کنند. براین‌اساس، چارچوب مفهومی سه‌لا یه شامل شفافیت فنّی، مستندسازی حاکمیتی و گزارشگری اطمینان‌بخشی پیشنهاد شده که با سناریویی فرضی در حوزه بانکداری نشان‌داده‌شده و می‌تواند مبنای پژوهش‌های تجربی آتی و راهنمای عملیاتی برای حسابرسان ایرانی باشد.*

**واژه‌های کلیدی:** *هوش مصنوعی توضیح‌پذیر، حاکمیت ریسک فناوری اطلاعات، اطمینان‌بخشی حسابرسی، پاسخ‌گویی الگوریتمی.*

**طبقه‌بندی موضوعی:** *M42, M15, O33.*

---

[1] https://doi.org/10.22034/JISTA.2026.603372.1107

[1] مقاله منتخب دومین همایش ملی حاکمیت شرکتی و مدیریت ریسک‌های فناوری اطلاعات

[2] استادیار گروه حسابداری، دانشکده اقتصاد و حسابداری، دانشگاه رازی، کرمانشاه، ایران. (نویسنده مسئول). (feivani@gmail.com)

[3] کارشناس ارشد حسابداری، دانشکده اقتصاد و حسابداری، دانشگاه رازی، کرمانشاه، ایران. (kazemidonya95@gmail.com)

**مقدمه**

در یک دهه اخیر، هوش مصنوعی از یک ابزار کمکی در تحلیل داده‌ها، به یکی از فناوری‌های مهم در فرایندهای تصمیم‌گیری و مدیریت سازمانی تبدیل شده است. استفاده از روش‌های یادگیری ماشین و سایر فناوری‌های هوش مصنوعی در فرایندهای حسابرسی و ارزیابی مدل‌های تصمیم‌گیری، ظرفیت‌هایی برای افزایش کارایی و کیفیت تحلیل‌ها ایجاد کرده است؛ هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی نیز بر ظرفیت فناوری برای ارتقای کیفیت کار حسابرسی و اطمینان‌بخشی تأکید کرده است (هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی[۱]، ۲۰۲۴: ۱).

با گسترش استفاده از مدل‌های پیچیده هوش مصنوعی، مسئله شفافیت و قابلیت توضیح تصمیم‌های الگوریتمی نیز اهمیت بیشتری یافته است. برخی مدل‌های یادگیری ماشین از نظر نحوه تبدیل ورودی‌ها به خروجی‌ها، برای کاربران و حتی ارزیابان فنّی به‌سادگی قابل‌تفسیر نیستند و از این منظر، موضوع «توضیح‌پذیری» و «قابلیت حسابرسی» مدل‌های هوش مصنوعی اهمیت ویژه‌ای پیدا می‌کند. پژوهش بهاومیک، دی و کایال[۲] (۲۰۲۲: ۱۲) با تمرکز بر حسابرسی مدل‌های چندسطحی، ارزیابی مدل، تبعیض، شفافیت و توضیح‌پذیری را از ابعاد مهم حسابرسی مدل‌های هوش مصنوعی معرفی می‌کند و استفاده از روش‌هایی مانند شپ[۳] و لایم[۴] را برای ارزیابی توضیح‌پذیری مورد بررسی قرار می‌دهد.

در حوزه حاکمیت فناوری اطلاعات نیز چارچوب‌هایی مانند کوبیت[۵] باهدف ایجاد سازوکارهای مناسب برای حاکمیت و مدیریت فناوری اطلاعات مورداستفاده قرار گرفته‌اند. با گسترش کاربرد هوش مصنوعی، این چارچوب‌ها با ضرورت توجه بیشتر به فرصت‌ها، ریسک‌ها و الزامات حاکمیت مرتبط با سامانه‌های هوش مصنوعی مواجه شده‌اند (انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی[۶]، ۲۰۲۵: ۳؛ مک‌اینتاش و همکاران[۷]، ۲۰۲۴: ۲-۱).

---

[1] International Auditing and Assurance Standards Board (IAASB)
[2] Bhaumik, Dey & Kayal
[3] SHapley Additive exPlanations (SHAP)
[4] Local Interpretable Model-agnostic Explanations (LIME)
[5] Control Objectives for Information and Related Technologies (COBIT)
[6] Information Systems Audit and Control Association (ISACA)
[7] McIntosh et al.

چهار چارچوب شامل چارچوب امنیت سایبری ان‌آی‌اس‌تی[1]، کوبیت ۲۰۱۹، ایزو ۲۷۰۰۱ و ایزو ۴۲۰۰۱ را از منظر آمادگی برای استفاده از مدل‌های زبانی بزرگ بررسی کرده است. نتایج این پژوهش نشان می‌دهد که ایزو ۴۲۰۰۱ در میان چارچوب‌های بررسی‌شده، جامع‌ترین ظرفیت را برای تسهیل فرصت‌های مرتبط با مدل‌های زبانی بزرگ داشته است؛ بااین‌حال، همچنان شکاف‌هایی در نظارت بر ریسک‌های مرتبط با این فناوری وجود دارد.

در سطح استانداردگذاری بین‌المللی، استاندارد ایزو ۴۲۰۰۱ در دسامبر ۲۰۲۳ منتشر شد. این استاندارد، الزامات مربوط به ایجاد، استقرار، نگهداری و بهبود مستمر «سیستم مدیریت هوش مصنوعی[2]» را مشخص می‌کند و توسط سازمان بین‌المللی استانداردسازی[3] به‌عنوان نخستین استاندارد سیستم مدیریت هوش مصنوعی معرفی شده است. این استاندارد همچنین بر مدیریت ریسک‌ها و فرصت‌های مرتبط باهوش مصنوعی، شفافیت و استفاده مسئولانه از این فناوری تأکید دارد (سازمان بین‌المللی استانداردسازی،۲۰۲۳: ۱؛ مک‌اینتاش و همکاران، ۲۰۲۴: ۱).

در ایران نیز پژوهش‌های انجام‌شده در زمینه کاربرد هوش مصنوعی در حسابداری و حسابرسی (شاه‌صاحبی و همکاران، ۱۳۹۹؛ سلیمانی‌امیری و محمدی‌سه‌دران، ۱۴۰۳؛ صحت‌برمچه و همکاران، ۱۴۰۵) بیشتر به بررسی نقش این فناوری در بهبود فرایندهای حسابرسی، افزایش کیفیت قضاوت حسابرسان و تحلیل برخی ابعاد مرتبط با توانایی مدیریت پرداخته‌اند. باوجوداین، در مطالعات بررسی‌شده، موضوع شفافیت و توضیح‌پذیری نحوه تصمیم‌گیری مدل‌های هوش مصنوعی و ارتباط آن با فرایندهای اطمینان‌بخشی در حسابرسی فناوری اطلاعات کمتر به طور مستقیم موردتوجه قرار گرفته است. به نظر می‌رسد بخش قابل‌توجهی از ادبیات داخلی همچنان بر استفاده از هوش مصنوعی برای انجام یا تقویت فعالیت‌های حسابرسی متمرکز است، درحالی‌که در ادبیات بین‌المللی، توجه بیشتری به بررسی و ارزیابی خود سامانه‌های هوش مصنوعی، از جمله سازوکارهای حاکمیت، مدیریت ریسک و توضیح‌پذیری آن‌ها، شکل‌گرفته است. از این منظر، بررسی هم‌زمان توضیح‌پذیری مدل‌های هوش مصنوعی و ارتباط آن با حاکمیت و مدیریت ریسک فناوری اطلاعات و فرایند

[1] NIST Cybersecurity Framework (NIST CSF)
[2] Artificial Intelligence Management System
[3] International Organization for Standardization (ISO)

اطمینان‌بخشی حسابرسی، از جمله موضوعاتی است که در پژوهش‌های داخلی کمتر موردتوجه قرار گرفته و می‌تواند زمینه مناسبی برای مطالعات بیشتر فراهم کند.

از این منظر، مسئله اساسی پژوهش حاضر آن است که با افزایش استفاده از سامانه‌های هوش مصنوعی در سازمان‌ها، حسابرس فناوری اطلاعات چگونه می‌تواند درباره شفافیت، قابلیت توضیح و کنترل ریسک‌های تصمیم‌های الگوریتمی اطمینان‌بخشی ارائه کند؛ چراکه پیچیدگی این مدل‌ها، ارزیابی منطق تصمیم‌گیری و تشخیص سوگیری را دشوار می‌سازد.

در سطح حرفه حسابرسی نیز تحولات فناوری موردتوجه نهادهای استاندارد گذار قرار گرفته است. هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی در بیانیه موضع فناوری خود، هم‌گرایی حسابرسی، اطمینان‌بخشی و فناوری را مبنای رویکرد خود دانسته و هشت اقدام راهبردی برای تسهیل و تشویق به‌کارگیری فناوری از سوی حسابرسان تعیین کرده است؛ از جمله رفع موانع واقعی یا ادراک‌شده در استانداردها برای استفاده از فناوری و تدوین الزامات و مواد کاربردی مرتبط با استفاده از آن در اجرای کار (هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی، ۲۰۲۴: ۱).

در حوزه حسابرسی داخلی نیز «استانداردهای جهانی حسابرسی داخلی[1]» در ژانویه ۲۰۲۴ منتشر شدند. این استانداردها، افزون بر دانش مربوط به فناوری اطلاعات، آشنایی با ابزارها و فنون گردآوری، تحلیل و ارزیابی داده را جزو شایستگی‌های لازم حسابرسان داخلی می‌شمارند (انجمن حسابرسان داخلی[2]، ۲۰۲۴: ۲، ۲۶).

براین‌اساس، سرعت گسترش و استفاده از فناوری‌های هوش مصنوعی در سازمان‌ها، در کنار نیاز به ایجاد سازوکارهای مناسب برای حاکمیت، مدیریت ریسک، شفافیت و توضیح‌پذیری این فناوری‌ها، یکی از مهم‌ترین زمینه‌های شکل‌گیری پژوهش حاضر است. در این راستا، پژوهش حاضر با ارائه یک چارچوب مفهومی سه‌لایه تلاش می‌کند توضیح‌پذیری هوش مصنوعی را صرفاً یک ویژگی فنّی در نظر نگیرد، بلکه آن را در ارتباط با حاکمیت و مدیریت ریسک فناوری اطلاعات و همچنین فرایند اطمینان‌بخشی حسابرسی فناوری اطلاعات بررسی

[1] Global Internal Audit Standards
[2] Institute of Internal Auditors (IIA)

کند. این رویکرد با درنظرگرفتن شرایط و الزامات سازمانی ایران، می‌تواند تصویری منسجم‌تر از جایگاه توضیح‌پذیری در فرایند ارزیابی و اطمینان‌بخشی سامانه‌های هوش مصنوعی ارائه دهد.

## مبانی نظری

### هوش مصنوعی توضیح‌پذیر

هوش مصنوعی توضیح‌پذیر[1]، به مجموعه‌ای از روش‌ها و رویکردهایی اشاره دارد که هدف آن‌ها افزایش قابلیت درک و تفسیر فرایند تصمیم‌گیری مدل‌های هوش مصنوعی برای کاربران انسانی است. در ادبیات مربوط به توضیح‌پذیری، میان روش‌های مبتنی بر مدل‌های ذاتاً تفسیرپذیر و روش‌های توضیح پسینی، تمایز قائل می‌شود. در روش‌های پسینی، رفتار مدل‌های پیچیده پس از آموزش با استفاده از ابزارهایی مانند شپ و لایم مورد تحلیل قرار می‌گیرد. علاوه بر این، روش‌های تبیین ضدواقعی[2] نیز با تمرکز بر تغییرات لازم در ویژگی‌های ورودی برای تغییر خروجی مدل، نوع دیگری از توضیح برای تصمیم‌های الگوریتمی فراهم می‌کنند. این رویکردها از منظر حسابرسی اهمیت دارند؛ زیرا حسابرس نه‌تنها به خروجی مدل، بلکه به شواهدی درباره نحوه شکل‌گیری آن خروجی نیاز دارد.

بهاومیک و همکاران (۲۰۲۲: ۱۲) با ارائه چارچوبی برای حسابرسی مدل‌های چندسطحی، سه حوزه مدل، تبعیض و شفافیت و توضیح‌پذیری را برای ارزیابی حسابرسی مدل‌ها موردتوجه قرار داده‌اند. آنان روش‌هایی مانند شپ و لایم را در ارزیابی توضیح‌پذیری بررسی کرده و نشان داده‌اند که این روش‌ها در مدل‌های موردمطالعه، در برخی جنبه‌های تفسیر اهمیت ویژگی‌ها و سهم ویژگی‌ها با محدودیت‌هایی مواجه هستند (بهاومیک و همکاران، ۲۰۲۲: ۱۹–۲۰). این یافته نشان می‌دهد که استفاده از ابزارهای توضیح‌پذیری به‌تنهایی برای اطمینان از قابلیت تفسیر یک مدل کافی نیست و خود روش‌های توضیح‌پذیری نیز می‌توانند موضوع ارزیابی و حسابرسی قرار گیرند.

---

[1] Explainable Artificial Intelligence (XAI)

[2] Counterfactual Explanations

## چارچوب‌های حاکمیت فناوری اطلاعات و هوش مصنوعی

حاکمیت فناوری اطلاعات، از سازوکارهای مهم برای تعیین مسئولیت‌ها، مدیریت ریسک و همسویی فناوری با اهداف سازمانی است. چارچوب کوبیت که توسط انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی توسعه‌یافته، از شناخته‌شده‌ترین چارچوب‌های حاکمیت فناوری اطلاعات است و با گسترش هوش مصنوعی، می‌تواند برای پاسخگویی، شفافیت، مدیریت ریسک و نظارت بر این سامانه‌ها نیز به کار رود (انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی، ۲۰۲۵: ۳).

انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی (۲۰۲۵: ۳، ۱۳-۱۴) در راهنمای «بهره‌گیری از کوبیت برای حاکمیت مؤثر سامانه‌های هوش مصنوعی» توضیح می‌دهد که کوبیت می‌تواند برای حاکمیت این سامانه‌ها در طول چرخه عمرشان، شامل پاسخگویی، آزمون، اعتبارسنجی و پایش مستمر، به کار رود. در کنار کوبیت، استاندارد ایزو ۴۲۰۰۱ به طور اختصاصی برای سیستم مدیریت هوش مصنوعی طراحی شده و چارچوبی برای ایجاد، استقرار، نگهداری و بهبود این سیستم فراهم می‌کند (سازمان بین‌المللی استانداردسازی، ۲۰۲۳). استفاده هم‌زمان از اصول حاکمیتی کوبیت و الزامات ایزو ۴۲۰۰۱ می‌تواند مبنای مناسبی برای ارزیابی حاکمیتی سامانه‌های هوش مصنوعی فراهم کند.

در سطح تنظیم‌گری نیز الزامات مرتبط با شفافیت، پاسخگویی، مدیریت ریسک و نظارت بر سامانه‌های هوش مصنوعی اهمیت فزاینده‌ای یافته‌اند. چونگ[1] (۲۰۲۴: ۱-۲) در یک مرور درباره شفافیت و پاسخگویی در سامانه‌های هوش مصنوعی، چالش‌های موجود را در چهار حوزه اصلی شامل رویکردهای فنّی، چارچوب‌های حقوقی و تنظیم‌گری، ملاحظات اخلاقی و اجتماعی و رویکردهای میان‌رشته‌ای و چندذی‌نفعی طبقه‌بندی می‌کند. این طبقه‌بندی نشان می‌دهد که ارزیابی سامانه‌های هوش مصنوعی صرفاً یک مسئله فنّی نیست و ابعاد حقوقی، اخلاقی، اجتماعی و حاکمیتی نیز باید در ارزیابی آن‌ها موردتوجه قرار گیرد.

[1] Cheong

## نظریه اطمینان‌بخشی حسابرسی در بستر الگوریتمی

اطمینان‌بخشی حسابرسی بر فراهم‌کردن شواهد کافی برای اظهارنظر حرفه‌ای استوار است. با ورود هوش مصنوعی، دامنه اطلاعات لازم فراتر از اسناد مالی سنتی می‌رود و شامل داده‌های مورداستفاده، طراحی و عملکرد مدل، فرایند اعتبارسنجی و شواهد مربوط به نحوه تولید خروجی می‌شود.

از این منظر، توضیح‌پذیری می‌تواند بُعدی مهم در ارزیابی سامانه‌های هوش مصنوعی باشد؛ زیرا حسابرس باید تاحدامکان درباره منطق تصمیم‌گیری و ریسک‌های خروجی مدل قضاوت کند (هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی، ۲۰۲۴: ۱؛ مک‌اینتاش و همکاران، ۲۰۲۴: ۲-۱).

بهاومیک و همکاران (۲۰۲۲: ۱۲، ۲۰) نیز نشان می‌دهند ارزیابی مدل باید فراتر از سنجش صرف عملکرد پیش‌بینی آن باشد. همچنین چونگ (۲۰۲۴: ۱-۲) نشان می‌دهد که شفافیت و پاسخگویی در سامانه‌های هوش مصنوعی با مجموعه‌ای از چالش‌های فنّی، حقوقی، اخلاقی و اجتماعی همراه است؛ بنابراین، در بستر حسابرسی فناوری اطلاعات، ارزیابی توضیح‌پذیری را می‌توان بخشی از یک رویکرد گسترده‌تر برای بررسی شفافیت، پاسخگویی و مدیریت ریسک سامانه‌های هوش مصنوعی در نظر گرفت.

## واکنش نهادهای بین‌المللی تنظیم‌گری حسابرسی

هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی در بیانیه موضع فناوری خود، افزون بر این، بر ایجاد توازن در اشاره به فرصت‌ها و ریسک‌های فناوری، هم‌راستایی با اصول اخلاقی و فرایند مستمر پایش روندهای فناورانه تأکید کرده است (هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی، ۲۰۲۴: ۱).

این روند در سال‌های ۲۰۲۵ و ۲۰۲۶ نیز با برگزاری میزگردهای جهانی «مدیریت کیفیت فناوری» ادامه یافته است. محور این میزگردها، تأثیر فناوری‌های نوظهور، از جمله هوش مصنوعی، بر حسابرسی و اطمینان‌بخشی و ضرورت حفظ اعتماد در استفاده از ابزارهای فناورانه بوده است (هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی، ۲۰۲۶).

این تحولات نشان می‌دهد که استفاده از هوش مصنوعی در حسابرسی صرفاً یک مسئله فنّی مربوط به عملکرد ابزارها نیست، بلکه به موضوعاتی همچون مدیریت کیفیت، حاکمیت، مدیریت ریسک و پاسخگویی نیز مرتبط شده است. از این منظر، توضیح‌پذیری و شفافیت مدل‌های هوش مصنوعی می‌توانند به‌عنوان بخشی از مسائل حاکمیتی و کیفیتی موردتوجه حسابرسی فناوری اطلاعات قرار گیرند.

## نظریه نمایندگی و ضرورت حاکمیت هوش مصنوعی

بر اساس نظریه نمایندگی، جدایی مالکیت از مدیریت می‌تواند به شکل‌گیری تضاد منافع و عدم تقارن اطلاعاتی میان مالکان و مدیران منجر شود و سازوکارهایی مانند نظارت و حسابرسی برای کاهش این مسائل اهمیت پیدا می‌کنند (جنسن و مکلینگ[1]، ۱۹۷۶: ۳۰۶، ۳۰۸).

ورود هوش مصنوعی به فرایندهای تصمیم‌گیری سازمانی می‌تواند شکل جدیدی از عدم تقارن اطلاعاتی ایجاد کند؛ زیرا ذی‌نفعان ممکن است درباره نحوه شکل‌گیری تصمیم‌های الگوریتمی اطلاعات کافی نداشته باشند. در چنین شرایطی، شفافیت و توضیح‌پذیری می‌توانند این عدم تقارن را کاهش داده و امکان نظارت را افزایش دهند (چونگ، ۲۰۲۴: ۲).

از این منظر، ارزیابی توضیح‌پذیری هوش مصنوعی را می‌توان امتدادی از منطق نظارتی نظریه نمایندگی در محیط الگوریتمی دانست: همان‌گونه که حسابرسی مستقل با کاهش عدم تقارن اطلاعاتی میان مدیریت و ذی‌نفعان یک سازوکار نظارتی است، ارزیابی شفافیت و توضیح‌پذیری سامانه‌های هوش مصنوعی نیز می‌تواند نظارت مؤثرتری بر تصمیم‌های الگوریتمی فراهم کند.

در ایران، بخشی از پژوهش‌های حوزه هوش مصنوعی و حسابداری و حسابرسی بر کاربرد این فناوری در فرایندهای حسابرسی، قضاوت حسابرسی، تحلیل توانایی مدیریت و ارزیابی عملکرد تمرکز داشته‌اند؛ ازجمله سلیمانی امیری و محمدی سه‌دران (۱۴۰۳: ۱) درباره حسابرسی در عصر هوش مصنوعی، صحت برمچه، شماخی و یلفانی (۱۴۰۵: ۱۹۱) درباره الگوی قضاوت حسابرسی مبتنی بر هوش مصنوعی، شاه صاحبی، دارابی و حمیدیان (۱۳۹۹: ۷۵) درباره توانایی مدیریت، و احمد حسین، زواری رضایی و آشتاب (۱۴۰۳: ۷۴) درباره عملکرد مالی بانک‌ها.

[1] Jensen & Meckling

بااین‌حال، تمرکز این مطالعات عمدتاً بر کاربرد هوش مصنوعی به‌عنوان ابزار تحلیل، پیش‌بینی یا تصمیم‌گیری بوده و توضیح‌پذیری و شفافیت فرایند تصمیم‌گیری مدل‌ها به‌عنوان موضوعی مستقل موردتوجه قرار نگرفته است. پژوهش حاضر با انتقال تمرکز از «استفاده از هوش مصنوعی در حسابرسی» به «ارزیابی قابلیت توضیح و شفافیت آن از منظر حسابرسی فناوری اطلاعات»، این بعد کمتر موردتوجه را بررسی می‌کند.

در حوزه حاکمیت فناوری اطلاعات نیز رونقی و محمودی (۱۳۹۴: ۶۱۵) رابطه حاکمیت فناوری اطلاعات و حاکمیت شرکتی را در سازمان‌های دولتی بررسی کرده و رونقی، فرهادی و خردمند (۱۳۹۷: ۹) به ارزیابی حاکمیت فناوری اطلاعات با رویکرد سلسله‌مراتبی خاکستری پرداخته‌اند. این مطالعات اهمیت حاکمیت فناوری اطلاعات را نشان می‌دهند، اما به شفافیت و توضیح‌پذیری مدل‌های هوش مصنوعی نپرداخته‌اند.

در ادبیات بین‌المللی نیز بهاومیک و همکاران (۲۰۲۲: ۱۲) رابطه میان حسابرسی مدل‌ها و توضیح‌پذیری را بررسی کرده و مک‌اینتاش و همکاران (۲۰۲۴: ۱) ظرفیت چارچوب‌های حاکمیتی، از جمله کوبیت و ایزو ۴۲۰۰۱، را در مواجهه با ریسک‌های مدل‌های زبانی بزرگ تحلیل کرده‌اند؛ ترکیب این دو جریان پژوهشی مبنایی برای چارچوب مفهومی پژوهش حاضر فراهم می‌کند.

باتوجه‌به ماهیت کیفی و مفهومی پژوهش حاضر، اهداف پژوهش به‌جای تدوین فرضیه‌های علّی، به‌صورت زیر تعیین شده‌اند:

۱) شناسایی جایگاه توضیح‌پذیری هوش مصنوعی در ادبیات داخلی و خارجی حسابرسی فناوری اطلاعات؛

۲) تحلیل تطبیقی ظرفیت چارچوب‌های حاکمیتی موجود، از جمله کوبیت، ایزو ۴۲۰۰۱ و چارچوب مدیریت ریسک هوش مصنوعی ان‌آی‌اس‌تی[1]، برای پوشش ابعاد مرتبط با توضیح‌پذیری، شفافیت، پاسخگویی و مدیریت ریسک هوش مصنوعی؛

۳) ارائه یک چارچوب مفهومی برای هدایت ارزیابی حسابرسی فناوری اطلاعات از توضیح‌پذیری سامانه‌های هوش مصنوعی در سازمان‌های ایرانی.

[1] National Institute of Standards and Technology AI Risk Management Framework (NIST AI RMF)

## روش‌شناسی پژوهش

این پژوهش با رویکردی کیفی و مفهومی و با استفاده از مرور و تحلیل تطبیقی ادبیات داخلی و بین‌المللی انجام شده است. راهبرد جست‌وجوی منابع بر اساس ترکیبی از کلیدواژه‌های مرتبط با «هوش مصنوعی توضیح‌پذیر»، «حاکمیت هوش مصنوعی[1]»، «حسابرسی فناوری اطلاعات[2]»، «کوبیت»، «ایزو ۴۲۰۰۱»، «چارچوب مدیریت ریسک هوش مصنوعی نیست» و «اطمینان‌بخشی الگوریتمی» در منابع علمی و حرفه‌ای مرتبط شکل گرفت.

منابع داخلی از میان مطالعات منتشرشده در حوزه حسابداری، حسابرسی، مدیریت فناوری اطلاعات و حاکمیت فناوری اطلاعات انتخاب شدند. برای بررسی ادبیات بین‌المللی نیز از پایگاه‌ها و ناشران علمی مرتبط از جمله اسکوپوس[3]، وب آو ساینس[4]، ساینس دایرکت[5]، فرانتیرز[6] و آرکایو[7] استفاده شد. جست‌وجو در بازه ژانویه ۲۰۱۸ تا ژوئن ۲۰۲۵ انجام شد. کلیدواژه‌های اصلی شامل ترکیب‌های مربوط به ترکیب‌های مربوط به هوش مصنوعی توضیح‌پذیر[8]، حاکمیت فناوری اطلاعات[9]، اطمینان‌بخشی حسابرسی[10] و مدل‌های جعبه سیاه[11] با عملگرهای بولی بود.

معیار اصلی ورود منابع، ارتباط مستقیم آن‌ها با دست‌کم یکی از سه محور اصلی پژوهش شامل توضیح‌پذیری هوش مصنوعی، حاکمیت فناوری اطلاعات و هوش مصنوعی، یا اطمینان‌بخشی حسابرسی در محیط‌های الگوریتمی بود. معیارهای خروج نیز شامل حذف مطالعات تکراری، منابع فاقد کیفیت علمی کافی، آثار نامرتبط با محورهای پژوهش و مطالعاتی بود که صرفاً به کاربرد ابزاری هوش مصنوعی در حسابرسی پرداخته و به جنبه‌های توضیح‌پذیری و حاکمیت توجهی نداشتند. در مجموع حدود ۱۵۰ منبع بازیابی و پس از غربالگری، ۱۸ منبع برای تحلیل نهایی انتخاب شد. پس از بررسی اولیه، مطالعات مرتبط از منظر موضوع، هدف، رویکرد و یافته‌های اصلی مقایسه شدند. در بخش بین‌المللی، علاوه بر مطالعات دانشگاهی، اسناد

---

[1] AI Governance
[2] IT Auditing
[3] Scopus
[4] Web of Science
[5] ScienceDirect
[6] Frontiers
[7] arXiv
[8] explainable AI / XAI
[9] IT governance
[10] Audit assurance
[11] Black-box models

حرفه‌ای مرتبط با حاکمیت هوش مصنوعی، از جمله کوبیت، ایزو ۴۲۰۰۱ و اسناد هیئت استانداردهای بین‌المللی حسابرسی، نیز موردتوجه قرار گرفتند تا ادبیات دانشگاهی با جهت‌گیری‌های حرفه‌ای مقایسه شود (انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی، ۲۰۲۵: ۳؛ مک‌اینتاش و همکاران، ۲۰۲۴: ۴).

جامعهٔ مورد بررسی، ادبیات علمی و حرفه‌ای مرتبط با موضوع است و ابزار گردآوری داده‌ها، مرور و مقایسه تطبیقی محتوای منابع منتخب است. پژوهش حاضر ماهیتی مفهومی-مروری دارد؛ ازاین‌رو هدف آن آزمون تجربی روابط علّی نیست، بلکه شناسایی شکاف پژوهشی و ارائه چارچوبی برای هدایت مطالعات آینده است.

## یافته‌های پژوهش

یافته‌های حاصل از بررسی و مقایسه تطبیقی ادبیات نشان می‌دهد میان ادبیات داخلی مرتبط با کاربرد هوش مصنوعی در حسابداری و حسابرسی، و ادبیات بین‌المللی مرتبط با توضیح‌پذیری و حاکمیت مدل‌ها، تفاوت‌های آشکاری وجود دارد: در مطالعات داخلی، هوش مصنوعی عمدتاً به‌عنوان ابزار تحلیل و بهبود فرایندها موردتوجه قرار گرفته است؛ در مقابل، بخشی از ادبیات بین‌المللی مستقیماً به حسابرسی مدل، توضیح‌پذیری و حاکمیت این سامانه‌ها پرداخته است (بهاومیک و همکاران، ۲۰۲۲: ۱۲؛ مک‌اینتاش و همکاران، ۲۰۲۴: ۱).

بر اساس این یافته و با تلفیق مباحث مربوط به توضیح‌پذیری، حاکمیت فناوری و اطمینان‌بخشی حسابرسی، پژوهش حاضر، یک چارچوب مفهومی سه‌لایه برای ارزیابی حسابرسی از توضیح‌پذیری هوش مصنوعی پیشنهاد می‌کند.

### لایه نخست: شفافیت فنی

در این لایه، حسابرس بررسی می‌کند که آیا اطلاعات و مستندات لازم درباره مدل، داده‌های مورداستفاده، نحوه آموزش و اعتبارسنجی مدل و روش‌های توضیح‌پذیری مورداستفاده در دسترس است یا خیر. در مدل‌های پیچیده، روش‌هایی مانند شپ و لایم می‌توانند برای تولید توضیحات پسینی مورداستفاده قرار گیرند؛ بااین‌حال، استفاده از چنین روش‌هایی نباید به معنای پذیرش خودکار توضیحات تولیدشده به‌عنوان شواهد کافی تلقی شود.

بهاومیک و همکاران (۲۰۲۲: ۲۰) نشان می‌دهند که روش‌های توضیح‌پذیری می‌توانند خود با محدودیت‌هایی مواجه باشند و بنابراین ارزیابی کیفیت و قابلیت اتکای توضیحات باید بخشی از فرایند ارزیابی مدل باشد. بر این اساس، حسابرس باید علاوه بر بررسی وجود مستندات توضیح‌پذیری، قابلیت اتکای روش مورداستفاده و محدودیت‌های آن را نیز موردتوجه قرار دهد.

### لایه دوم: مستندسازی حاکمیتی

در لایه دوم، تمرکز از ویژگی‌های فنّی مدل به سازوکارهای حاکمیتی و سازمانی منتقل می‌شود. حسابرس بررسی می‌کند که آیا سازمان فرایندهای مشخصی برای طراحی، توسعه، آموزش، استقرار، اعتبارسنجی، پایش و بازبینی مدل‌های هوش مصنوعی دارد و آیا مسئولیت‌ها و اختیارات مربوط به مدیریت ریسک مدل به‌صورت مشخص تعیین شده‌اند.

چارچوب کوبیت می‌تواند از منظر حاکمیت و مدیریت فناوری اطلاعات در این ارزیابی مورداستفاده قرار گیرد. انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی (۲۰۲۵: ۳، ۱۳) نیز ظرفیت کوبیت را برای پشتیبانی از حاکمیت و مدیریت سامانه‌های هوش مصنوعی و موضوعاتی مانند پاسخگویی، مدیریت ریسک و کنترل‌های مرتبط با چرخه عمر فناوری موردتوجه قرار داده است.

در کنار کوبیت، ایزو ۴۲۰۰۱ به طور اختصاصی برای سیستم مدیریت هوش مصنوعی طراحی شده و چارچوبی برای ایجاد، استقرار، نگهداری و بهبود سیستم مدیریت هوش مصنوعی فراهم می‌کند (سازمان بین‌المللی استانداردسازی، ۲۰۲۳). بنابراین، استفاده هم‌زمان از اصول حاکمیت کوبیت و الزامات سیستم مدیریت هوش مصنوعی ایزو ۴۲۰۰۱ می‌تواند مبنای مناسبی برای ارزیابی حاکمیتی سامانه‌های هوش مصنوعی فراهم کند.

### لایه سوم: گزارشگری اطمینان‌بخشی

در لایه سوم، نتایج ارزیابی فنّی و حاکمیتی به فرایند گزارشگری حسابرسی منتقل می‌شود. حسابرس باید بتواند محدودیت‌های شناسایی‌شده در زمینه مستندات، شفافیت، قابلیت توضیح یا کنترل‌های حاکمیتی مدل را در چارچوب مناسب گزارشگری منعکس کند.

## جدول ۱

*چارچوب سه‌لایه پیشنهادی برای ارزیابی حسابرسی از توضیح‌پذیری هوش مصنوعی*

| لایه | مؤلفه‌های اصلی | پرسش کلیدی حسابرس |
|---|---|---|
| اول: شفافیت فنّی | نوع مدل، داده‌های مورداستفاده، آموزش و اعتبارسنجی، شپ/لایم و محدودیت‌های توضیح | آیا مدل و روش توضیح‌پذیری مستند، قابل‌فهم و از نظر فنی قابل‌اتکا هستند؟ |
| دوم: مستندسازی حاکمیتی | کوبیت، ایزو ۴۲۰۰۱، نقش‌ها و مسئولیت‌ها، مالکیت ریسک مدل، پایش مستمر | آیا مسئولیت‌ها و کنترل‌های حاکمیتی مدل به‌صورت رسمی تعریف و پایش می‌شوند؟ |
| سوم: گزارشگری اطمینان‌بخشی | یافته‌های حسابرسی، محدودیت‌های توضیح‌پذیری، گزارش نتایج و توصیه‌های اصلاحی | آیا محدودیت‌های مهم در شفافیت و توضیح‌پذیری در گزارش مربوط منعکس شده‌اند؟ |

در این پژوهش، افشای محدودیت‌های شناسایی‌شده به‌عنوان یک پیشنهاد مفهومی مطرح می‌شود، نه به‌عنوان یک الزام استاندارد موجود؛ بنابراین، پیشنهاد نمی‌شود که حسابرس الزاماً از قالب گزارشگری حسابرسی صورت‌های مالی برای گزارش توضیح‌پذیری هوش مصنوعی استفاده کند؛ بلکه پیشنهاد می‌شود در خدمات اطمینان‌بخشی یا حسابرسی فناوری اطلاعات، محدودیت‌های مهم مربوط به قابلیت توضیح و اتکاپذیری مدل به‌صورت شفاف در گزارش مربوط منعکس شود. بر اساس یافته‌های حاصل از مقایسه تطبیقی ادبیات، چارچوب سه‌لایه پیشنهادی برای ارزیابی حسابرسی توضیح‌پذیری هوش مصنوعی در جدول ۱ ارائه شده است.

## جدول ۲

*تحلیل تطبیقی چارچوب‌های حاکمیتی*

| چارچوب | کانون اصلی | پوشش مرتبط باهوش مصنوعی | کاربرد پیشنهادی در حسابرسی |
|---|---|---|---|
| کوبیت ۲۰۱۹ | حاکمیت و مدیریت فناوری اطلاعات | حاکمیت، مسئولیت‌پذیری، کنترل و مدیریت ریسک | ارزیابی ساختار حاکمیتی و کنترل‌های سازمانی |
| ایزو ۴۲۰۰۱ | سیستم مدیریت هوش مصنوعی | تمرکز اختصاصی بر مدیریت و حاکمیت هوش مصنوعی | ارزیابی سیستم مدیریت هوش مصنوعی و چرخه بهبود |
| چارچوب مدیریت ریسک هوش مصنوعی نیست | مدیریت ریسک هوش مصنوعی | شناسایی، اندازه‌گیری و مدیریت ریسک هوش مصنوعی | ساختاردهی ارزیابی ریسک مدل |
| ایزو ۲۷۰۰۱ | امنیت اطلاعات | پوشش عمومی امنیت و کنترل اطلاعات | کنترل‌های امنیتی مرتبط با داده و سامانه |

منبع: تدوین‌شده توسط نویسندگان بر اساس مک‌اینتاش و همکاران (۲۰۲۴)، انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی (۲۰۲۵) و سازمان بین‌المللی استانداردسازی (۲۰۲۳).

## جدول ۳

*سیاهه اولیه ارزیابی توضیح‌پذیری*

| لایه | شاهد موردانتظار | پرسش ارزیابی |
|---|---|---|
| شفافیت فنی | گزارش فنی مدل | آیا نوع مدل، داده‌های مورداستفاده و روش توضیح‌پذیری مستند شده است؟ |
| شفافیت فنی | گزارش اعتبارسنجی | آیا عملکرد و محدودیت‌های روش توضیح‌پذیری ارزیابی و مستند شده است؟ |
| مستندسازی حاکمیتی | سند نقش‌ها و مسئولیت‌ها | آیا مالکیت و مدیریت ریسک مدل به طور رسمی مشخص شده است؟ |
| مستندسازی حاکمیتی | رویه نظارت مستمر | آیا فرایند مشخصی برای بازبینی دوره‌ای عملکرد و ریسک مدل وجود دارد؟ |
| گزارشگری اطمینان‌بخشی | گزارش نهایی ارزیابی | آیا محدودیت‌های مهم شناسایی‌شده در توضیح‌پذیری در گزارش مربوط منعکس شده‌اند؟ |

منبع: تدوین‌شده توسط نویسندگان

## سناریوی کاربردی فرضی: به‌کارگیری چارچوب در یک بانک ایرانی

برای نشان‌دادن نحوه عملیاتی‌شدن چارچوب سه‌لایه، یک سناریوی فرضی و غیرواقعی در نظر گرفته می‌شود. فرض کنید یک بانک ایرانی از یک سامانه مبتنی بر یادگیری ماشین برای امتیازدهی اعتباری متقاضیان تسهیلات خرد استفاده می‌کند.

در لایه نخست، یعنی شفافیت فنّی، حسابرس فناوری اطلاعات مستندات فنّی سامانه را بررسی می‌کند و مشخص می‌سازد که نوع مدل، داده‌های آموزشی، فرایند اعتبارسنجی و روش توضیح‌پذیری مورداستفاده مستند شده‌اند یا خیر. درصورتی‌که از روش‌هایی مانند شپ استفاده شده باشد، حسابرس باید علاوه بر بررسی وجود توضیحات، محدودیت‌ها و قابلیت اتکای روش توضیح‌پذیری را نیز موردتوجه قرار دهد (بهاومیک و همکاران، ۲۰۲۲: ۲۰).

در لایه دوم، یعنی مستندسازی حاکمیتی، حسابرس بررسی می‌کند که آیا مسئولیت مدیریت ریسک مدل به‌صورت رسمی تعیین شده، فرایند بازبینی دوره‌ای مدل وجود دارد و سازوکار مشخصی برای شناسایی و مدیریت تغییرات عملکرد یا ریسک‌های مدل در نظر گرفته شده است. در این مرحله می‌توان از اصول حاکمیت و مدیریت کوبیت و الزامات سیستم مدیریت هوش مصنوعی ایزو ۴۲۰۰۱ به‌عنوان مبنای ارزیابی استفاده کرد (انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی، ۲۰۲۵: ۱۳-۱۴؛ سازمان بین‌المللی استانداردسازی، ۲۰۲۳).

در لایه سوم، یعنی گزارشگری اطمینان‌بخشی، حسابرس یافته‌های مربوط به کمبود مستندات، محدودیت در قابلیت توضیح یا ضعف کنترل‌های حاکمیتی را در گزارش اطمینان‌بخشی یا حسابرسی فناوری اطلاعات منعکس می‌کند. در این پژوهش، این اقدام پیشنهادی مفهومی است، نه الزامی استاندارد.

بنابراین، چارچوب پیشنهادی تلاش می‌کند ارزیابی هوش مصنوعی را از یک موضوع صرفاً فنی فراتر برده و آن را به سه سطح مرتبط با یکدیگر شامل شفافیت فنّی، حاکمیت سازمانی و گزارشگری اطمینان‌بخشی پیوند دهد. این چارچوب می‌تواند مبنایی مفهومی برای توسعه چک‌لیست‌های حسابرسی و انجام پژوهش‌های تجربی آینده در زمینه حسابرسی فناوری اطلاعات و حاکمیت هوش مصنوعی باشد.

## بحث و نتیجه‌گیری

این پژوهش نشان داد که توضیح‌پذیری هوش مصنوعی، به‌عنوان بُعدی مستقل از عملکرد و دقت مدل، در ادبیات داخلی حسابرسی فناوری اطلاعات کمتر موردتوجه قرار گرفته، درحالی‌که ادبیات بین‌المللی و چارچوب‌های حرفه‌ای به طور فزاینده‌ای بر شفافیت، پاسخ‌گویی و حاکمیت سامانه‌های هوش مصنوعی تأکید می‌کنند (بهاومیک و همکاران، ۲۰۲۲: ۱۲؛ مک‌اینتاش و همکاران، ۲۰۲۴: ۱؛ انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی، ۲۰۲۵: ۱۲)

یافته‌های پژوهش باهدف نخست مطالعه همخوانی دارد و تا حد زیادی شکاف مطرح‌شده در مقدمه را تأیید می‌کند. مقایسه رویکردهای مطرح‌شده از سوی هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی با مطالعات انجام‌شده در داخل کشور نشان می‌دهد که میان این دو حوزه هنوز فاصله‌هایی وجود دارد و روند حرکت آن‌ها به سمت یک رویکرد مشترک و هماهنگ کامل نشده است (هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی، ۲۰۲۴ و ۲۰۲۶؛ سلیمانی امیری و محمدی سه‌دران، ۱۴۰۳: ۱). در چنین شرایطی، تدوین راهنماها و دستورالعمل‌های عملیاتی متناسب با ویژگی‌ها و الزامات محیط حسابرسی ایران می‌تواند به کاهش این فاصله و استفاده مؤثرتر از رویکردهای نوین در حسابرسی فناوری اطلاعات کمک کند.

ازسوی‌دیگر، نتایج پژوهش رونقی و محمودی (۱۳۹۴: ۶۱۵) درباره ارتباط میان حاکمیت فناوری اطلاعات و حاکمیت شرکتی نشان می‌دهد که موضوع حاکمیت هوش مصنوعی نیز نمی‌تواند صرفاً در محدوده وظایف واحد فناوری اطلاعات قرار گیرد و لازم است در سطح ساختار حاکمیتی سازمان نیز موردتوجه باشد. همچنین، باتوجه‌به گسترش استفاده از سامانه‌های هوش مصنوعی، افزایش دانش و مهارت حسابرسان در زمینه مفاهیم پایه این فناوری و شیوه‌های ارزیابی توضیح‌پذیری مدل‌ها، می‌تواند نقش مهمی در تقویت توانمندی حرفه‌ای حسابرسی و پاسخ‌گویی آن به الزامات جدید در ایران داشته باشد.

مهم‌ترین نوآوری پژوهش حاضر، ارائه یک چارچوب مفهومی سه‌لایه شامل شفافیت فنّی، مستندسازی حاکمیتی و گزارشگری اطمینان‌بخشی است. در این چارچوب، توضیح‌پذیری هوش مصنوعی صرفاً یک ویژگی فنّی در نظر گرفته نشده، بلکه به‌عنوان یکی از اجزای مرتبط با حاکمیت و مدیریت ریسک فناوری اطلاعات و فرایند اطمینان‌بخشی حسابرسی موردتوجه

قرار گرفته است. همچنین، با درنظرگرفتن شرایط سازمانی ایران، این چارچوب می‌تواند مبنایی برای طراحی چک‌لیست‌ها و رویه‌های حسابرسی مرتبط با سامانه‌های هوش مصنوعی و نیز انجام مطالعات تجربی در آینده قرار گیرد.

## نتایج کاربردی

یافته‌های پژوهش می‌تواند برای گروه‌های مختلفی از ذی‌نفعان حرفه‌ای و دانشگاهی قابل‌استفاده باشد. از جمله، مؤسسات حسابرسی می‌توانند با توجه بیشتری به مفاهیم مرتبط باهوش مصنوعی و روش‌های ارزیابی توضیح‌پذیری مدل‌ها بپردازند. باتوجه‌به افزایش توجه نهادهای حرفه‌ای بین‌المللی به آثار فناوری‌های نوظهور بر فرایند حسابرسی و اطمینان‌بخشی، تقویت این مهارت‌ها می‌تواند به آماده‌تر شدن حسابرسان برای مواجهه با سامانه‌های هوش مصنوعی کمک کند (هیئت استانداردهای بین‌المللی حسابرسی و اطمینان‌بخشی، ۲۰۲۴ و ۲۰۲۶). همچنین، چارچوب سه‌لایه ارائه‌شده در این پژوهش می‌تواند نقطه شروعی برای تدوین رویه‌ها و چک‌لیست‌های مرتبط با حسابرسی فناوری اطلاعات در مؤسسات حسابرسی ایران باشد.

در مورد کمیته‌های حسابرسی، نتایج نشان می‌دهد که نظارت بر هوش مصنوعی نباید تنها در سطح واحد فناوری اطلاعات دنبال شود. موضوعاتی مانند مسئولیت‌پذیری، مدیریت ریسک مدل‌ها و نحوه مستندسازی تصمیمات الگوریتمی، نیازمند توجه در سطح مدیریتی و حاکمیتی سازمان هستند (انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی، ۲۰۲۵: ۳؛ سازمان بین‌المللی استانداردسازی، ۲۰۲۳). ازاین‌رو، کمیته‌های حسابرسی می‌توانند در نظارت بر نحوه استفاده سازمان از سامانه‌های هوش مصنوعی و ارزیابی ریسک‌های مرتبط با آن نقش فعال‌تری داشته باشند.

برای نهادهای حرفه‌ای حسابرسی در ایران، از جمله انجمن حسابرسی فناوری اطلاعات ایران، یافته‌های این پژوهش می‌تواند زمینه‌ای برای تدوین راهنماها و دستورالعمل‌های اجرایی متناسب با شرایط کشور فراهم کند. استفاده از چارچوب‌هایی مانند کوبیت و ایزو ۴۲۰۰۱ در کنار درنظرگرفتن الزامات و شرایط محیط حرفه‌ای ایران، می‌تواند به شکل‌گیری رویه‌های منسجم‌تر در زمینه حسابرسی سامانه‌های هوش مصنوعی کمک کند.

همچنین، جدول ۲ پژوهش را می‌توان به‌عنوان یک ابزار اولیه برای بررسی وضعیت و آمادگی سازمان‌ها از منظر حاکمیت هوش مصنوعی در نظر گرفت. بااین‌حال، ازآنجاکه این جدول بر اساس چارچوب مفهومی پژوهش حاضر طراحی شده است، نمی‌توان آن را در وضعیت فعلی یک ابزار عملیاتی نهایی دانست. استفاده گسترده از آن در محیط حرفه‌ای، مستلزم آزمون و اعتبارسنجی تجربی و بررسی میزان قابلیت اتکای شاخص‌های آن در سازمان‌های مختلف است.

در مجموع، نتایج این پژوهش می‌تواند ارتباط میان مباحث نظری مربوط به توضیح‌پذیری هوش مصنوعی و نیازهای عملی حسابرسی فناوری اطلاعات را تا حدی روشن‌تر کند. چارچوب پیشنهادی نیز می‌تواند نقطه شروعی برای توسعه ابزارهای ارزیابی، تدوین رویه‌های حسابرسی و انجام مطالعات تجربی در زمینه حاکمیت و اطمینان‌بخشی سامانه‌های هوش مصنوعی در محیط سازمانی ایران باشد.

پژوهش حاضر از نظر روش‌شناختی ماهیتی مفهومی و مروری دارد و بر داده‌های حاصل از بررسی میدانی یا مطالعه موردی سازمان‌های مشخص استوار نیست. ازاین‌رو، چارچوب سه‌لایه ارائه‌شده در این پژوهش را نمی‌توان به‌عنوان چارچوبی نهایی و آزمون شده در محیط واقعی سازمانی تلقی کرد و بررسی میزان اعتبار و کارایی آن به پژوهش‌های تجربی آینده نیاز دارد. ازسوی‌دیگر، باتوجه‌به جدید بودن استاندارد ایزو ۴۲۰۰۱ و شکل‌گیری تدریجی ادبیات مرتبط با سیستم‌های مدیریت هوش مصنوعی، هنوز شواهد کافی درباره نحوه استقرار، ارزیابی و کنترل الزامات این استاندارد در سازمان‌های ایرانی وجود ندارد؛ بنابراین، بخشی از چالش‌های اجرایی و الزامات بومی‌سازی آن همچنان نیازمند بررسی بیشتر است (مک‌اینتاش و همکاران، ۲۰۲۴: ۱؛ سازمان بین‌المللی استانداردسازی، ۲۰۲۳).

محدودیت دیگر به تفاوت میان زمینه پژوهش حاضر و بخش قابل‌توجهی از مطالعات پیشین مربوط می‌شود. بسیاری از پژوهش‌های انجام‌شده در سایر کشورها، توضیح‌پذیری هوش مصنوعی و حسابرسی مدل‌ها را عمدتاً از منظر فنی بررسی کرده‌اند یا بر استفاده از هوش مصنوعی به‌عنوان ابزاری برای انجام فرایندهای حسابرسی تمرکز داشته‌اند. در مقابل، ارتباط میان توضیح‌پذیری مدل‌های هوش مصنوعی، حاکمیت و مدیریت ریسک فناوری اطلاعات و الزامات حسابرسی فناوری اطلاعات، به‌ویژه در شرایط نهادی، قانونی و سازمانی ایران، کمتر

موردتوجه قرار گرفته است. این موضوع نشان می‌دهد که برای دستیابی به چارچوبی متناسب با شرایط کشور، انجام مطالعات بومی و مبتنی بر تجربه واقعی سازمان‌ها ضروری است.

باتوجه‌به این محدودیت‌ها، چند مسیر برای پژوهش‌های آینده پیشنهاد می‌شود:

۱) آزمون تجربی چارچوب پیشنهادی: چارچوب ارائه‌شده می‌تواند در یک یا چند سازمان ایرانی، به‌ویژه بانک‌ها و مؤسسات مالی، موردمطالعه قرار گیرد. این سازمان‌ها به دلیل استفاده از سامانه‌هایی مانند اعتبارسنجی، تشخیص تقلب و تصمیم‌گیری الگوریتمی، بستر مناسبی برای بررسی عملی الزامات توضیح‌پذیری و حاکمیت هوش مصنوعی هستند.

۲) بررسی دیدگاه حسابرسان: می‌توان با طراحی و اجرای پرسش‌نامه‌ای معتبر، میزان آمادگی و توانمندی حسابرسان داخلی و مستقل ایران برای ارزیابی حاکمیت هوش مصنوعی، مدیریت ریسک‌های مرتبط با آن و بررسی توضیح‌پذیری سامانه‌های هوش مصنوعی را مورد سنجش قرارداد.

۳) مطالعه تطبیقی چارچوب‌های حاکمیتی: انجام پژوهش‌های تجربی برای مقایسه قابلیت‌ها و محدودیت‌های چارچوب‌هایی همچون کوبیت، ایزو ۴۲۰۰۱ و چارچوب مدیریت ریسک هوش مصنوعی در شرایط واقعی سازمان‌های ایرانی می‌تواند مشخص کند که هر یک از این چارچوب‌ها در کدام بخش از فرایند حاکمیت و حسابرسی هوش مصنوعی کاربرد بیشتری دارند (انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی، ۲۰۲۵؛ سازمان بین‌المللی استانداردسازی، ۲۰۲۳).

۴) تدوین ابزارهای اجرایی متناسب با شرایط ایران: همکاری میان نهادهای حرفه‌ای حسابرسی، از جمله انجمن حسابرسی فناوری اطلاعات ایران، دانشگاه‌ها و متخصصان حوزه فناوری اطلاعات می‌تواند به تدوین راهنماها، دستورالعمل‌ها و چک‌لیست‌هایی منجر شود که علاوه بر توجه به استانداردهای بین‌المللی، با الزامات قانونی، مقرراتی و نیازهای حرفه‌ای حسابرسان در ایران نیز سازگار باشند.

در مجموع، اجرای این پیشنهادها می‌تواند زمینه را برای بررسی تجربی چارچوب پیشنهادی و شناسایی نقاط قوت و ضعف آن در محیط واقعی فراهم کند. چنین مطالعاتی، علاوه بر کاهش فاصله میان مباحث نظری و الزامات عملی حسابرسی فناوری اطلاعات، می‌تواند به شکل‌گیری

ادبیات بومی در زمینه حاکمیت هوش مصنوعی، مدیریت ریسک مدل‌ها و حسابرسی سامانه‌های هوش مصنوعی در ایران کمک کند.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع

احمد حسین، سهیله؛ زواری رضایی، اکبر؛ آشتاب، علی. (۱۴۰۳). تحلیل اثرات حسابداری بخش عمومی، حاکمیت شرکتی و کیفیت حسابرسی بر عملکرد مالی بانک‌ها قبل و پس از کووید-۱۹: رویکرد هوش مصنوعی. *حسابداری و بودجه‌ریزی بخش عمومی*، ۵(۴): ۷۴-۱۰۹. https://doi.org/10.22034/psab.2025.209761

رونقی، محمدحسین؛ فرهادی، پیام؛ خردمند، صنوبر. (۱۳۹۷). ارزیابی حاکمیت فناوری اطلاعات با رویکرد سلسله‌مراتبی خاکستری (مورد مطالعاتی: دانشکده آموزش‌های الکترونیک دانشگاه شیراز). *رشد فناوری*، ۱۴(۵۴): ۹-۱۶. https://sid.ir/paper/145043/en

رونقی، محمدحسین؛ محمودی، جعفر. (۱۳۹۴). رابطه حاکمیت فناوری اطلاعات و حاکمیت شرکتی میان سازمان‌های دولتی حوزه فناوری اطلاعات. *مدیریت فناوری اطلاعات*، ۷(۳): ۶۱۵-۶۳۴. https://doi.org/10.22059/jitm.2015.54329

سلیمانی امیری، غلامرضا؛ محمدی سه‌دران، سارا. (۱۴۰۳). حسابرسی در عصر هوش مصنوعی. *حسابداری و منافع اجتماعی*، ۱۴(۳): ۱-۳۶. https://doi.org/10.22051/jaasci.2024.47350.1862

شاه صاحبی، سید مصطفی؛ دارابی، رؤیا؛ حمیدیان، محسن. (۱۳۹۹). تحلیل توانایی مدیریت با تأکید بر نقش شاخص‌های حسابداری و حاکمیت شرکتی (روش هوش مصنوعی). *دانش حسابداری و حسابرسی مدیریت*، ۹(۳۳): ۷۵-۹۰. https://sid.ir/paper/392637/en

صحت برمچه، اعظم؛ شماخی، حمیدرضا؛ یلفانی، امیر. (۱۴۰۵). ارائه الگوی قضاوت حسابرسی مبتنی بر هوش مصنوعی. *دانش حسابداری و حسابرسی مدیریت*، ۱۵(۶۰): ۱۹۱-۲۱۰. https://doi.org/10.22034/jmaak.2025.77853.4352

## References


Bhaumik, D., Dey, D., & Kayal, S. (2022). A framework for auditing multilevel models using explainability methods. *The International Conference on AI Research Proceedings*, 4(1), 12–21. https://doi.org/10.34190/icair.4.1.874

Cheong, B. C. (2024). Transparency and accountability in AI systems: Safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, 6, 1421273. https://doi.org/10.3389/fhumd.2024.1421273

Hussein, S. A., Zavari Rezaei, A., & Ashtab, A. (2025). Analyzing the impact of public sector accounting, corporate governance, and audit quality on banks' financial performance before and after COVID-19: An artificial intelligence approach. *Journal of Public Sector Accounting and Budgeting*, 5(4), 74–109. https://doi.org/10.22034/psab.2025.209761 (in Persian)

IAASB. (2024). *Technology position statement: 8 guiding actions*. International Auditing and Assurance Standards Board. https://www.iaasb.org/publications/technology-position-statement-8-guiding-actions

IAASB. (2026). *Technology quality management roundtables: Outcomes and next steps*. International Auditing and Assurance Standards Board. https://www.iaasb.org/publications/technology-quality-management-roundtables-outcomes-and-next-steps

IIA. (2024). *Global internal audit standards*. The Institute of Internal Auditors.

ISACA. (2025). *Leveraging COBIT for effective AI system governance*. ISACA. https://www.isaca.org/resources/white-papers/2025/leveraging-cobit-for-effective-ai-system-governance

ISO. (2023). *ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system*. International Organization for Standardization. https://www.iso.org/standard/81230.html

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P. A., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security*, 144, 103964. https://doi.org/10.1016/j.cose.2024.103964

Ronaghi, M. H., Farhadi, P., & Kheradmand, S. (2018). Evaluating information technology governance by grey theory. *Roshd-e-Fanavari*, 14(54), 9–16. https://sid.ir/paper/145043/en (in Persian)

Ronaghi, M. H., & Mahmoudi, J. (2015). The relationship between IT governance and corporate governance among IT-related government organizations. *Journal of Information Technology Management*, 7(3), 615–634. https://doi.org/10.22059/jitm.2015.54329 (in Persian)

Sehat Baramcheh, A., Shamakhi, H. R., & Yalfani, A. (2026). Providing an Audit Judgment Model based on Artificial Intelligence. *Journal of Management Accounting and Auditing Knowledge*, 15(60), 191–210. https://doi.org/10.22034/jmaak.2025.77853.4352 (in Persian)

Shahsahebi, S. M., Darabi, R., & Hamidian, M. (2021). Analysis of Ability Management with Emphasis on the Role of Accounting and Corporate Governance Indicators (Artificial Intelligence Method). *Journal of Accounting Knowledge and Management Auditing*, 9(33), 75–90. https://sid.ir/paper/392637/en (in Persian)

Soleimany Amiri, G., & Mohammadi Sedaran, S. (2024). Auditing in the Age of Artificial Intelligence. *Journal of Accounting and Social Interests*, 14(3), 1–36. https://doi.org/10.22051/jaasci.2024.47350.1862 (in Persian)

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Research Paper**

# The Impact of Corporate Governance and Board Characteristics on Information Technology and Cybersecurity Risks: Evidence from Manufacturing Firms Listed on the Tehran Stock Exchange [1]

**Maryam Ghasemiansaghi [2] and Aghil Farhangian [*3]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 187-232

Received: 2026.08.11
Revised: 2026.09.30
Accepted: 2026.10.28

## Abstract

The purpose of this study is to examine the impact of corporate governance and board characteristics on information technology (IT) and cybersecurity risk disclosure among manufacturing companies listed on the Tehran Stock Exchange. To measure the level of IT and cybersecurity risk disclosure, a researcher-developed index, CSRisk, was designed based on the components of the COBIT 2019 and NIST CSF 2.0 frameworks and evaluated using content analysis of corporate official reports. The research sample comprises 117 manufacturing companies over the period from 2021 to 2025(1400–1404 SH), totaling 585 firm-year observations. The research hypotheses were tested using panel data regression with cross-sectional fixed effects. Explanatory variables include board independence, board size, board financial expertise, board IT expertise, CEO duality, and the presence of a specialized IT/risk committee, while firm size, financial leverage, return on assets(ROA), and Tobin's Q serve as control variables. The empirical findings reveal that, among the examined variables, only the presence of a specialized IT/risk committee exhibits a statistically significant relationship with the level of IT and cybersecurity risk disclosure. The direction of this relationship is negative, indicating that the existence of such a committee is associated with a reduction in public cyber risk disclosure. This phenomenon can be attributed to the adoption of a "security confidentiality" approach and a preference for internal risk management over public disclosure.

**Keywords**: Corporate Governance; Board of Directors; Cybersecurity Risk Disclosure; Cybersecurity; Information Technology.

**JEL classification:** *G34, M41, M15, G32.*

---

[1] https://doi.org/10.22034/JISTA.2026.578486.1085
[1] Selected paper of the 2nd National Conference on Corporate Governance and Information Technology Risk Management
[2] Department of Management and Accounting, National University of Skills, Tehran, Iran. Email: mehrabghasemy6@gmail.com
[3] Department of Accounting, ST.C., Islamic Azad University, Tehran, Iran. (Corresponding Author). Email: aghil.farhangian@iau.ac.ir

## 1. INTRODUCTION

In the contemporary digital economy, corporate information technology (IT) systems and cyber assets have become integral to strategic operations, value creation, and competitive positioning. Concurrently, the proliferation, sophistication, and severity of cyber threats have elevated cybersecurity and IT-related risks from operational hazards to primary strategic and systemic challenges. Effective corporate governance mechanisms are conventionally perceived as structural instruments that enforce financial transparency, mitigate information asymmetry, and promote voluntary disclosures to safeguard shareholder wealth. However, within the specific domain of cybersecurity, corporate boards encounter an acute informational and strategic paradox: while capital markets, institutional investors, and regulatory bodies demand granular disclosures to evaluate corporate risk exposures accurately, public disclosure of technical vulnerabilities, incident management architectures, or security configurations creates significant proprietary hazards. Malicious external actors may exploit detailed disclosures, inadvertently jeopardizing firm security and corporate value. Grounded in Agency Theory, Resource Dependency Theory, and Proprietary Cost Theory, this empirical research investigates the relationship between board structural characteristics, specialized governance committees, and the extent of IT and cybersecurity risk disclosure among non-financial manufacturing firms listed on the Tehran Stock Exchange (TSE). By examining an emerging market characterized by regulatory transitions, digital transformation, and geopolitical cyber pressures, this study provides novel empirical insights into the delicate balance between corporate governance oversight and selective confidentiality.

## 2. MATERIALS AND METHODS

The target statistical population encompasses non-financial manufacturing companies continuously listed on the Tehran Stock Exchange over a 5-year observation period from 2021 to 2025 (corresponding to the Iranian calendar years 1400–1404). Applying

a systematic multi-stage screening procedure—excluding financial intermediaries, investment companies, banks, firms with fiscal year-end changes, and entities with incomplete trading or financial datasets—yielded a balanced panel of 117 manufacturing firms, generating 585 firm-year observations.

The dependent variable, the Cybersecurity and Information Technology Risk Disclosure Index ($CSRisk$), was constructed using structured manual content analysis applied to comprehensive annual financial reports, board of directors' activity reports, and published market disclosures. Drawing upon international cybersecurity and governance frameworks—principally COBIT 2019 and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF 2.0)—the disclosure index spans seven core functional dimensions: Governance, Identify, Protect, Detect, Respond, Recover, and Continual Improvement. The finalized checklist encompasses 21 distinct items scored on a trichotomous scale: 0 for non-disclosure, 1 for qualitative or general narrative disclosure, and 2 for specific, quantitative, or technically verifiable disclosure, resulting in a maximum potential disclosure score of 42. Inter-coder reliability was confirmed through independent dual-coding, achieving a Cohen's Kappa coefficient of $\kappa = 0.697$, indicating substantial inter-rater consistency.

The independent variables operationalizing board governance attributes comprise: board independence ($BIND$, proportion of non-executive directors), board size ($BSIZE$, total number of board members), board financial expertise ($BFIN$, proportion of directors holding certified financial, accounting, or economic qualifications), board IT expertise ($BIT$, proportion of directors with formal technological, computer science, or IT backgrounds), CEO duality ($DUAL$, a binary indicator capturing simultaneous tenure as board chairman and chief executive officer), and the presence of a specialized Risk or IT Committee ($ITC$, an indicator variable denoting an active specialized committee). To control for extraneous confounding firm-level heterogeneity, the econometric specifications incorporate firm size ($SIZE$, natural logarithm of total assets), financial leverage ($LEV$, total liabilities over total assets), firm profitability ($ROA$, return on assets), and market valuation prospects ($Tobin's$).

## 3. RESULTS AND DISCUSSION

Descriptive statistics revealed that the dependent variable ($CSRisk$) exhibited a sample mean of 21.19 (standard deviation of 9.23), ranging from 8 to 40, representing an average disclosure level of approximately 45.7% relative to the theoretical maximum. Model specification diagnostics decisively rejected the pooled OLS estimator via the Chow test ($F = 5.563, p < 0.001$). Furthermore, the Hausman specification test yielded a significant test statistic ($\chi^2 = 23.234, p = 0.0099$), confirming that the Cross-Section Fixed Effects panel model was the statistically appropriate estimator. Diagnostic testing for cross-sectional heteroskedasticity indicated residual variance instability; consequently, the empirical model was estimated employing Cross-Section SUR (PCSE) robust standard errors. The fitted regression model exhibited substantial explanatory power ($R^2 = 0.6212$, Adjusted $R^2 = 0.5170$, and $F = 5.962, p < 0.001$).

Contrary to agency theory assumptions regarding internal monitoring efficacy, conventional board governance characteristics failed to demonstrate statistically significant associations with cybersecurity disclosure: board independence ($\beta = 1.495, t = 0.251, p = 0.8018$), board size ($\beta = -1.554, t = -0.206, p = 0.8368$), board financial expertise ($\beta = -4.194, t = -0.393, p = 0.6942$), board IT expertise ($\beta = 0.622, t = 0.059, p = 0.9530$), and CEO duality ($\beta = -2.189, t = -1.026, p = 0.3052$). Likewise, firm-level control variables ($SIZE$, $LEV$, $ROA$, and $Tobin's$) showed no statistically significant coefficients. Crucially, the presence of an active specialized Risk/IT Committee ($ITC$) was the sole explanatory mechanism displaying a statistically significant relationship, exerting a marked negative impact on cybersecurity risk disclosure ($\beta = -8.635, t = -2.239, p = 0.0257$). This empirical outcome directly corroborates Proprietary Cost Theory: specialized committees, possessing advanced technical sophistication and deep comprehension of digital vulnerability landscapes, deliberately curtail public disclosures of cyber risks and IT vulnerabilities to prevent asymmetric exploitation by hostile threat actors and to safeguard critical corporate assets.

## 4. CONCLUSION

The empirical evidence indicates that corporate governance in the context of digital vulnerability operates through selective withholding rather than broad transparency. Specialized IT and risk oversight committees perceive technical cybersecurity disclosures as asymmetric competitive liabilities rather than value-enhancing market signals. Consequently, these governance bodies strategically constrain external disclosure to minimize proprietary costs and avert targeted cyber-attacks. These findings generate vital policy implications for capital market authorities, notably the Securities and Exchange Organization (SEO). Regulatory entities must formulate standardized, mandatory cyber-incident and risk-reporting frameworks that distinguish defensive technical configurations—which warrant strict proprietary confidentiality—from high-level strategic posture and governance assessments required by market participants for sound capital allocation.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# رابطه حاکمیت شرکتی و ویژگی‌های هیئت‌مدیره با ریسک فناوری اطلاعات و امنیت سایبری: شواهدی از شرکت‌های تولیدی پذیرفته‌شده در بورس اوراق بهادار تهران [1]

**مریم قاسمیان سقی [2] و عقیل فرهنگیان *[3]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۱۸۷ - ۲۳۲

تاریخ دریافت: ۱۴۰۵/۰۵/۲۰
تاریخ بازنگری: ۱۴۰۵/۰۷/۰۸
تاریخ پذیرش: ۱۴۰۵/۰۸/۰۶

## چکیده

*هدف پژوهش حاضر بررسی تأثیر حاکمیت شرکتی و ویژگی‌های هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های تولیدی پذیرفته‌شده در بورس اوراق بهادار تهران است. در این پژوهش، به‌منظور سنجش سطح افشای ریسک فناوری اطلاعات و امنیت سایبری، شاخص پژوهشگرساخته CSRisk بر اساس مؤلفه‌های چارچوب COBIT 2019 و NIST CSF 2.0 طراحی و با استفاده از تحلیل محتوای گزارش‌های رسمی شرکت‌ها اندازه‌گیری شد. نمونه پژوهش شامل ۱۱۷ شرکت تولیدی طی دوره ۱۴۰۰ تا ۱۴۰۴ و در مجموع ۵۸۵ مشاهده شرکت ـ سال است. برای آزمون فرضیه‌ها از رگرسیون داده‌های تابلویی با اثرات ثابت مقطعی استفاده شد. متغیرهای توضیحی پژوهش شامل استقلال، اندازه، تخصص مالی و تخصص فناوری اطلاعات هیئت‌مدیره، دوگانگی مدیرعامل و وجود کمیته تخصصی ریسک فناوری اطلاعات و متغیرهای کنترلی شامل اندازه شرکت، اهرم مالی، بازده دارایی‌ها و کیوتوبین بودند. نتایج پژوهش نشان داد در میان متغیرهای مورد بررسی، تنها وجود کمیته تخصصی فناوری اطلاعات/ریسک رابطه آماری معناداری با سطح افشای ریسک فناوری اطلاعات و امنیت سایبری دارد. جهت این رابطه منفی است؛ بدین معنا که وجود کمیته مذکور با کاهش میزان افشای عمومی ریسک‌های سایبری همراه است؛ پدیده‌ای که می‌تواند ناشی از اتخاذ رویکرد «محرمانگی امنیتی» و تمرکز بر مدیریت درون‌سازمانی ریسک‌ها به‌جای افشای عمومی آن‌ها باشد.*

**واژه‌های کلیدی:** *حاکمیت شرکتی، هیئت‌مدیره، افشای ریسک امنیت سایبری، امنیت سایبری، فناوری اطلاعات.*

**طبقه‌بندی موضوعی:** *G34, M41, M15, G32.*

---

[1] https://doi.org/10.22034/JISTA.2026.578486.1085

[1] مقاله منتخب دومین همایش ملی حاکمیت شرکتی و مدیریت ریسک‌های فناوری اطلاعات

[2] گروه مدیریت و حسابداری، دانشگاه شریعتی، تهران، ایران. (mehrabghasemy6@gmail.com)

[3] گروه حسابداری، واحد تهران‌جنوب، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول). (aghil.farhangian@iau.ac.ir)

## مقدمه

تحول دیجیتال و گسترش فناوری‌های نوین، شیوه انجام فعالیت‌های اقتصادی، پردازش اطلاعات و تصمیم‌گیری سازمان‌ها را به طور اساسی تغییر داده است. وابستگی فزاینده شرکت‌ها به سامانه‌های اطلاعاتی، رایانش ابری، هوش مصنوعی و زیرساخت‌های دیجیتال، در کنار ایجاد فرصت‌های جدید، سازمان‌ها را با ریسک‌های گسترده‌ای همچون اختلال سامانه‌ها، افشای اطلاعات، حملات سایبری و تهدیدهای مرتبط با امنیت داده مواجه کرده است. ازاین‌رو، افشای ریسک فناوری اطلاعات و امنیت سایبری دیگر صرفاً یک موضوع فنّی و درون‌سازمانی نیست، بلکه به یکی از موضوعات مهم حاکمیت شرکتی و مسئولیت‌های نظارتی هیئت‌مدیره تبدیل شده است. شواهد پژوهش‌های اخیر نیز بر اهمیت نظارت هیئت‌مدیره و تخصص فناوری اطلاعات اعضای آن در تقویت حاکمیت و افشای ریسک‌های سایبری تأکید دارند (گائو وکالدرون [1]، ۲۰۲۵: ۸؛ لینگ و همکاران [2]، ۲۰۲۵: ۶).

در این میان، ساختار و ویژگی‌های هیئت‌مدیره می‌تواند بر توانایی شرکت در شناسایی، ارزیابی، کنترل و افشای ریسک‌های فناوری اطلاعات و امنیت سایبری اثرگذار باشد. استقلال و اندازه هیئت‌مدیره، تخصص مالی و فناوری اطلاعات اعضا، دوگانگی مدیرعامل و وجود ساختارهای تخصصی مانند کمیته ریسک فناوری اطلاعات، از جمله سازوکارهایی هستند که می‌توانند کیفیت نظارت بر ریسک‌های دیجیتال را تحت‌تأثیر قرار دهند (جنسن و مکلینگ [3]، ۱۹۷۶: ۳۱۰). اهمیت این موضوع برای شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران، باتوجه‌به حجم بالای اطلاعات، ارتباط مستمر با سرمایه‌گذاران و وابستگی روزافزون فعالیت آنها به فناوری‌های دیجیتال، دوچندان است. باوجوداین، بخش عمده مطالعات داخلی حاکمیت شرکتی بر عملکرد، کیفیت گزارشگری مالی و ریسک‌های مالی متمرکز بوده و نقش ویژگی‌های هیئت‌مدیره در افشای ریسک فناوری اطلاعات و امنیت سایبری کمتر مورد بررسی قرار گرفته است؛ بنابراین، بررسی این رابطه در محیط نهادی و اطلاعاتی ایران می‌تواند شکاف موجود در ادبیات پژوهش را تا حدی پوشش دهد.

---

[1] Gao & Calderon
[2] Ling et al.
[3] Jensen & Meckling

باتوجه‌به محدودیت دسترسی پژوهشگران و ذی‌نفعان بیرونی به اطلاعات داخلی مربوط به فرایندهای افشای ریسک فناوری اطلاعات و امنیت سایبری، سنجش مستقیم کیفیت مدیریت این ریسک‌ها در سطح شرکت دشوار است. ازاین‌رو، در پژوهش حاضر، «افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری» به‌عنوان سنجه قابل مشاهده‌ای از میزان توجه سازمان به شفافیت، پاسخگویی و اطلاع‌رسانی درباره سازوکارهای مرتبط با این ریسک‌ها در نظر گرفته شده است. براین‌اساس، هدف پژوهش حاضر بررسی تأثیر ویژگی‌های حاکمیت شرکتی و هیئت‌مدیره بر میزان افشای ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های نمونه است.

## مبانی نظری و توسعه فرضیه‌ها

افزایش وابستگی شرکت‌ها به فناوری اطلاعات و زیرساخت‌های دیجیتال، ریسک‌های ناشی از اختلال سامانه‌ها، حملات سایبری، افشای اطلاعات و نقض محرمانگی داده‌ها را به یکی از مهم‌ترین ریسک‌های نوظهور سازمانی تبدیل کرده است. در چنین شرایطی، افشای ریسک فناوری اطلاعات و امنیت سایبری را نمی‌توان صرفاً مسئولیتی فنّی در سطح واحد فناوری اطلاعات دانست؛ بلکه این موضوع به بخشی از نظام حاکمیت شرکتی و نظارت هیئت‌مدیره تبدیل شده است. چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری[1] با افزودن و برجسته‌سازی کارکرد حاکمیت[2] در کنار شناسایی[3]، حفاظت[4]، تشخیص[5]، پاسخگویی[6] و بازیابی[7]، بر نقش حاکمیت و مدیریت ارشد در هدایت و نظارت بر ریسک سایبری تأکید می‌کند (پاسکو و همکاران[8]، ۲۰۲۴: ۱۴). از سوی دیگر، چارچوب کوبیت ۲۰۱۹ نیز فناوری اطلاعات را در چارچوب حاکمیت و مدیریت سازمانی قرار داده و بر بهینه‌سازی ریسک، پاسخگویی و ایجاد ارزش از فناوری اطلاعات تأکید دارد(ایساکا[9]، ۲۰۱۹: ۴۲).

[1] NIST CSF 2.0
[2] Govern
[3] Identify
[4] Protect
[5] Detect
[6] Respond
[7] Recover
[8] *Pascoe* et al.
[9] ISACA

از منظر نظری، نظریه نمایندگی یکی از مبانی اصلی تبیین رابطه میان ویژگی‌های هیئت‌مدیره و مدیریت ریسک سایبری است بر اساس این نظریه، جدایی مالکیت از مدیریت می‌تواند موجب شکل‌گیری تضاد منافع و عدم تقارن اطلاعاتی میان مدیران و سهام‌داران شود. در این شرایط، هیئت‌مدیره به‌عنوان سازوکار اصلی نظارت بر مدیریت، باید بر ریسک‌های اساسی شرکت نیز نظارت کند. ریسک‌های فناوری اطلاعات و امنیت سایبری، به دلیل آثار بالقوه آنها بر عملکرد، ارزش شرکت و اعتبار سازمان، بخشی از همین مسئولیت نظارتی محسوب می‌شوند (امانی و همکاران[1]، ۲۰۲۵: ۶۱۰)؛ بنابراین، هرچه ظرفیت نظارتی هیئت‌مدیره بیشتر باشد، انتظار می‌رود شرکت سازوکارهای منسجم‌تری برای افشای ریسک‌های سایبری ایجاد کند (الودات و همکاران[2]، ۲۰۲۵: ۱۸؛ هروکس و فورتین[3]، ۲۰۲۴: ۵۴۰).

در کنار نظریه نمایندگی، نظریه وابستگی به منابع نیز می‌تواند رابطه میان ویژگی‌های هیئت‌مدیره و حاکمیت ریسک فناوری اطلاعات را توضیح دهد (پفر و سالانسیک[4]، ۲۰۰۳: ۴۵). بر اساس این دیدگاه، هیئت‌مدیره علاوه بر نقش نظارتی، منبعی از دانش، تجربه، ارتباطات و تخصص برای شرکت محسوب می‌شود. از این منظر، تنوع تخصصی اعضای هیئت‌مدیره، به‌ویژه برخورداری از دانش مالی و فناوری اطلاعات، می‌تواند ظرفیت شرکت برای شناخت و پاسخگویی به ریسک‌های پیچیده دیجیتال را افزایش دهد. همچنین، دیدگاه مبتنی بر منابع بیان می‌کند که دانش و تخصص اعضای هیئت‌مدیره می‌تواند به‌عنوان یک منبع سازمانی ارزشمند، قابلیت شرکت را برای مواجهه با محیط‌های پیچیده و متغیر افزایش دهد (الودات و همکاران، ۲۰۲۵: ۶).

این مبانی نظری با شواهد تجربی جدید نیز سازگار است؛ لینگ و همکاران (۲۰۲۵) با بررسی شرکت‌های پذیرفته‌شده چینی طی سال‌های ۲۰۰۷ تا ۲۰۲۲ نشان دادند که حضور اعضای دارای سابقه فناوری اطلاعات در هیئت‌مدیره، حاکمیت ریسک سایبری شرکت را بهبود می‌دهد و این اثر از طریق افزایش سرمایه‌گذاری فناوری اطلاعات و نوآوری دیجیتال نیز تقویت می‌شود. همچنین گائو و کالدرون[5] (۲۰۲۵) نشان دادن که نظارت هیئت‌مدیره و تخصص سایبری اعضای

[1] Amani et al.
[2] Alodat et al.
[3] Héroux & Fortin
[4] Pfeffer and Salancik
[5] Gao & Calderon

آن با افشای طولانی‌تر، شفاف‌تر و مشخص‌تر ریسک‌های امنیت سایبری ارتباط دارد؛ بااین‌حال، هنگامی که نظارت هیئت‌مدیره جنبه نمادین داشته باشد و از سوی کمیته تخصصی پشتیبانی نشود، این اثر کاهش می‌یابد.

شواهد جدید در سال ۲۰۲۵ نیز اهمیت ساختار هیئت‌مدیره را تأیید می‌کند. مطالعه‌ای بر شرکت‌های فوتسی ۱۰۰[1] بریتانیا نشان داده است که اندازه هیئت‌مدیره با سطح افشای امنیت سایبری رابطه مثبت دارد و وجود کمیته اختصاصی امنیت سایبری نیز به ارائه اطلاعات آینده‌نگرتر درباره ریسک‌ها و اقدامات کاهنده منجر می‌شود (الودات و همکاران، ۲۰۲۵: ۱۰). در محیط ایران نیز افزایش توجه سیاست‌گذاران به امنیت سایبری نشان‌دهنده اهمیت فزاینده این موضوع است. برای نمونه، «سند ستاد توسعه علوم و فناوری افتا» در سال ۱۴۰۴ با هدف توسعه ظرفیت‌های علمی و فناورانه امنیت سایبری به تصویب رسید (هیئت وزیران، ۱۴۰۴: مصوبه شماره ۳۶۶۰۸).

باوجود این تحولات، شواهد تجربی درباره رابطه میان ساختار هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های ایرانی همچنان محدود است. همچنین، مطالعات موجود عمدتاً یکی از ابعاد ساختار هیئت‌مدیره، مانند استقلال یا تخصص فناوری را بررسی کرده‌اند و کمتر پژوهشی مجموعه‌ای از ویژگی‌های ساختاری، تخصصی و نظارتی هیئت‌مدیره را به‌صورت هم‌زمان با یک شاخص ترکیبی و ساختاریافته برای افشای ریسک فناوری اطلاعات و امنیت سایبری ارزیابی نموده‌اند. پژوهش حاضر با تمرکز بر شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران و استفاده از شاخصی مبتنی بر چارچوب کوبیت ۲۰۱۹ و چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری، درصدد پاسخگویی به این خلأ است.

## استقلال هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

استقلال هیئت‌مدیره یکی از مهم‌ترین سازوکارهای حاکمیت شرکتی برای کاهش مشکلات نمایندگی و تقویت نظارت بر مدیریت است. اعضای مستقل و غیرموظف به دلیل وابستگی کمتر به مدیریت اجرایی و تمایل به حفظ اعتبار و سرمایه حرفه‌ای خود، از انگیزه و

[1] FTSE100

ظرفیت بیشتری برای ارزیابی بی‌طرفانه تصمیمات مدیران و نظارت بر ریسک‌های اساسی شرکت برخوردارند (هروکس و فورتین، ۲۰۲۴: ۵۳۱). در حوزه امنیت سایبری نیز استقلال هیئت‌مدیره موجب می‌شود موضوعات مرتبط با امنیت اطلاعات، کنترل‌های فناوری و ریسک‌های دیجیتال با دیدگاه مستقل‌تر و نقادانه‌تری بررسی شوند و احتمال پنهان‌سازی یا کم‌اهمیت جلوه دادن آسیب‌پذیری‌های سایبری توسط مدیران اجرایی کاهش یابد (ماتمانه و همکاران[1]، ۲۰۲۴: ۳۸؛ الودات و همکاران[2]، ۲۰۲۵: ۷؛ گائو و کالدرون، ۲۰۲۵: ۴).

از منظر نظریه نمایندگی، هیئت‌مدیره مستقل می‌تواند عدم تقارن اطلاعاتی میان مدیران و سهام‌داران را کاهش داده و مدیران را نسبت به شناسایی و افشای ریسک‌های بااهمیت پاسخگوتر کند؛ بنابراین، انتظار می‌رود شرکت‌هایی که از هیئت‌مدیره مستقل‌تری برخوردارند، سازوکارهای نظارتی قوی‌تر و سطح افشای جامع‌تری در زمینه ریسک‌های فناوری اطلاعات و امنیت سایبری داشته باشند. شواهد پژوهش‌های جدید نیز نشان می‌دهد ویژگی‌های هیئت‌مدیره می‌توانند در شکل‌دهی به کیفیت افشای سایبری مؤثر باشند، هرچند شدت این رابطه به ساختارهای مکمل نظارتی نیز وابسته است (ماتمانه و همکاران، ۲۰۲۴: ۴۸).

**اندازه هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری**

اندازه هیئت‌مدیره از دو مسیر بر کیفیت نظارت اثرگذار است. از یک سو، افزایش تعداد اعضا موجب تنوع بیشتر در دانش، تجربه، تخصص و دیدگاه‌های اعضا شده و ظرفیت هیئت‌مدیره را برای مواجهه با ریسک‌های پیچیده‌ای؛ مانند ریسک سایبری افزایش می‌دهد. ازسوی‌دیگر، بزرگ‌شدن بیش از اندازه هیئت‌مدیره ممکن است هماهنگی، ارتباطات و سرعت تصمیم‌گیری را کاهش دهد. بااین‌حال در زمینه ریسک سایبری، اهمیت تنوع دانش و تخصص برجسته‌تر است. شواهد تجربی شرکت‌های شاخص فوتسی ۱۰۰ نشان داد که اندازه هیئت‌مدیره با سطح افشای امنیت سایبری رابطه مثبت دارد که ناشی از تنوع مهارتی در هیئت‌مدیره‌های بزرگ‌تر است؛ بنابراین، در بازار سرمایه ایران نیز انتظار می‌رود اندازه بهینه هیئت‌مدیره، ظرفیت نظارت بر ریسک‌های دیجیتال را بهبود بخشد (الودات و همکاران، ۲۰۲۵: ۹).

[1] Matemane et al.
[2] Alodat et al.

### تخصص مالی هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

تخصص مالی اعضای هیئت‌مدیره یکی از ویژگی‌هایی است که می‌تواند کیفیت نظارت بر ریسک‌های سازمانی را افزایش دهد (فصیحی و برشد، ۱۴۰۲: ۴۵؛ اسماعیلی و همکاران[1]، ۲۰۲۳: ۱۱۲). اعضای دارای دانش حسابداری، مالی و حسابرسی، توانایی بیشتری در تحلیل پیامدهای اقتصادی ریسک‌ها، ارزیابی کنترل‌های داخلی و تفسیر اطلاعات مالی دارند. اگرچه امنیت سایبری در ظاهر ماهیتی فناورانه دارد، پیامدهای آن می‌تواند مستقیماً به زیان مالی، کاهش ارزش شرکت، اختلال عملیاتی، هزینه‌های بازیابی و کاهش اعتماد سرمایه‌گذاران منجر شود (امانی و همکاران، ۲۰۲۵: ۶۰۸).

از این منظر، تخصص مالی می‌تواند به هیئت‌مدیره کمک کند تا ریسک فناوری اطلاعات را صرفاً به‌عنوان یک مسئله فنّی تلقی نکند، بلکه پیامدهای مالی و راهبردی آن را نیز ارزیابی کند؛ بنابراین، انتظار می‌رود هیئت‌مدیره‌هایی که از اعضای دارای تخصص مالی بیشتری برخوردارند، انگیزه و توان بیشتری برای نظارت بر افشای ریسک‌های فناوری اطلاعات و امنیت سایبری داشته باشند (اسماعیلی و همکاران، ۲۰۲۳: ۱۱۵).

این استدلال با منطق نظریه نمایندگی نیز سازگار است؛ زیرا اعضای دارای تخصص مالی می‌توانند کیفیت نظارت بر گزارشگری و کنترل‌های مرتبط با ریسک را تقویت کنند و از کاهش شفافیت ناشی از عدم تقارن اطلاعاتی جلوگیری نمایند (امانی و همکاران، ۲۰۲۵: ۶۱۲).

### تخصص فناوری اطلاعات هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

تخصص فناوری اطلاعات را می‌توان یکی از مهم‌ترین قابلیت‌های هیئت‌مدیره در عصر تحول دیجیتال دانست. پیچیدگی تهدیدهای سایبری، وابستگی شرکت‌ها به سامانه‌های اطلاعاتی و سرعت تغییر فناوری موجب شده است که نظارت مؤثر بر این حوزه بدون درک حداقلی از فناوری‌های نوین، معماری اطلاعات، امنیت داده‌ها و تهدیدهای سایبری دشوار باشد.

لینگ و همکاران (۲۰۲۵) در مطالعه شرکت‌های بورسی چین نشان دادند که وجود مدیران دارای سابقه فناوری اطلاعات، به طور معناداری حاکمیت ریسک سایبری را بهبود می‌دهد و این اثر از طریق افزایش سرمایه‌گذاری فناوری اطلاعات و نوآوری دیجیتال نیز شکل می‌گیرد.

---

[1] Smaili et al.

همچنین، پژوهش گائو و کالدرون (۲۰۲۵) درباره حاکمیت ریسک سایبری نشان داد که تخصص سایبری هیئت‌مدیره با افشای دقیق‌تر و باکیفیت‌تر ریسک‌های امنیت سایبری ارتباط دارد؛ بنابراین، انتظار می‌رود حضور اعضای دارای دانش و تجربه فناوری اطلاعات در هیئت‌مدیره شرکت‌های ایرانی نیز ظرفیت شناسایی، ارزیابی و نظارت بر ریسک‌های فناوری و امنیت سایبری را افزایش دهد. در کنار ویژگی‌های مدیرعامل، ویژگی‌های فردی مدیران ارشد نیز مستقیماً بر میزان افشای سایبری اثرگذار است (ترین و همکاران[1]، ۲۰۲۵: ۳).

**دوگانگی مدیرعامل و افشای ریسک فناوری اطلاعات و امنیت سایبری**

دوگانگی مدیرعامل به ساختاری اشاره دارد که در آن یک فرد به طور هم‌زمان سمت مدیرعامل و ریاست هیئت‌مدیره را بر عهده دارد. این ساختار از یک سو با ایجاد وحدت فرماندهی، تسریع تصمیم‌گیری و بهبود هماهنگی میان مدیریت اجرایی و هیئت‌مدیره همراه است؛ اما ازسوی‌دیگر استقلال نظارتی هیئت‌مدیره را کاهش می‌دهد و قدرت نظارت مدیران غیرموظف بر مدیرعامل را محدود می‌کند (نمازی و ابراهیمی میمند، ۱۳۹۵: ۱؛ الشیراح[2]، ۲۰۲۴: ۵۴).

از منظر نظریه نمایندگی، تجمیع هم‌زمان قدرت اجرایی و نظارتی در دست یک فرد می‌تواند تعارض منافع را تشدید و اثربخشی سازوکارهای کنترل مدیریت را تضعیف کند (الشاعر و همکاران[3]، ۲۰۲۵). این مسئله در زمینه ریسک‌های فناوری اطلاعات و امنیت سایبری از اهمیت بیشتری برخوردار است؛ زیرا تصمیمات مرتبط با سرمایه‌گذاری فناوری، طراحی کنترل‌های امنیتی و افشای ریسک، ذاتاً به نظارت مستقل هیئت‌مدیره نیازمندند (ترین و همکاران، ۲۰۲۵: ۳).

بنابراین، از منظر تئوری نمایندگی انتظار می‌رود در صورت وجود هم‌زمانی احتمالی سمت مدیرعامل و رئیس هیئت‌مدیره، استقلال نظارت بر ریسک‌های فناوری اطلاعات و امنیت سایبری کاهش‌یافته و در نتیجه سطح افشای این ریسک‌ها پایین‌تر باشد؛ هرچند مقررات

[1] Trinh et al.
[2] Alshira'h
[3] Al-Shaer et al.

حاکمیت شرکتی سازمان بورس اوراق بهادار تفکیک این دو سمت را الزامی کرده است، اما بررسی نمونه‌های پژوهش نشان‌دهنده لزوم کنترل این متغیر است.

**کمیته ریسک فناوری اطلاعات و افشای ریسک فناوری اطلاعات و امنیت سایبری**

تشکیل کمیته تخصصی ریسک یا فناوری اطلاعات، سازوکاری ساختاریافته برای نظارت مستمر بر تهدیدها، ارزیابی کنترل‌های امنیتی و گزارش‌دهی مستقیم به هیئت‌مدیره به شمار می‌رود. گائو و کالدرون (۲۰۲۵) تأکید می‌کنند که نظارت هیئت‌مدیره درصورتی‌که با پشتیبانی کمیته‌های تخصصی همراه نباشد، از اثربخشی پایینی برخوردار خواهد بود. افزون بر این، الودات و همکاران (۲۰۲۵) نشان دادند شرکت‌های دارای کمیته تخصصی، اطلاعات جامع‌تر و آینده‌نگرانه‌تری پیرامون ریسک‌ها و اقدامات کاهنده ارائه می‌دهند. با این وجود، درخصوص جهت‌گیری اثرگذاری این کمیته‌ها بر سطح افشای عمومی، دو رویکرد نظری متمایز در ادبیات حاکمیت شرکتی قابل ردیابی است:

از یک طرف، بر مبنای نظریه نمایندگی، استقرار این کمیته‌ها از مجرای ارتقای کارآمدی نظارت و کاهش عدم‌تقارن اطلاعاتی، مدیریت را به سمت شفاف‌سازی بیش‌تر مخاطرات و سازوکارهای کنترلی در گزارش‌های برون‌سازمانی سوق می‌دهد (گائو و کالدرون، ۲۰۲۵: ۴؛ الودات و همکاران، ۲۰۲۵: ۹).

در مقابل، نظریه هزینه‌های مالکانه استدلال می‌کند که افشای اطلاعات همواره سودمند نیست؛ زیرا انتشار عمومی اطلاعات حساس، ممکن است به جایگاه رقابتی یا امنیت شرکت آسیب برساند. در حوزه امنیت سایبری، اطلاعات مربوط به زیرساخت‌های فناوری، آسیب‌پذیری‌های سیستم و نقاط ضعف امنیتی، ماهیتی کاملاً استراتژیک و محرمانه دارند. از این دیدگاه، افشای تفصیلی این اطلاعات می‌تواند همانند ارائه یک «نقشه راه» به مهاجمان سایبری و رقبا عمل کرده و احتمال نفوذ و تحمیل هزینه‌های سنگین را به بنگاه افزایش دهد (لینگ و همکاران، ۲۰۲۵: ۶؛ فیروزی و محسنی[1]، ۲۰۲۳: ۴۶۰). از این‌رو، اعضای کمیته‌های تخصصی فناوری اطلاعات و ریسک با درک عمق این مخاطرات و اتخاذ رویکرد «صیانت امنیتی»، ترجیح می‌دهند تمرکز خود را بر تقویت کنترل‌های داخلی سازمان معطوف سازند و از

[1] Firoozi & Mohsni

افشای علنی جزئیات این ریسک‌ها پرهیز کنند. بنابراین، سطح افشای ریسک سایبری حاصل یک موازنه بین دو نیروی متضاد است: ایجاد شفافیت اطلاعاتی برای بازار از یک‌سو، و حفاظت از اطلاعات حساس و حریم امنیتی شرکت از سوی دیگر (هروکس و فورتین، ۲۰۲۴: ۳۸۵).

لینگ و همکاران (۲۰۲۵)، با تحلیل داده‌های شرکت‌های بورسی چین طی سال‌های ۲۰۰۷ تا ۲۰۲۲ دریافتند که حضور اعضای دارای سابقه فناوری اطلاعات در هیئت‌مدیره، حاکمیت ریسک سایبری و نوآوری دیجیتال شرکت را بهبود می‌بخشد.

گائو و کالدرون (۲۰۲۵)، نیز نشان دادند که نظارت هیئت‌مدیره و تخصص سایبری اعضا با افشای طولانی‌تر، شفاف‌تر و مشخص‌تر ریسک‌های امنیت سایبری ارتباط دارد؛ هرچند در صورت نمادین بودن نظارت و نبودِ کمیته اختصاصی، این اثر تضعیف می‌شود.

الودات و همکاران (۲۰۲۵)، بامطالعه شرکت‌های شاخص فوتسی ۱۰۰ بریتانیا دریافتند که اندازه و استقلال هیئت‌مدیره با سطح افشای امنیت سایبری رابطه مثبت دارد و سازوکارهای نظارتی اختصاصی، ارائه اطلاعات آینده‌نگرتر درباره ریسک‌ها و اقدامات کاهنده را تسهیل می‌کند.

ماتمانه و همکاران (۲۰۲۴)، با اتکا به نظریه نمایندگی در بازارهای نوظهور نشان دادند که سازوکارهای نظارتی هیئت‌مدیره، انگیزه مدیران برای پنهان‌سازی ضعف‌های امنیتی را کاهش داده و کیفیت افشای ریسک سایبری را ارتقا می‌دهد.

کرمی و صیفی (۱۴۰۳)، نشان دادند متغیرهای ساختاری هیئت‌مدیره از جمله درصد اعضای غیرموظف و وجود کمیته حسابرسی/ریسک، شرکت‌ها را به ارائه اطلاعات تحلیلی‌تر درباره خطرات نوظهور عملیاتی و دیجیتال ترغیب می‌کند.

فصیحی و برشد (۱۴۰۲)، دریافتند حضور اعضای دارای سواد مالی و تسلط بر فناوری‌های نوین، تمایل به مخفی‌کاری درباره ریسک‌های زیرساختی را کاهش داده و شفافیت شرکتی را به‌صورت معنادار تقویت می‌کند.

بر اساس تئوری نمایندگی، در شرکت‌هایی که با وجود ضوابط سازمان بورس، به‌صورت موردی یا انتقالی مدیرعامل هم‌زمان رئیس یا نایب‌رئیس هیئت‌مدیره است، به دلیل تمرکز قدرت و تضعیف نقش نظارتی هیئت‌مدیره، تمایل کمتری به شفاف‌سازی تهدیدات و آسیب‌پذیری‌های فناوری وجود دارد؛ این موضوع در پژوهش‌های ( نمازی و ابراهیمی میمند،

۱۳۹۵) در بازار ایران و (الگمال و همکاران[1]، ۲۰۱۸) در سطح بین‌المللی مورد تأیید قرار گرفته است.

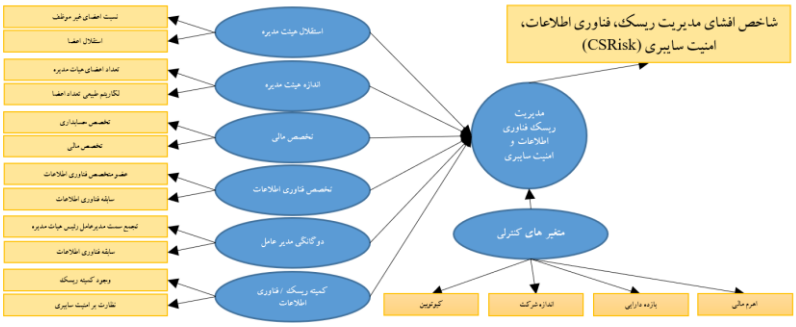
مرور اجمالی پژوهش‌های داخلی از جمله نمازی و ابراهیمی میمند (۱۳۹۵)؛ فصیحی و برشد (۱۴۰۲) و کرمی و صیفی (۱۴۰۳) حاکی از آن است که ادبیات موجود عمدتاً بر افشای ریسک‌های سنتی (مالی، اعتباری و بازار) یا شفافیت گزارشگری مالی متمرکز بوده‌اند و باوجود رشد تهدیدات دیجیتال، ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های تولیدی ایرانی کمتر به‌صورت تجربی و با یک شاخص ترکیبی و ساختاریافته ارزیابی شده است. افزون بر این، در ادبیات داخلی متغیرهای نوینی مانند تخصص فناوری اطلاعات اعضای هیئت‌مدیره و وجود کمیته تخصصی ریسک/فناوری اطلاعات، به‌ندرت در کنار متغیرهای کلاسیک حاکمیت شرکتی و متغیرهای کنترلی مالی در قالب یک مدل یکپارچه آزمون شده‌اند. پژوهش حاضر باهدف پوشش این شکاف، به تبیین نقش هم‌زمان این ویژگی‌ها با استفاده از شاخص ترکیبی در شرکت‌های تولیدی بورس اوراق بهادار تهران طی سال‌های ۱۴۰۰ تا ۱۴۰۴ می‌پردازد.

## فرضیه‌های پژوهش

- استقلال هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- اندازه هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- تخصص مالی هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- تخصص فناوری اطلاعات هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- دوگانگی مدیرعامل بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- بین وجود کمیته تخصصی فناوری اطلاعات/ریسک در هیئت‌مدیره و سطح افشای ریسک فناوری اطلاعات و امنیت سایبری رابطه معناداری وجود دارد.

[1] Elgammal et al.

## مدل مفهومی پژوهش




**شکل ۱.** مدل مفهومی پژوهش

## روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، کاربردی و از نظر روش اجرا، توصیفی ـ همبستگی و مبتنی بر تحلیل داده‌های کمّی است. هدف پژوهش، بررسی تجربی تأثیر ویژگی‌های حاکمیت شرکتی و ساختار هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری شرکت‌های تولیدی پذیرفته‌شده در بورس اوراق بهادار تهران است. داده‌های پژوهش از طریق بررسی اسناد و گزارش‌های منتشرشده شرکت‌ها در دوره زمانی ۱۴۰۰ تا ۱۴۰۴ گردآوری و پس از آماده‌سازی، با استفاده از روش‌های آماری مناسب تجزیه‌وتحلیل شد.

در این پژوهش، افشای ریسک فناوری اطلاعات و امنیت سایبری به‌عنوان متغیر وابسته و ویژگی‌های هیئت‌مدیره شامل استقلال، اندازه، تخصص مالی، تخصص فناوری اطلاعات، دوگانگی مدیرعامل و وجود کمیته تخصصی ریسک فناوری اطلاعات به‌عنوان متغیرهای توضیحی در نظر گرفته شد. همچنین اندازه شرکت، اهرم مالی، بازده دارایی‌ها و کیوتوبین به‌عنوان متغیرهای کنترلی وارد مدل شدند.

## جامعه آماری و نمونه پژوهش

جامعه آماری پژوهش حاضر شامل کلیه شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران در بازه زمانی پنج‌ساله ۱۴۰۰ الی ۱۴۰۴ است. در این پژوهش، تمرکز بر شرکت‌های تولیدی (غیرمالی) قرار گرفته است؛ چرا که نهادهای مالی و واسطه‌گری نظیر بانک‌ها، بیمه‌ها و شرکت‌های سرمایه‌گذاری به دلیل ماهیت عملیاتی متمایز، ساختار ترازنامه و سرمایه متفاوت و همچنین تبعیت از الزامات نظارتی و استانداردهای گزارشگریِ خاصِ نهادهای بالادستی (نظیر بانک مرکزی و بیمه مرکزی)، از سازوکارهای حاکمیتی و رفتارهای افشای متفاوتی نسبت به بخش تولیدی پیروی می‌کنند. بنابراین، ادغام آن‌ها با شرکت‌های تولیدی موجب ناهمگنی شدید و سوگیری در نتایج مدل‌های رگرسیونی می‌گردید.

**جدول ۱**

*جامعه آماری پژوهش*

| مرحله | معیار | تعداد شرکت‌های باقیمانده |
|---|---|---|
| ۱ | کل شرکت‌های جامعه آماری | ۳۹۵ |
| ۲ | حذف شرکت دارای توقف معاملاتی بیش از ۳ ماه و عدم دسترسی به اطلاعات | (۸۰) |
| ۳ | حذف شرکت‌هایی که سال مالی آنها منتهی به اسفندماه نیست | (۷۵) |
| ۴ | حذف شرکت‌های سرمایه‌گذاری، بانک و بیمه | (۱۲۳) |
| **نهایی** | **شرکت‌های واجد شرایط** | **۱۱۷** |

پس از اعمال محدودیت‌های فوق، تعداد ۱۱۷ شرکت به‌عنوان نمونه نهایی پژوهش انتخاب شد که با درنظرگرفتن دوره زمانی پنج‌ساله، مجموعاً ۵۸۵ مشاهده شرکت سال را تشکیل می‌دهند.

## روش گردآوری اطلاعات

اطلاعات پژوهش به روش کتابخانه‌ای و اسنادی گردآوری شد. برای استخراج اطلاعات مربوط به متغیرهای حاکمیت شرکتی و ویژگی‌های هیئت‌مدیره، گزارش‌های هیئت‌مدیره،

صورت‌های مالی، گزارش‌های سالانه و سایر اطلاعات منتشرشده توسط شرکت‌ها بررسی شد. همچنین اطلاعات مالی موردنیاز برای محاسبه متغیرهای کنترلی از صورت‌های مالی و اطلاعات تاریخی شرکت‌ها استخراج گردید. برای سنجش افشای ریسک فناوری اطلاعات و امنیت سایبری، گزارش‌های هیئت‌مدیره و سایر گزارش‌های رسمی شرکت‌ها با استفاده از تحلیل محتوای ساختاریافته بررسی شد. شاخص مورداستفاده با اتکا به مؤلفه‌های مرتبط با حاکمیت، مدیریت ریسک و امنیت سایبری در چارچوب COBIT 2019 و NIST CSF 2.0 طراحی شد و اطلاعات کیفی موجود در گزارش‌های شرکت‌ها به شاخص کمی و قابل‌مقایسه تبدیل گردید.

### سنجش متغیر وابسته و نحوه گردآوری اطلاعات

متغیر وابسته پژوهش، شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری ($CSRisk$) است که میزان جزئیات افشای شرکت را در ۷ حوزه (حاکمیت، شناسایی، حفاظت، کشف، پاسخ، بازیابی و بهبود مستمر) اندازه‌گیری می‌کند. با توجه به عدم دسترسی مستقیم به فرآیندهای درون‌سازمانی، اسناد رسمی شرکت‌ها در دوره ۱۴۰۰ تا ۱۴۰۴ شامل «گزارش‌های هیئت‌مدیره»، «یادداشت‌های توضیحی صورت‌های مالی» و «گزارش‌های کنترل داخلی و حسابرس» از طریق سامانه کدال ($Codal.ir$) و پایگاه مدیریت فناوری بورس استخراج شد (داده‌های مالی کنترلی نیز با استفاده از پایگاه ره‌آورد نوین صحه‌گذاری شدند). سپس با استفاده از روش تحلیل محتوای ساختاریافته، متون اسناد بر مبنای ۲۱ قلم افشا (برگرفته از استانداردهای *COBIT 2019* و *NIST CSF 2.0*) ارزیابی شدند. امتیاز هر قلم در مقیاس سه‌سطحی (عدم افشا: ۰، افشای کلی: ۱، و افشای تفصیلی: ۲) تعیین شد؛ به‌گونه‌ای که مجموع امتیازات شاخص $CSRisk$ را در دامنه ۰ تا ۴۲ تشکیل می‌دهد.

### تعریف عملیاتی متغیرهای پژوهش

تعریف عملیاتی متغیرهای پژوهش در جدول ۲ نشان داده شده است.

**جدول ۲**

*تعریف عملیاتی متغیر های پژوهش*

| نوع متغیر | متغیر | نماد | تعریف عملیاتی |
|---|---|---|---|
| وابسته | افشای ریسک فناوری اطلاعات و امنیت سایبری | CSRisk | شاخص افشای مبتنی بر مؤلفه‌های COBIT 2019 و NIST CSF |
| مستقل | استقلال هیئت‌مدیره | BIND | نسبت اعضای غیرموظف/مستقل به کل اعضای هیئت‌مدیره |
| مستقل | اندازه هیئت‌مدیره | BSIZE | لگاریتم طبیعی تعداد اعضای هیئت‌مدیره |
| مستقل | تخصص مالی هیئت‌مدیره | BFIN | نسبت اعضای دارای تحصیلات یا تجربه حرفه‌ای مرتبط با مالی، حسابداری یا حسابرسی به کل اعضا |
| مستقل | تخصص فناوری اطلاعات | BIT | نسبت اعضای دارای تحصیلات یا تجربه حرفه‌ای مرتبط با فناوری اطلاعات، سیستم‌های اطلاعاتی یا امنیت سایبری به کل اعضا |
| مستقل | دوگانگی مدیرعامل | DUAL | در صورت هم‌زمانی سمت مدیرعامل و رئیس هیئت‌مدیره برابر ۱ و در غیر این صورت صفر |
| مستقل | کمیته ریسک فناوری اطلاعات | ITC | متغیر مجازی؛ در صورت وجود کمیته تخصصی مرتبط با ریسک فناوری اطلاعات/امنیت سایبری برابر ۱ و در غیر این صورت صفر |
| کنترلی | اندازه شرکت | Size | لگاریتم طبیعی مجموع دارایی‌های شرکت |
| کنترلی | اهرم مالی | Lev | نسبت کل بدهی‌ها به کل دارایی‌ها |
| کنترلی | بازده دارایی‌ها | ROA | نسبت سود خالص به کل دارایی‌ها |
| کنترلی | Q توبین | TQ | ارزش بازار حقوق صاحبان سهام + ارزش دفتری بدهی‌ها / ارزش دفتری دارایی‌ها |

## مدل آزمون فرضیه‌ها

برای آزمون فرضیه‌های پژوهش، از مدل رگرسیون چندمتغیره استفاده می‌شود. مدل پایه پژوهش به‌صورت زیر تعریف می‌شود:

$$CSRisk_{i,t} = \beta_0 + \beta_1 BIND_{i,t} + \beta_2 BSIZE_{i,t} + \beta_3 BFIN_{i,t} + \beta_4 BIT_{i,t} + \beta_5 DUAL_{i,t} + \beta_6 ITC_{i,t} + \beta_7 Size_{i,t} + \beta_8 Lev_{i,t} + \beta_9 ROA_{i,t} + \beta_{10} TQ_{i,t} + \varepsilon_{i,t}$$

که در آن، CSRisk افشای ریسک فناوری اطلاعات و امنیت سایبری، BIND استقلال هیئت‌مدیره، BSIZE اندازه هیئت‌مدیره، BFIN تخصص مالی، BITتخصص فناوری اطلاعات، DUAL دوگانگی مدیرعامل و ITC وجود کمیته ریسک فناوری اطلاعات است. همچنین Size، Lev، ROA و TQ متغیرهای کنترلی مدل هستند. در آزمون فرضیه‌ها، علامت و معناداری ضرایب $\beta_1$ تا $\beta_6$ مبنای ارزیابی فرضیه‌های پژوهش قرار می‌گیرد. به طور مشخص، انتظار می‌رود ضرایب استقلال هیئت‌مدیره، اندازه هیئت‌مدیره، تخصص مالی، تخصص فناوری اطلاعات و کمیته ریسک فناوری اطلاعات مثبت و ضریب دوگانگی مدیرعامل منفی باشد.

## فنون تجزیه‌وتحلیل داده‌ها

در مرحله نخست، از آمار توصیفی شامل میانگین، میانه، انحراف معیار، حداقل و حداکثر برای توصیف متغیرهای پژوهش استفاده و سپس پیش‌فرض‌های لازم برای برآورد مدل بررسی شد. از جمله این آزمون‌ها می‌توان به بررسی هم‌خطی بین متغیرهای توضیحی، ناهمسانی واریانس، خودهمبستگی و وابستگی مقطعی اشاره کرد. باتوجه‌به ساختار داده‌ها که شامل اطلاعات چند شرکت در چند سال است، داده‌ها به‌صورت تابلویی تحلیل شدند. پس از تعیین مدل مناسب از طریق آزمون‌های چاو و هاسمن، مدل رگرسیونی با اثرات ثابت مقطعی برآورد و معناداری ضرایب با استفاده از آماره t بررسی شد. همچنین، برای بررسی هم‌خطی میان متغیرهای توضیحی، شاخص‌های VIF و Tolerance محاسبه شدند. در صورت مشاهده ناهمسانی واریانس یا خودهمبستگی بر اساس آزمون‌های تشخیصی مربوط، برآورد مدل با استفاده از خطاهای استاندارد مقاوم یا روش برآورد متناسب با ویژگی داده‌ها انجام شد.

## روایی و پایایی شاخص پژوهش

ازآنجاکه متغیر وابسته با استفاده از یک شاخص پژوهشگرساخته و مبتنی بر تحلیل محتوای گزارش‌های شرکت‌ها اندازه‌گیری می‌شود، اعتبار آن از دو جنبه بررسی شد.

نخست، روایی محتوایی شاخص از طریق انطباق مؤلفه‌ها با چارچوب‌های کوبیت ۲۰۱۹ و چارچوب امنیت سایبری نیست (NIST CSF 2.0)[1] تأمین می‌شود. استفاده از چارچوب‌های

[1] NIST Cybersecurity Framework (NIST CSF)

استاندارد و شناخته‌شده بین‌المللی موجب می‌شود شاخص طراحی‌شده ابعاد اصلی حاکمیت، مدیریت و پاسخگویی به ریسک‌های فناوری اطلاعات و امنیت سایبری را پوشش دهد.

دوم، برای افزایش پایایی کدگذاری، دستورالعمل مشخصی برای تحلیل محتوای گزارش‌ها شد و کدگذاری اقلام شاخص بر اساس معیارهای ازپیش‌تعیین‌شده انجام شد. در صورت امکان، بخشی از گزارش‌ها توسط کدگذار دوم نیز بررسی و میزان توافق میان کدگذاران با استفاده از ضریب مناسب توافق ارزیابی می‌شود.

## مراحل انجام پژوهش

فرایند اجرای پژوهش در چند مرحله انجام شد:

- مرحله اول: شناسایی مبانی نظری و مطالعات مرتبط با حاکمیت شرکتی، ساختار هیئت‌مدیره، افشای ریسک فناوری اطلاعات و امنیت سایبری.
- مرحله دوم: طراحی شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری بر اساس مؤلفه‌های مرتبط در چارچوب‌ها.
- مرحله سوم: شناسایی شرکت‌های جامعه آماری و اعمال معیارهای انتخاب نمونه.
- مرحله چهارم: جمع‌آوری گزارش‌های سالانه، گزارش‌های هیئت‌مدیره، صورت‌های مالی و سایر اطلاعات موردنیاز شرکت‌ها برای دوره ۱۴۰۰ تا ۱۴۰۴.
- مرحله پنجم: کدگذاری اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری و محاسبه شاخص CSRisk.
- مرحله ششم: محاسبه متغیرهای مستقل و کنترلی بر اساس اطلاعات منتشرشده شرکت‌ها.
- مرحله هفتم: انجام آمار توصیفی و آزمون‌های تشخیصی و بررسی ویژگی‌های داده‌های ترکیبی.
- مرحله هشتم: برآورد مدل رگرسیونی و آزمون فرضیه‌های پژوهش.
- مرحله نهم: تفسیر ضرایب، بررسی معناداری روابط و ارائه نتایج و پیامدهای کاربردی پژوهش.

در مجموع، پژوهش حاضر با استفاده از داده‌های شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران طی سال‌های ۱۴۰۰ تا ۱۴۰۴، رابطه میان ویژگی‌های حاکمیت شرکتی و هیئت‌مدیره

و سطح افشای ریسک فناوری اطلاعات و امنیت سایبری را بررسی کرد. نوآوری رو ش‌شناختی پژوهش در این است که به‌جای اتکا به سنجه‌های کلی ریسک، شاخص مشخصی برای افشای ریسک فناوری اطلاعات و امنیت سایبری بر اساس چارچوب‌های کوبیت ۲۰۱۹ (COBIT 2019)و چارچوب امنیت سایبری ان‌آی‌اس‌تی (NIST CSF) ایجاد شده و سپس ارتباط آن با ویژگی‌های ساختاری و تخصصی هیئت‌مدیره در قالب داده‌های ترکیبی آزمون می‌شود.

## طراحی و محاسبه شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری(CSRisk)

در پژوهش حاضر، به‌منظور اندازه‌گیری سطح افشای ریسک فناوری اطلاعات و امنیت سایبری، شاخصی ترکیبی با عنوان CSRisk طراحی شده است. مبنای طراحی این شاخص، مؤلفه‌های مرتبط با حاکمیت، مدیریت ریسک و امنیت سایبری بر اساس چارچوب‌های کوبیت ۲۰۱۹ وچارچوب امنیت سایبری(NIST CSF 2.0) است.

انتخاب این دو چارچوب به این دلیل است که کوبیت ۲۰۱۹ بر حاکمیت و مدیریت فناوری اطلاعات در سطح سازمان تأکید دارد، در حالی که چارچوب امنیت سایبری نیست (NIST CSF 2.0) چارچوبی ساختاریافته برای مدیریت ریسک امنیت سایبری ارائه می‌کند. ترکیب این دو رویکرد امکان می‌دهد شاخص پژوهش علاوه بر جنبه‌های فنّی امنیت سایبری، ابعاد حاکمیتی، مدیریتی، کنترلی و پاسخگویی ریسک‌های فناوری اطلاعات را نیز پوشش دهد.

**جدول ۳**

*چارچوب شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری CSRisk*

| بُعد اصلی | مؤلفه مورد بررسی | نمونه موارد قابل‌شناسایی در گزارش شرکت | منبع چارچوبی |
|---|---|---|---|
| حاکمیت و راهبری | مسئولیت هیئت‌مدیره و مدیریت ارشد | اشاره به مسئولیت هیئت‌مدیره، مدیریت ارشد یا کمیته تخصصی در قبال امنیت اطلاعات و ریسک سایبری | COBIT 2019 / NIST CSF 2.0 |
| | سیاست‌ها و راهبرد امنیت سایبری | وجود سیاست، برنامه یا راهبرد رسمی امنیت اطلاعات و سایبری | COBIT 2019 / NIST CSF 2.0 |
| | نظارت بر ریسک فناوری اطلاعات | اشاره به نظارت، گزارش‌دهی یا پایش ریسک‌های فناوری اطلاعات | COBIT 2019 / NIST CSF 2.0 |
| | شناسایی دارایی‌ها و زیرساخت‌های اطلاعاتی | شناسایی سامانه‌ها، داده‌ها، زیرساخت‌ها و دارایی‌های دیجیتال | NIST CSF 2.0 |

| بُعد اصلی | مؤلفه مورد بررسی | نمونه موارد قابل‌شناسایی در گزارش شرکت | منبع چارچوبی |
|---|---|---|---|
| **شناسایی و ارزیابی ریسک** | شناسایی تهدیدها و آسیب‌پذیری‌ها | اشاره به تهدیدهای سایبری، آسیب‌پذیری‌ها یا مخاطرات فناوری | NIST CSF 2.0 |
| | ارزیابی ریسک | شناسایی، ارزیابی یا اولویت‌بندی ریسک‌های فناوری اطلاعات و سایبری | COBIT 2019 / NIST CSF 2.0 |
| **حفاظت و کنترل** | کنترل دسترسی | کنترل دسترسی کاربران، احراز هویت و مدیریت مجوزها | NIST CSF 2.0 |
| | حفاظت از داده‌ها | پشتیبان‌گیری، رمزنگاری، حفاظت از اطلاعات محرمانه و داده‌های حساس | NIST CSF 2.0 |
| | کنترل‌های امنیتی و فناوری | استفاده از کنترل‌ها و راهکارهای امنیتی برای حفاظت از سامانه‌ها | COBIT 2019 / NIST CSF 2.0 |
| **کشف و پایش** | پایش مستمر | نظارت مستمر بر سامانه‌ها و رویدادهای امنیتی | NIST CSF 2.0 |
| | شناسایی رخدادهای سایبری | سازوکارهای شناسایی حملات، نفوذ و رخدادهای امنیتی | NIST CSF 2.0 |
| | ارزیابی کنترل‌ها | ممیزی، ارزیابی یا آزمون اثربخشی کنترل‌های فناوری اطلاعات | COBIT 2019 |
| **پاسخ و مدیریت رخداد** | برنامه پاسخ به رخداد | وجود برنامه یا رویه مشخص برای مقابله با رخدادهای سایبری | NIST CSF 2.0 |
| | مسئولیت‌ها و فرایند پاسخگویی | تعیین مسئولیت افراد یا واحدهای سازمانی در زمان وقوع رخداد | NIST CSF 2.0 |
| | اطلاع‌رسانی و گزارش رخداد | گزارش‌دهی رخدادهای مهم به مدیریت یا مراجع ذی‌ربط | NIST CSF 2.0 |
| **بازیابی و تاب‌آوری** | تداوم کسب‌وکار | برنامه‌های تداوم فعالیت در صورت اختلال فناوری یا حمله سایبری | COBIT 2019 / NIST CSF 2.0 |
| | بازیابی سامانه‌ها و داده‌ها | پشتیبان‌گیری و بازیابی اطلاعات و سامانه‌ها پس از رخداد | NIST CSF 2.0 |
| | درس‌آموخته‌ها و بهبود مستمر | اصلاح فرایندها و کنترل‌ها پس از رخدادهای امنیتی | NIST CSF 2.0 |
| **مدیریت و بهبود مستمر** | آموزش و آگاهی امنیتی | آموزش کارکنان و افزایش آگاهی امنیت سایبری | COBIT 2019 / NIST CSF 2.0 |
| | مدیریت ریسک تأمین‌کنندگان | توجه به ریسک‌های امنیتی ناشی از طرف‌های ثالث و تأمین‌کنندگان | NIST CSF 2.0 |
| | بهبود مستمر حاکمیت سایبری | بازنگری سیاست‌ها، کنترل‌ها و فرایندهای مدیریت ریسک | COBIT 2019 / NIST CSF 2.0 |

منبع: یافته‌های پژوهشگر

این ساختار، ۲۱ قلم قابل مشاهده برای سنجش افشای ریسک فناوری اطلاعات و امنیت سایبری را در هفت حوزه محتوایی پوشش می‌دهد. هر قلم بر اساس محتوای واقعی گزارش‌های رسمی شرکت‌ها کدگذاری و امتیازدهی شد و مجموع امتیازات به‌عنوان شاخص CSRisk مورداستفاده قرار گرفت.

**نحوه امتیازدهی**: برای هر قلم، در صورت نبود اطلاعات مربوط، امتیاز صفر؛ در صورت ارائه اطلاعات کلی، امتیاز یک؛ و در صورت ارائه اطلاعات مشخص، تفصیلی و قابل‌شناسایی، امتیاز دو در نظر گرفته شد؛ بنابراین، امتیاز بالاتر بیانگر سطح بالاتر افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری است.

**روش امتیازدهی شاخص:** برای جلوگیری از قضاوت ذهنی و افزایش قابلیت تکرارپذیری پژوهش، برای هر قلم شاخص از مقیاس امتیازدهی سه سطحی استفاده می‌شود.

**جدول ٤**

*روش امتیاز دهی شاخص‌ها*

| وضعیت افشا | امتیاز | معیار |
|---|---|---|
| عدم افشا | ۰ | هیچ اطلاعات قابل‌شناسایی درباره مؤلفه موردنظر ارائه نشده است |
| افشای کلی | ۱ | به موضوع اشاره شده، اما اطلاعات محدود و غیر تفصیلی است |
| افشای مشخص و تفصیلی | ۲ | اطلاعات مشخص، قابل‌مشاهده و نسبتاً تفصیلی درباره سازوکار، فرایند یا اقدام شرکت است |

استفاده از مقیاس سه سطحی امکان تمایز میان نبود افشا، افشای کلی و افشای مشخص و تفصیلی را فراهم می‌کند و در مقایسه با کدگذاری دودویی، اطلاعات بیشتری درباره عمق و سطح جزئیات افشا در اختیار پژوهش قرار می‌دهد. امتیاز خام هر شرکت ـ سال از رابطه زیر محاسبه می‌شود:

$$\mathrm{CSRisk}_{it} = \sum_{j=1}^{21} Score_{ijt}$$

حداکثر امتیاز قابل کسب برابر است با:

$$\mathbf{0} \leq \mathrm{CSRisk}_{it} \leq \mathbf{42}$$

$$\text{Maximum Score} = 21 \times 2 = 42$$

حداکثر امتیاز نظری شاخص برابر با ۴۲ است؛ بنابراین، CSRisk = 0 نشان‌دهنده نبود افشای قابل‌شناسایی در اقلام شاخص و CSRisk = 42 نشان‌دهنده دریافت بالاترین امتیاز ممکن در تمام اقلام شاخص است. در نتیجه، مقدار بالاتر CSRisk بیانگر سطح بالاتر افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری است.

### کنترل روایی شاخص CSRisk

به‌منظور کنترل روایی محتوایی شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری، ابتدا فهرست اولیه‌ای مشتمل بر ۲۴ مؤلفه بر پایه چارچوب‌های بین‌المللی COBIT 2019 و NIST CSF 2.0 تدوین گردید. سپس این فهرست به همراه تعاریف عملیاتی در اختیار پنلی متشکل از ۷ نفر از خبرگان دانشگاهی و حرفه‌ای (شامل ۳ عضو هیئت‌علمی حسابداری و حاکمیت شرکتی، ۲ حسابرس ارشد معتمد بورس و ۲ متخصص مدیریت فناوری اطلاعات و امنیت سایبری) قرار گرفت. خبرگان هر مؤلفه را از حیث «میزان اهمیت»، «ارتباط مفهومی با افشای ریسک» و «قابلیت سنجش در گزارش‌های هیئت‌مدیره بورس تهران» ارزیابی نمودند. بر اساس جمع‌بندی نظرات خبرگان:

- سه مؤلفه به دلیل همپوشانی بالا و عدم امکان افشای عمومی به دلایل محرمانگی (نظیر افشای مستقیم آسیب‌پذیری‌های فنّی و تفکیک جزئی درس‌آموخته‌ها) حذف یا در سایر مؤلفه‌ها ادغام گردیدند.
- سه مؤلفه جدید و بااهمیت متناسب با بستر گزارشگری ایران (از جمله الزام به افشای گواهینامه‌های انطباق و استانداردهای امنیتی، ممیزی‌های دوره‌ای فناوری اطلاعات و نظارت کمیته‌های تخصصی هیئت‌مدیره) به چارچوب افزوده شد.
- نگارش و تعریف عملیاتی ۴ مؤلفه نیز به‌منظور رفع ابهام و سهولت در کدگذاری اصلاح شد.

در نهایت، ۲۱ مؤلفه نهایی در قالب ۷ بُعد اصلی (شامل: ۱. حاکمیت و راهبری، ۲. شناسایی و ارزیابی ریسک، ۳. حفاظت و کنترل، ۴. کشف و پایش، ۵. پاسخ و مدیریت رخداد، ۶. بازیابی

و تاب‌آوری، ۷. مدیریت و بهبود مستمر) به تأیید نهایی پنل خبرگان رسید و مبنای کدگذاری و سنجش شاخص SCRISK در پژوهش حاضر قرار گرفت.

### پایایی کدگذاری شاخص

به‌منظور بررسی پایایی فرایند کدگذاری شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری، ۴۰ شرکت به‌صورت تصادفی انتخاب شد و گزارش‌های آنها در کل دوره ۱۴۰۰ تا ۱۴۰۴ به‌صورت مستقل توسط کدگذار دوم کدگذاری شد و سپس میزان توافق میان دو کدگذار با استفاده از ضریب کاپای کوهن در نرم‌افزار SPSS محاسبه گردید. مقدار ضریب کاپا برابر با ۰/۶۹۷ به دست آمد که بیانگر توافق قابل‌قبول میان دو کدگذار در فرایند کدگذاری اقلام شاخص است. موارد اختلاف نیز از طریق بازبینی تعاریف عملیاتی اقلام و بررسی مجدد متن گزارش‌ها تعیین تکلیف و همسان‌سازی شد.

## یافته‌های پژوهش

### آمار توصیفی پژوهش

خلاصه آماره‌های توصیفی متغیرهای مورد بررسی شامل شاخص‌های مرکزی (میانگین و میانه) و شاخص‌های پراکندگی (انحراف معیار، حداقل و حداکثر) در جدول ۵ قابل مشاهده است.

نتایج مندرج در جدول ۵ نشان می‌دهد متغیر وابسته افشای ریسک فناوری اطلاعات و امنیت سایبری دارای میانگین ۲۱/۱۹ و انحراف معیار ۹/۲۳ است. دامنه تغییرات این شاخص بین حداقل ۸ و حداکثر ۴۰ قرار دارد. با توجه به حداکثر امتیاز نظری ۴۲، میانگین مشاهده‌شده معادل حدود ۴۵/۷ درصد از حداکثر امتیاز قابل کسب است که بیانگر سطح متوسط افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های مورد بررسی است. همچنین، انحراف معیار شاخص نشان‌دهنده تفاوت قابل توجه در سطح افشای این اطلاعات میان شرکت‌های نمونه است. علاوه بر این، آماره‌های مربوط به دوگانگی مدیرعامل نشان می‌دهد میانگین این متغیر ۰/۰۷ است؛ این مقدار بیانگر آن است که تنها در حدود ۷ درصد از مشاهدات سال-شرکت، هم‌زمانی این دو سمت یا عدم تفکیک کامل مشاهده شده و در اکثریت قریب به اتفاق شرکت‌ها تفکیک وظایف رعایت شده است.

**جدول ۵**

*آماره‌های توصیفی متغیرهای پژوهش*

| نماد متغیر | نام متغیر | میانگین | میانه | حداکثر | حداقل | انحراف معیار |
|---|---|---|---|---|---|---|
| CSRISKe | افشای ریسک فناوری اطلاعات و سایبری | ۱۹/۲۱ | ۱۵/۰۰ | ۴۰/۰۰ | ۸/۰۰ | ۹/۲۳ |
| BIND | استقلال هیئت‌مدیره | ۰/۷۱ | ۰/۷۰ | ۱/۰۰ | ۰/۲۰ | ۰/۱۲ |
| BSIZE | اندازه هیئت‌مدیره | ۱/۶۲ | ۱/۶۱ | ۱/۹۵ | ۱/۶۱ | ۰/۰۶ |
| BFIN | تخصص مالی هیئت‌مدیره | ۰/۲۹ | ۰/۳۰ | ۰/۴۰ | ۰/۰۰ | ۰/۱۱ |
| BIT | تخصص فناوری اطلاعات هیئت‌مدیره | ۰/۰۱ | ۰/۰۰ | ۰/۲۰ | ۰/۰۰ | ۰/۰۴ |
| DUAL | دوگانگی وظیفه مدیرعامل | ۰/۰۷ | ۰/۰۰ | ۱/۰۰ | ۰/۰۰ | ۰/۲۶ |
| ITC | کمیته ریسک / فناوری اطلاعات | ۰/۰۳ | ۰/۰۰ | ۱/۰۰ | ۰/۰۰ | ۰/۱۶ |
| SIZE | اندازه شرکت | ۱۷/۴۳ | ۱۷/۱۰ | ۲۲/۴۶ | ۱۳/۰۳ | ۱/۷۸ |
| LEV | اهرم مالی | ۰/۵۲ | ۰/۴۹ | ۲/۶۴ | ۰/۰۸ | ۰/۲۷ |
| ROA | بازده دارایی‌ها | ۲۰/۹۵ | ۲۰/۷۵ | ۷۱/۱۴ | -۶۲/۳۴ | ۱۸/۱۴ |
| TQ | کیوتوبین | ۰/۹۸ | ۰/۹۰ | ۳/۲۰ | ۰/۲۵ | ۰/۳۹ |

منبع: یافته‌های پژوهشگر

## ماتریس همبستگی پیرسون

نتایج ماتریس همبستگی پیرسون در جدول ۶، نشان می‌دهد که ضرایب همبستگی دوتایی میان متغیرهای توضیحی عمدتاً در سطح پایینی قرار دارند. بالاترین همبستگی مثبت میان متغیرهای توضیحی مربوط به تخصص مالی هیئت‌مدیره و استقلال هیئت‌مدیره با ضریب ۰/۳۶ است. با توجه به پایین بودن ضرایب همبستگی دوتایی، نشانه‌ای از همبستگی شدید میان متغیرهای توضیحی مشاهده نمی‌شود. بااین‌حال، ازآنجاکه بررسی همبستگی دوتایی به‌تنهایی برای تشخیص هم‌خطی چندگانه کافی نیست، شاخص‌های VIF و Tolerance نیز محاسبه و در جدول ۷ گزارش شده‌اند.

## جدول ٦

*ماتریس همبستگی پیرسون*

| متغیر | BFIN | BIND | BIT | BSIZE | CSRISK | DUAL | ITC | LEV | ROA | SIZE | TQ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| BFIN | ۱/۰۰ | | | | | | | | | | |
| | — | | | | | | | | | | |
| BIND | ۰/۳۶ | ۱/۰۰ | | | | | | | | | |
| | (۰/۰۰) | — | | | | | | | | | |
| BIT | ۰/۰۱ | ۰/۰۱ | ۱/۰۰ | | | | | | | | |
| | (۰/۷۴) | (۰/۷۴) | — | | | | | | | | |
| BSIZE | −۰/۰۸ | −۰/۰۲ | ۰/۰۱ | ۱/۰۰ | | | | | | | |
| | (۰/۰۴) | (۰/۵۹) | (۰/۸۷) | — | | | | | | | |
| CSRISK | −۰/۰۶ | −۰/۲۱ | ۰/۱۴ | ۰/۰۹ | ۱/۰۰ | | | | | | |
| | (۰/۱۶) | (۰/۰۰) | (۰/۰۰) | (۰/۰۲) | — | | | | | | |
| DUAL | −۰/۲۳ | −۰/۱۴ | −۰/۰۶ | −۰/۰۱ | ۰/۰۱ | ۱/۰۰ | | | | | |
| | (۰/۰۰) | (۰/۰۰) | (۰/۱۳) | (۰/۷۹) | (۰/۸۵) | — | | | | | |
| ITC | ۰/۱۷ | ۰/۰۷ | −۰/۰۴ | −۰/۰۳ | ۰/۰۱ | −۰/۰۵ | ۱/۰۰ | | | | |
| | (۰/۰۰) | (۰/۰۷) | (۰/۳۸) | (۰/۴۹) | (۰/۷۶) | (۰/۲۸) | — | | | | |
| LEV | ۰/۰۳ | −۰/۱۶ | −۰/۰۵ | −۰/۰۳ | ۰/۰۳ | −۰/۰۳ | ۰/۰۴ − | ۱/۰۰ | | | |
| | (۰/۴۷) | (۰/۰۰) | (۰/۲۲) | (۰/۵۲) | (۰/۵۰) | (۰/۵۳) | (۰/۲۶) | — | | | |
| ROA | ۰/۱۰ | ۰/۱۱ | −۰/۰۱ | ۰/۰۲ | −۰/۰۳ | −۰/۰۳ | ۰/۰۶ | −۰/۶۵ | ۱/۰۰ | | |
| | (۰/۰۱) | (۰/۰۱) | (۰/۷۹) | (۰/۶۸) | (۰/۴۲) | (۰/۴۷) | (۰/۱۵) | (۰/۰۰) | — | | |
| SIZE | ۰/۲۷ | ۰/۰۲ | −۰/۰۶ | −۰/۱۹ | ۰/۰۵ | −۰/۱۴ | ۰/۱۹ | −۰/۰۱ | −۰/۰۲ | ۱/۰۰ | |
| | (۰/۰۰) | (۰/۶۰) | (۰/۱۶) | (۰/۰۰) | (۰/۲۰) | (۰/۰۰) | ۰/۰۰) ( | (۰/۷۵) | (۰/۵۹) | — | |
| TQ | ۰/۲۶ | ۰/۰۹ | −۰/۰۷ | −۰/۱۰ | ۰/۰۷ | −۰/۱۰ | ۰/۰۶ | ۰/۰۵ − | ۰/۰۴ | ۰/۱۸ | ۷۰۰ |
| | (۰/۰۰) | (۰/۰۳) | (۰/۰۱) | (۰/۰۲) | (۰/۱۲) | (۰/۰۲) | (۰/۱۶) | (۰/۲۱) | (۰/۳۵) | (۰/۰۰) | — |

منبع: یافته‌های پژوهشگر

**جدول ۷**

*نتیجه شاخص هم خطی*

| متغیر مستقل | $R^2$ کمکی | شاخص VIF | تحمل تقریبی[1] | وضعیت هم‌خطی |
|---|---|---|---|---|
| BIND (استقلال هیئت‌مدیره) | ۰/۱۵۹ | ۱/۱۸۹ | ۰/۸۴۱ | هم‌خطی در سطح قابل‌قبول |
| BSIZE (اندازه هیئت‌مدیره) | ۰/۰۴۴ | ۱/۰۴۶ | ۰/۹۵۶ | هم‌خطی در سطح قابل‌قبول |
| BFIN (تخصص مالی) | ۰/۲۶۴ | ۱/۳۵۹ | ۰/۷۳۶ | هم‌خطی در سطح قابل‌قبول |
| BIT (تخصص فناوری اطلاعات) | ۰/۰۱۶ | ۱/۰۱۷ | ۰/۹۸۴ | هم‌خطی در سطح قابل‌قبول |
| DUAL (دوگانگی مدیرعامل) | ۰/۰۷۵ | ۱/۰۸۲ | ۰/۹۲۵ | هم‌خطی در سطح قابل‌قبول |
| ITC (کمیته فناوری اطلاعات) | ۰/۱۰۱ | ۱/۱۱۳ | ۰/۸۹۹ | هم‌خطی در سطح قابل‌قبول |
| SIZE (اندازه شرکت) | ۰/۱۴۸ | ۱/۱۷۳ | ۰/۸۵۲ | هم‌خطی در سطح قابل‌قبول |
| LEV (اهرم مالی) | ۰/۴۵۶ | ۱/۸۴۰ | ۰/۵۴۴ | هم‌خطی در سطح قابل‌قبول |
| ROA (بازده دارایی‌ها) | ۰/۴۴۳ | ۱/۷۹۶ | ۰/۵۵۷ | هم‌خطی در سطح قابل‌قبول |
| TQ (کیوتوبین) | ۰/۱۱۹ | ۱/۱۳۴ | ۰/۸۸۱ | هم‌خطی در سطح قابل‌قبول |

منبع: یافته‌های پژوهشگر

مطابق نتایج جدول ۷، مقدار VIF تمام متغیرهای توضیحی کمتر از ۲ و مقادیر شاخص تحمل تقریبی نیز بیشتر از ۰/۵۰ است؛ بنابراین، بر اساس معیارهای متعارف، شواهدی از هم‌خطی چندگانه شدید میان متغیرهای توضیحی مشاهده نمی‌شود.

## تحلیل آزمون‌های تشخیصی و انتخاب مدل

برای انتخاب مناسب‌ترین روش برآورد از میان مدل‌های تلفیقی[2] و تابلویی[3] با اثرات ثابت یا تصادفی، از آزمون‌های استاندارد زیر استفاده شده است. تمام محاسبات با استفاده از نرم‌افزار EViews انجام گرفته است.

[1] Tolerance
[2] Pooled
[3] Panel

**بررسی اولیه**

به‌منظور بررسی اولیه رابطه میان ویژگی‌های حاکمیت شرکتی و افشای ریسک فناوری اطلاعات و امنیت سایبری، ابتدا مدل پژوهش با استفاده از روش حداقل مربعات معمولی تلفیقی[1] برآورد شد که نتایج در جدول ۸، قابل مشاهده است.

**جدول ۸**

*نتایج برآورد مدل رگرسیون تجمعی اولیه*

| متغیر | نماد | ضریب | خطای معیار | آماره t | سطح معناداری( $p$ -value) |
|---|---|---|---|---|---|
| عرض از مبدأ | C | -۶/۸۳۰ | ۱۲/۲۰۲ | -۰/۵۶۰ | ۰/۵۷۵۹ |
| استقلال هیئت‌مدیره | BIND | -۱۵/۳۸۱ | ۳/۲۵۷ | -۴/۷۲۳ | ۰/۰۰۰۰ |
| اندازه هیئت‌مدیره | BSIZE | ۱۷/۳۶۷ | ۶/۴۰۸ | ۲/۷۱۰ | ۰/۰۰۶۹ |
| تخصص مالی | BFIN | -۲/۰۴۴ | ۴/۰۳۸ | -۰/۵۰۶ | ۰/۶۱۳۰ |
| تخصص IT | BIT | ۳۳/۶۶۱ | ۸/۷۲۳ | ۳/۸۵۹ | ۰/۰۰۰۱ |
| دوگانگی مدیرعامل | DUAI | ۰/۲۰۰ | ۱/۴۸۱ | ۰/۱۳۵ | ۰/۸۹۲۸ |
| کمیته IT و ریسک | ITC | ۱/۲۸۰ | ۲/۳۹۳ | ۰/۵۳۵ | ۰/۵۹۲۸ |
| اندازه شرکت | SIZE | ۰/۳۷۶ | ۰/۲۲۵ | ۱/۶۷۴ | ۰/۰۹۴۷ |
| اهرم مالی | LEV | ۰/۴۲۳ | ۱/۸۶۸ | ۰/۲۲۷ | ۰/۸۲۰۸ |
| بازده دارایی‌ها | ROA | -۰/۰۰۱ | ۰/۰۲۷ | -۰/۰۵۲ | ۰/۹۵۸۲ |
| کیوتوبین | TQ | ۲/۳۳۷ | ۰/۹۸۱ | ۲/۳۸۲ | ۰/۰۱۷۶ |
| ضریب تعیین($R^2$) | | ۰/۰۸۸ | میانگین متغیر وابسته | | ۱۹/۲۰۹ |
| ضریب تعیین تعدیل‌شده | | ۰/۰۷۲ | انحراف معیار متغیر وابسته | | ۹/۲۳۳ |
| آمارهF | | ۵/۵۰۹ | سطح معناداری آمارهF | | ۰/۰۰۰۰ |
| آماره دوربین - واتسون | | ۰/۶۶۳ | تعداد کل مشاهدات | | ۵۸۵ |

منبع: یافته‌های پژوهشگر

نتایج ارائه‌شده در جدول ۸ نشان می‌دهد که ضریب تعیین $R^2$ مدل برابر با ۰/۰۸۸ است؛ به این معنا که حدود ۸/۸ درصد از تغییرات متغیر وابسته (افشای ریسک فناوری اطلاعات و امنیت سایبری) توسط مجموع متغیرهای توضیحی و کنترلی مدل تبیین می‌شود. همچنین ضریب تعیین تعدیل‌شده برابر با ۰/۰۷۲ برآورد شده است.

[1] Pooled OLS

آماره F مدل برابر با ۵/۵۰۹ و سطح معناداری آن برابر با ۰/۰۰۰است. ازآنجاکه سطح معناداری آماره F کمتر از سطح خطای ۵ درصد است، فرضیه صفر مبنی بر عدم معناداری کلی مدل رد می‌شود؛ بنابراین مدل رگرسیون در مجموع از نظر آماری معنادار بوده و متغیرهای توضیحی به‌صورت هم‌زمان دارای توان تبیین‌کنندگی متغیر وابسته هستند.

در برآورد اولیه به روش تلفیقی، آماره دوربین–واتسون برابر با ۰/۶۶۳ به دست آمد که فاصله قابل‌توجهی از مقدار (۲) دارد و نشان‌دهنده وجود خودهمبستگی مثبت پسماندها و عدم لحاظ ناهمگنی‌های خاص هر شرکت در ساختار تلفیقی است. ازاین‌رو، برای تعیین دقیق ساختار داده‌ها و انتخاب میان روش داده‌های تلفیقی و داده‌های تابلویی و سپس گزینش نوع اثرات (ثابت یا تصادفی)، آزمون‌های تشخیصی چاو (F لیمر) و هاسمن اجرا گردید.

## آزمون چاو (F لیمر)

به‌منظور بررسی وجود ناهمگنی‌های فردی میان شرکت‌های موردمطالعه و انتخاب میان الگوی داده‌های تلفیقی و الگوی داده‌های تابلویی، آزمون چاو (F لیمر) اجرا گردید که در جدول ۹ قابل مشاهده است. فرضیه صفر $H_0$ در این آزمون بیانگر همگنی عرض از مبدأها بین مقاطع و ترجیح روش تلفیقی است، در حالی که فرضیه مقابل $H_1$ بر وجود ناهمگنی‌های مقطعی و برتری روش داده‌های تابلویی تأکید دارد.

**جدول ۹**

*نتایج آزمون چاو*

| نوع آزمون | آماره آزمون | درجه آزادی | سطح معناداری (*p* - value) | نتیجه آزمون | مدل منتخب |
|---|---|---|---|---|---|
| آماره F مقطعی (Cross-section F) | ۵/۵۶۳ | (۴۵۸، ۱۱۶) | ۰/۰۰۰ | رد فرضیه $H_0$ | داده‌های تابلویی |
| آماره کای‌دو مقطعی $\chi 2$ | ۵۱۴/۳۴۵ | ۱۱۶ | ۰/۰۰۰ | رد فرضیه $H_0$ | داده‌های تابلویی |

منبع: یافته‌های پژوهشگر

با توجه به نتایج حاصل از آزمون مطابق جدول ۹، مقدار آماره F مقطعی با درجه آزادی (۴۵۸، ۱۱۶) برابر با ۵/۵۶۳ و سطح معناداری آن برابر با ۰/۰۰۰ به‌دست آمده است. همچنین آماره کای‌دو مقطعی ($X^2$) با ۱۱۶ درجه آزادی برابر با ۵۱۴/۳۴۵ و با سطح معناداری ۰/۰۰۰ گزارش شده است. ازآنجاکه سطح معناداری هر دو آماره بسیار کمتر از سطح خطای ۵ درصد است، فرضیه صفر با اطمینان ۹۵ درصد رد می‌شود؛ بنابراین، تفاوت‌های مقطعی معناداری میان شرکت‌های تولیدی مورد بررسی وجود دارد و استفاده از الگوی داده‌های تابلویی (پانل) نسبت به روش تلفیقی ارجحیت دارد. در گام بعد، برای انتخاب بین مدل تلفیقی و مدل اثرات تصادفی، آزمون نسبت واریانس بروش - پاگان اجرا می‌شود.

### آزمون بروش - پاگان (LM)

برای انتخاب بین مدل تلفیقی و مدل اثرات تصادفی[1]، از آزمون نسبت واریانس بروش - پاگان استفاده شد. فرضیات آزمون به‌صورت جدول ۱۰ است:

**جدول ۱۰**

*نتایج آزمون LM بروش - پاگان*

| نوع اثر | آماره بروش– پاگان | سطح معناداری |
|---|---|---|
| مقطعی(Cross-section) | ۲۲۸/۵۰۳ | ۰/۰۰۰۰ |
| زمانی(Time) | ۱۲/۹۰۴ | ۰/۰۰۰۳ |
| هر دو / کل(Both) | ۲۴۱/۴۰۷ | ۰/۰۰۰۰ |

منبع: یافته‌های پژوهشگر

باتوجه‌به اینکه سطح معناداری آماره آزمون در تمام حالات (مقطعی، زمانی و کل) کمتر از سطح خطای ۱ درصد است($p < 0.01$) ، فرضیه صفر مبنی بر برابری واریانس اثرات مقطعی/زمانی با صفر رد می‌شود. این نتیجه بیانگر عدم کفایت مدل تلفیقی و وجود اثرات تصادفی (ناهمگنی‌های انفرادی و زمانی) در داده‌ها است؛ بنابراین، برآورد مدل با رگرسیون

[1] Random Effects

ساده/تلفیقی مجاز نبوده و جهت انتخاب نهایی میان مدل اثرات ثابت و مدل اثرات تصادفی، انجام آزمون هاسمن ضرورت می‌یابد.

## آزمون هاسمن

به‌منظور انتخاب الگوی برتر میان مدل اثرات ثابت و مدل اثرات تصادفی، از آزمون هاسمن استفاده شد که نتایج آن در جدول ۱۱، قابل مشاهده است. فرضیه صفر این آزمون بر عدم وجود همبستگی میان خطاهای انفرادی مقاطع و متغیرهای توضیحی تأکید داشته و کارایی مدل اثرات تصادفی را تأیید می‌کند؛ در مقابل، فرضیه یک حاکی از وجود همبستگی میان این دو جزء بوده و لزوم به‌کارگیری مدل اثرات ثابت را نشان می‌دهد.

**جدول ۱۱**

*نتایج آزمون هاسمن برای انتخاب بین اثرات ثابت و اثرات تصادفی*

| خلاصه آزمون | آماره کای‌دو | درجه آزادی | سطح معناداری | نتیجه آزمون |
|---|---|---|---|---|
| اثرات تصادفی مقطعی | ۲۳/۲۳۴ | ۱۰ | ۰/۰۰۹۹ | رد فرضیه صفر |

منبع: یافته‌های پژوهشگر

باتوجه‌به نتایج ارائه‌شده در جدول شماره ۱۱ آماره کای‌دو با ۱۰ درجه آزادی برابر با ۲۳/۲۳۴ و سطح معناداری آن برابر با ۰/۰۰۹۹ برآورد گردیده است. ازآنجاکه مقدار سطح معناداری کمتر از سطح خطای ۵ درصد است، فرضیه صفر با اطمینان ۹۹ درصد رد می‌شود؛ بنابراین، مدل داده‌های تابلویی با اثرات ثابت مقطعی به‌عنوان مدل مناسب و برتر جهت برآورد روابط رگرسیونی و آزمون فرضیه‌های پژوهش انتخاب می‌گردد.

## جمع‌بندی مراحل انتخاب مدل

نتایج مراحل انتخاب مدل به‌صورت خلاصه در جدول ۱۲ ارائه شده است.

**جدول ۱۲**

*جمع‌بندی فرآیند انتخاب مدل*

| مرحله | آزمون / روش | مقایسه انجام‌شده | مقدار آماره آزمون | مقدار احتمال | تصمیم و نتیجه‌گیری |
|---|---|---|---|---|---|
| ۱ | حداقل مربعات تلفیقی | برآورد اولیه داده‌ها | — | — | نیاز به اجرای آزمون‌های تشخیص ساختار |
| ۲ | آزمون چاو / لیمر | مدل تلفیقی در برابر اثرات ثابت | ۵/۵۶۳ | ۰/۰۰۰۰ | رد مدل تلفیقی و تأیید مدل تابلویی |
| ۳ | آزمون بروش – پاگان | مدل تلفیقی در برابر اثرات تصادفی | ۲۴۱/۴۰۷ | ۰/۰۰۰۰ | رد مدل تلفیقی و تأیید وجود اثرات تصادفی |
| ۴ | آزمون هاسمن | مدل اثرات ثابت در برابر اثرات تصادفی | ۲۳/۲۳۴ | ۰/۰۰۹۹ | رد مدل اثرات تصادفی و برتری اثرات ثابت |
| ۵ | الگوی نهایی منتخب | تعیین ساختار نهایی مدل رگرسیون | — | — | برآورد نهایی با روش ثابت مقطعی |

منبع: یافته‌های پژوهشگر

آزمون بروش – پاگان نیز وجود اثرات تصادفی را نسبت به مدل تلفیقی تأیید می‌کند؛ بااین‌حال، انتخاب نهایی میان اثرات ثابت و تصادفی بر اساس آزمون هاسمن انجام شد.

### انتخاب مدل نهایی پژوهش

در مرحله نخست، فرض شد که تفاوت معناداری میان شرکت‌ها وجود ندارد و برای همه آن‌ها یک عرض از مبدأ مشترک در نظر گرفته می‌شود. مدل اولیه پژوهش به‌صورت زیر برآورد شد:

$$CSRISKit = \alpha + \beta 1\ BINDit + \beta 2\ BSIZEit + \beta 3\ BFINit + \beta 4\ BITit + \beta 5\ DUALit + \beta 6\ ITCit + \beta 7\ LEVit + \beta 8\ ROAit + \beta 9\ SIZEit + \beta 10\ TQit + \varepsilon it$$

سپس، با انجام مراحل ذکر شده در جدول ۱۲ و انتخاب مدل اثرات ثابت، مدل دوباره در نرم‌افزار EViews برآورد شد؛ اما این بار در بخش Effects Specification گزینه Cross-section Fixed Effects انتخاب شد. در این مدل، برای هر شرکت یک اثر ثابت یا عرض از

مبدأ جداگانه در نظر گرفته می‌شود؛ بنابراین، تفاوت‌های ثابت و مشاهده‌نشده شرکت‌ها، مانند فرهنگ سازمانی، کیفیت مدیریت، ساختار داخلی و ویژگی‌های خاص شرکت، کنترل می‌شود.

براین‌اساس، مدل نهایی پژوهش با درنظرگرفتن اثرات ثابت برای شرکت‌ها به‌صورت زیر برآورد شد:

$$CSRISKit = \alpha i + \beta 1\ BINDit + \beta 2\ BSIZEit + \beta 3\ BFINit + \beta 4\ BITit + \beta 5\ DUALit + \beta 6\ ITCit + \beta 7\ LEVit + \beta 8\ ROAit + \beta 9\ SIZEit + \beta 10\ TQit + \varepsilon it$$

در این مدل، αi بیانگر اثرات ثابت مختص هر شرکت است و تفاوت‌های مشاهده‌نشده و پایدار میان شرکت‌ها را کنترل می‌کند. در نهایت، پس از انتخاب مدل اثرات ثابت مقطعی، رگرسیون نهایی پژوهش برآورد شد.

**جدول ۱۳**

*رگرسیون نهایی پژوهش*

| نام متغیر | نماد متغیر | ضریب β | خطای معیار | آماره t | سطح معناداری ( p - value) |
|---|---|---|---|---|---|
| عرض از مبدأ | C | ۳۳/۹۵۳ | ۱۶/۰۷۰ | ۲/۱۱۳ | ۰/۰۳۵۲ |
| استقلال هیئت‌مدیره | BIND | ۱/۴۹۵ | ۵/۹۵۱ | ۰/۲۵۱ | ۰/۸۰۱۸ |
| اندازه هیئت‌مدیره | BSIZE | -۱/۵۵۴ | ۷/۵۴۰ | -۰/۲۰۶ | ۰/۸۳۶۸ |
| تخصص مالی هیئت‌مدیره | BFIN | -۴/۱۹۴ | ۱۰/۶۶۱ | -۰/۳۹۳ | ۰/۶۹۴۲ |
| تخصص فناوری اطلاعات | BIT | ۰/۶۲۲ | ۱۰/۵۴۰ | ۰/۰۵۹ | ۰/۹۵۳۰ |
| دوگانگی وظیفه مدیرعامل | DUAL | -۲/۱۸۹ | ۲/۱۳۲ | -۱/۰۲۶ | ۰/۳۰۵۲ |
| کمیته فناوری اطلاعات/ریسک | ITC | -۸/۶۳۵ | ۳/۸۵۷ | -۲/۲۳۹ | ۰/۰۲۵۷ |
| اندازه شرکت | SIZE | -۰/۸۵۱ | ۰/۵۷۹ | -۱/۴۶۹ | ۰/۱۴۲۶ |
| اهرم مالی | LEV | -۱/۳۷۱ | ۲/۶۳۴ | -۰/۵۲۰ | ۰/۶۰۳۱ |
| بازده دارایی‌ها | ROA | ۰/۰۴۱ | ۰/۰۳۷ | ۱/۱۱۰ | ۰/۲۶۷۷ |
| کیوتوبین (ارزش بازار) | TQ | ۳/۰۳۹ | ۲/۷۵۷ | ۱/۱۰۲ | ۰/۲۷۰۹ |

منبع: یافته‌های پژوهشگر

بر اساس نتایج مندرج در جدول ۱۳، از میان متغیرهای اصلی حاکمیت شرکتی و ویژگی‌های هیئت‌مدیره، تنها متغیر کمیته فناوری اطلاعات/ریسک دارای ضریب منفی (۸/۶۳۵-) و سطح معناداری کمتر از خطای ۵ درصد ($p = 0.0257$) است؛ این امر نشان می‌دهد وجود کمیته تخصصی ریسک یا فناوری اطلاعات بر سطح افشای ریسک‌های امنیت سایبری تأثیر معنادار دارد. در مقابل، سایر متغیرهای مرتبط با هیئت‌مدیره شامل استقلال ($p = 0.8018$)، اندازه ($p = 0.8368$)، تخصص مالی($p = 0.6942$) ، تخصص فناوری اطلاعات$= p$) (0.9530و دوگانگی وظیفه مدیرعامل ($p = 0.3052$) سطوح معناداری بالاتر از ۰/۰۵ کسب کرده‌اند و بنابراین از نظر آماری تأثیر معناداری بر متغیر وابسته (CSRisk) نداشته‌اند. همچنین، متغیرهای کنترلی پژوهش (اندازه شرکت، اهرم مالی، بازده دارایی‌ها و ارزش بازار) نیز در سطح اطمینان ۹۵ درصد اثر معناداری بر افشای ریسک سایبری نشان ندادند.

برای بررسی اعتبار مدل بر اساس جدول شماره ۱۴ شاخص‌های این مدل موارد زیر استخراج شد.

**جدول ۱٤**

*شاخص های مدل*

| شاخص آماری | مقدار |
|---|---|
| ضریب تعیین($R^2$) | ۰/۶۲۱۲ |
| ضریب تعیین تعدیل‌شده(Adjusted $R^2$) | ۰/۵۱۷ |
| آماره F مدل رگرسیون | ۵/۹۶۲ |
| سطح معناداری آماره F ( $p$ -value p-value) | P<۰/۰۰۱ |
| آماره دوربین – واتسون( D-W D-W) | ۱/۴۸۷ |
| تعداد کل مشاهدات | ۵۸۵ (۱۱۷ شرکت در ۵ سال) |
| روش برآورد | Panel Least Squares (Fixed Effects) |

منبع: یافته‌های پژوهشگر

بر اساس جدول ۱۴، ضریب تعیین مدل برابر با ۰/۶۲۱۲ (حدود ۶۲/۱ درصد از تغییرات متغیر وابسته در چارچوب مشخصات مدل و متغیرهای واردشده به آن تبیین می‌شود) و ضریب تعیین تعدیل‌شده برابر با ۰/۵۱۷ است. همچنین، آماره F مدل برابر با ۵/۹۶۲ و سطح معناداری آن کمتر

از ۰/۰۰۱ گزارش شده است که نشان‌دهنده معناداری کلی مدل رگرسیون در سطح ۱ درصد است. مقدار آماره دوربین–واتسون برابر با ۱/۴۸۷ بوده و قرارگیری مقادیر عامل تورم واریانس (VIF)در دامنه مجاز، حاکی از عدم وجود هم‌خطی چندگانه شدید میان متغیرهای مستقل است.

**جدول ۱۵**

*نتایج فرضیه‌ها*

| فرضیه | متغیر مستقل | ضریب | سطح معناداری | نتیجه فرضیه |
|---|---|---|---|---|
| H1 | استقلال هیئت‌مدیره | ۱/۴۹۵ | ۰/۸۰۱۸ | عدم تأیید |
| H2 | اندازه هیئت‌مدیره | -۱/۵۵۴ | ۰/۸۳۶۸ | عدم تأیید |
| H3 | تخصص مالی | -۴/۱۹۴ | ۰/۶۹۴۲ | عدم تأیید |
| H4 | تخصص IT | ۰/۶۲۲ | ۰/۹۵۳۰ | عدم تأیید |
| H5 | دوگانگی مدیرعامل | -۲/۱۸۹ | ۰/۳۰۵۲ | عدم تأیید |
| H6 | کمیته IT/ ریسک | -۸/۶۳۵ | ۰/۰۲۵۷ | تأیید |

منبع: یافته‌های پژوهشگر

**تفسیر فرضیه‌ها**

**فرضیه اول: استقلال هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.**

نتایج برآورد مدل نشان می‌دهد ضریب مربوط به استقلال هیئت‌مدیره برابر با ۱/۴۹۵ بوده، اما سطح معناداری آن برابر با ۰/۸۰۱۸ است؛ بنابراین، باتوجه‌به بالاتر بودن سطح معناداری از سطح خطای ۵ درصد، شواهد آماری کافی برای تأیید اثر معنادار استقلال هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری مشاهده نشد. ازاین‌رو، فرضیه اول پژوهش تأیید نمی‌شود. این نتیجه به معنای اثبات نبود هرگونه رابطه میان دو متغیر نیست، بلکه بیانگر آن است که در نمونه و دوره مورد بررسی، اثر آماری معناداری مشاهده نشده است.

**فرضیه دوم: اندازه هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.**

ضریب اندازه هیئت‌مدیره برابر با ۱/۵۵۴- و سطح معناداری آن برابر با ۰/۸۳۶۸ به دست آمده است. باتوجه‌به عدم معناداری آماری این ضریب در سطح ۵ درصد، شواهد کافی برای تأیید اثر معنادار اندازه هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری وجود ندارد؛ بنابراین، فرضیه دوم پژوهش تأیید نمی‌شود.

**فرضیه سوم: تخصص مالی اعضای هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.**

نتایج نشان می‌دهد ضریب تخصص مالی اعضای هیئت‌مدیره برابر با ۴/۱۹۴- و سطح معناداری آن برابر با ۰/۶۹۴۲ است؛ بنابراین، رابطه مشاهده‌شده از نظر آماری معنادار نیست و شواهد کافی برای تأیید اثر تخصص مالی هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری به دست نیامد. براین‌اساس، فرضیه سوم پژوهش تأیید نمی‌شود.

**فرضیه چهارم: تخصص فناوری اطلاعات اعضای هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.**

ضریب تخصص فناوری اطلاعات اعضای هیئت‌مدیره برابر با ۰/۶۲۲ و سطح معناداری آن برابر با ۰/۹۵۳۰ است. اگرچه جهت ضریب برآوردشده مثبت است، مقدار سطح معناداری نشان می‌دهد این رابطه از نظر آماری معنادار نیست؛ بنابراین، در نمونه و دوره مورد بررسی، شواهد کافی برای تأیید اثر تخصص فناوری اطلاعات اعضای هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری مشاهده نشد و فرضیه چهارم تأیید نمی‌شود.

**فرضیه پنجم: دوگانگی مدیرعامل بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.**

ضریب دوگانگی مدیرعامل برابر با ۲/۱۸۹- و سطح معناداری آن برابر با ۰/۳۰۵۲ است؛ بنابراین، اثر دوگانگی مدیرعامل بر افشای ریسک فناوری اطلاعات و امنیت سایبری در سطح ۵ درصد معنادار نیست. در نتیجه، شواهد آماری کافی برای تأیید فرضیه پنجم پژوهش وجود ندارد.

**فرضیه ششم: وجود کمیته ریسک یا کمیته فناوری اطلاعات بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.**

ضریب مربوط به وجود کمیته تخصصی فناوری اطلاعات/ریسک برابر با ۸/۶۳۵- و سطح معناداری آن برابر با ۰/۰۲۵۷ است. باتوجه‌به اینکه سطح معناداری کمتر از ۵ درصد می‌باشد، این رابطه از نظر آماری معنادار است. اگرچه علامت منفی ضریب نشان می‌دهد شرکت‌های دارای این کمیته‌ها، میزان افشای ریسک سایبری کمتری در گزارش‌های عمومی خود دارند، اما این یافته از منظر نظری قابل‌تبیین است؛ به این معنا که این کمیته‌ها با درک عمق تهدیدات و بر اساس «نظریه هزینه‌های مالکانه»، جهت جلوگیری از افزایش احتمال حملات هکری و حفظ موقعیت رقابتی، افشای عمومی آسیب‌پذیری‌ها را محدود می‌کنند. همچنین، مهار ریسک‌های سایبری در سطوح درون‌سازمانی توسط این کمیته‌ها، نیاز به افشای گسترده ریسک‌های باقیمانده را کاهش می‌دهد. ازاین‌رو، فرضیه ششم پژوهش با جهت اثر منفی تأیید می‌گردد.

در میان متغیرهای توضیحی مدل، هیچ یک از متغیرها رابطه معناداری با افشای ریسک فناوری اطلاعات و امنیت سایبری نشان ندادند. به‌عنوان نمونه، ضریب مربوط به اهرم مالی برای برابر با ۱/۳۷۰- با سطح معناداری ۰/۶۰۳۱ برآورد شده است که نشان می‌دهد باتوجه‌به بالاتر بودن سطح معناداری از سطح خطای بالای ۵ درصد، اهرم مالی تاثیر معناداری بر میزان افشای ریسک‌های سایبری در شرکت های مورد بررسی ندارد.

## بحث و نتیجه‌گیری

پژوهش حاضر با هدف بررسی تجربی رابطه سازوکارهای حاکمیت شرکتی و ویژگی‌های ساختاری هیئت‌مدیره با سطح افشای ریسک‌های فناوری اطلاعات و امنیت سایبری در شرکت‌های تولیدی پذیرفته‌شده در بورس اوراق بهادار تهران انجام گرفت. با گسترش تحول دیجیتال و تشدید تهدیدات امنیتی، نیاز مبرم بازار سرمایه و ذی‌نفعان به شفافیت اطلاعاتی، تبیین نقش نظارتی ارکان حاکمیتی را ضروری ساخته است. در ادامه، نتایج حاصل از آزمون فرضیه‌های پژوهش به تفکیک مورد بحث، تبیین نظری و مقایسه با ادبیات پیشین قرار می‌گیرد:

### بحث پیرامون فرضیه اول: استقلال هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

یافته‌های پژوهش نشان داد که استقلال هیئت‌مدیره تأثیر معناداری بر سطح افشای ریسک‌های فناوری اطلاعات و امنیت سایبری در شرکت‌های نمونه ندارد و این فرضیه تأیید

نشد. این نتیجه با یافته‌های الودات و همکاران (۲۰۲۵) و ماتمانه و همکاران (۲۰۲۴) که بر اساس نظریه نمایندگی، اعضای مستقل را محرک اصلی ارتقای شفافیت و افشای داوطلبانه ریسک‌ها می‌دانند، غیرهمسو است؛ اما با نتایج هروکس و فورتین (۲۰۲۳) تطابق دارد. در تبیین این ناهمسویی می‌توان بیان نمود که در شرکت‌های فعال در بازار سرمایه ایران، اعضای مستقل و غیرموظف هیئت‌مدیره عمدتاً فاقد سواد و تخصص فنّی لازم در حوزه سامانه‌های اطلاعاتی و پدافند سایبری هستند. افزون بر این، در بسیاری از ساختارهای شرکتی داخلی، حضور اعضای مستقل جنبه انطباق صوری با الزامات دستورالعمل‌های حاکمیت شرکتی را داشته و این اعضا به‌دلیل محدودیت دسترسی به داده‌های عملیاتی و عمق رویدادهای فنّی، نقش فعالی در سیاست‌گذاری افشای ریسک‌های پیچیده فناوری ایفا نمی‌کنند.

## بحث پیرامون فرضیه دوم: اندازه هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

بر اساس یافته‌ها، اندازه هیئت‌مدیره اثر معناداری بر افشای ریسک‌های فناوری اطلاعات و امنیت سایبری بر جای نگذاشت و فرضیه دوم مورد تأیید قرار نگرفت. این یافته با نتیجه الشیراح (۲۰۲۴) که هیئت‌مدیره‌های بزرگ‌تر را به‌دلیل تنوع مهارت‌ها عاملی برای ارتقای سطح افشا دانسته بود، ناهمخوان است؛ لیکن با نتایج فصیحی و برشد (۱۴۰۲) و گائو و کالدرون (۲۰۲۵) همسویی دارد. تبیین نظری این وضعیت بیانگر آن است که اگرچه افزایش تعداد اعضای هیئت‌مدیره می‌تواند منابع و دیدگاه‌های متنوع‌تری فراهم آورد، اما هم‌زمان چالش‌های هماهنگی، کندی فرایند تصمیم‌گیری، تعارضات درون‌گروهی و پدیده سواری رایگان را در نظارت راهبردی تشدید می‌کند؛ بنابراین صرفِ تعدد اعضا بدون داشتن درک تخصصی از تهدیدات دیجیتال، پیامد مثبت معناداری بر شفافیت سایبری در پی نداشته است.

## بحث پیرامون فرضیه سوم: تخصص مالی اعضای هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

نتایج آزمون حاکی از عدم وجود رابطه معنادار میان تخصص مالی اعضای هیئت‌مدیره و سطح افشای ریسک‌های فناوری اطلاعات و امنیت سایبری است؛ ازاین‌رو فرضیه سوم رد شد. این نتیجه با یافته‌های اسماعیلی و همکاران (۲۰۲۳) و امانی و همکاران (۲۰۲۵) که تخصص مالی را پیش‌ران ارتقای شفافیت افشای ریسک در گزارشگری می‌دانند مغایر بوده، اما با

یافته‌های هروکس و فورتین (۲۰۲۳) سازگار است. دلیل این ناهمسویی را می‌توان به تمرکز سنتی مدیران دارای پیشینه مالی و حسابداری در ایران بر شاخص‌های عملکرد مالی، مدیریت سود، مباحث مالیاتی و ساختار تأمین مالی نسبت داد. از منظر این مدیران، مباحث امنیت داده و ریسک زیرساخت‌های فناوری اطلاعات همچنان مقوله‌ای صرفاً فنّی تلقی شده و ارزیابی پیامدهای مالی یا تعهدات ناشی از حملات سایبری در اولویت تصمیمات گزارشگری آنان قرار نگرفته است.

### بحث پیرامون فرضیه چهارم: تخصص فناوری اطلاعات اعضای هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

یافته‌های این مطالعه نشان داد که تخصص فناوری اطلاعات اعضای هیئت‌مدیره رابطه معناداری با افشای ریسک‌های سایبری برقرار نمی‌کند و فرضیه چهارم تأیید نگردید. این یافته با نتایج گائو و کالدرون (۲۰۲۵) و حسینی و همکاران (۱۴۰۱) که حضور مدیران مسلط به فناوری را عاملی کلیدی در جهت‌دهی شرکت به افشای دقیق ریسک‌های دیجیتال معرفی کرده‌اند، غیرهمسو است. دلیل اصلی این نتیجه را باید در بافتار ترکیب هیئت‌مدیره شرکت‌های تولیدی بورس تهران جست‌وجو کرد؛ جایی که تعداد اعضای دارای مدارک یا تجارب مدیریتی مرتبط با فناوری اطلاعات بسیار اندک بوده و این اقلیت محدود توانایی اثرگذاری غالب بر مصوبات جمعی هیئت‌مدیره در خصوص سیاست‌های گزارشگری بیرونی را ندارند.

### بحث پیرامون فرضیه پنجم: دوگانگی وظیفه مدیرعامل و افشای ریسک فناوری اطلاعات و امنیت سایبری

نتایج حاصل از آزمون مدل نشان داد که تمرکز قدرت ناشی از دوگانگی مدیرعامل اثر آماری معناداری بر سطح افشای ریسک امنیت سایبری ندارد و فرضیه پنجم تأیید نشد. این یافته با پژوهش‌های الشاعر و همکاران (۲۰۲۵) و ترین و همکاران (۲۰۲۵) که رابطه منفی و کاهنده معناداری میان تمرکز نقش‌ها و افشای داوطلبانه مستند کرده بودند ناهمسو، ولی با یافته‌های نمازی و ابراهیمی میمند (۱۳۹۵) در بازار سرمایه ایران همسو است. تبیین این یافته بر این مبنا استوار است که به‌موجب قوانین و دستورالعمل‌های حاکمیت شرکتی سازمان بورس و اوراق بهادار، تفکیک پست مدیرعامل از ریاست هیئت‌مدیره به‌طور گسترده پیاده‌سازی شده و وقوع

دوگانگی در شرکت‌های نمونه به حداقل رسیده است؛ در نتیجه نوسانات این متغیر نمی‌تواند تعیین‌کننده اصلی در نوسان سطح افشای سایبری در سطح بازار باشد.

### بحث پیرامون فرضیه ششم: وجود کمیته تخصصی فناوری اطلاعات/ریسک و افشای ریسک فناوری اطلاعات و امنیت سایبری

تنها یافته معنادار حاصل از متغیرهای حاکمیتی پژوهش، تأیید رابطه معکوس (منفی) و معنادار میان وجود کمیته تخصصی فناوری اطلاعات/ریسک با سطح افشای ریسک فناوری اطلاعات و امنیت سایبری است؛ بدین‌ترتیب فرضیه ششم با جهت اثر منفی تأیید شد. اگرچه بر پایه فرضیه کلاسیک نمایندگی و یافته‌های ماتمانه و همکاران (۲۰۲۴)، انتظار می‌رفت ایجاد کمیته‌های تخصصی به شفافیت بیشتر بینجامد، اما یافته معکوس این پژوهش با مبانی «نظریه هزینه‌های مالکانه» و نتایج فیروزی و محسنی (۲۰۲۳) و لینگ و همکاران (۲۰۲۵) انطباق کامل دارد. در چارچوب هزینه‌های مالکانه، اعضای این کمیته‌ها با درک عمیق از آسیب‌پذیری‌های امنیتی و حساسیت داده‌های صنعتی، افشای عمومی و پرجزئیات رخدادها را موجب تضعیف موقعیت رقابتی و راهنمایی مهاجمان سایبری می‌دانند. ازاین‌رو، وجود این کمیته‌ها بیشتر به جای تحریک گزارشگری عمومی، نقش سازوکاری تدافعی را ایفا نموده که به مهار درون‌سازمانی، اصلاح آسیب‌پذیری‌ها و اتخاذ تدابیر احتیاطی بدون افشای بیرونی می‌انجامد.

### پیشنهادهای کاربردی

یافته‌های این پژوهش حامل دلالت‌های مهمی برای ارکان حاکمیتی و سیاست‌گذاران بازار سرمایه است:

- **به هیئت‌مدیره شرکت‌ها** پیشنهاد می‌شود سازوکار نظارت سایبری را از سطح یک اقدام تدافعی صرف به یک مزیت راهبردی تبدیل کنند. همچنین ارتقای سواد سایبری اعضای غیرموظف و مستقل و استفاده از مشاوران تخصصی در کمیته‌های حسابرسی و ریسک می‌تواند تصمیم‌گیری در خصوص میزان افشای متوازن را تسهیل نماید.
- **به سازمان بورس و اوراق بهادار** پیشنهاد می‌گردد نسبت به تدوین راهنماها و چارچوب‌های استاندارد افشای حوادث و ریسک‌های امنیت سایبری اقدام کند تا ضمن

حفظ محرمانگی راهبردی شرکت‌ها (کاهش هزینه‌های مالکانه)، کف شفافیت لازم برای تصمیم‌گیری سرمایه‌گذاران تأمین شود.

## محدودیت‌های پژوهش

تفسیر نتایج حاضر باید با در نظر داشتن این محدودیت‌ها صورت پذیرد. نخست، انحصار جامعه آماری به شرکت‌های بخش تولیدی، تعمیم‌پذیری مستقیم یافته‌ها به نهادهای مالی دارای حساسیت شدید داده‌ای (نظیر بانک‌ها و بیمه‌ها) را با احتیاط مواجه می‌سازد. دوم، تکیه بر تحلیل محتوای گزارش‌های سالانه و تفسیری مدیریت که بازتاب‌دهنده افشای عمومی است و ممکن است با وضعیت واقعی و زیرساخت‌های پنهان امنیتی شرکت‌ها انطباق کامل نداشته باشد. محدودیت سوم، محرمانگی رخدادهای امنیتی در ایران و عدم دسترسی به داده‌های هزینه‌ای مربوط به نقض داده‌ها یا خسارات سایبری، می‌باشد.

## پیشنهاد برای پژوهش‌های آتی

- ارزیابی این الگو در شرکت‌های خدمات مالی، بانکی و فین‌تک‌ها که مواجهه مستقیم‌تری با حملات سایبری دارند.
- بررسی متغیرهای واسطه‌ای نظیر اثربخشی حسابرسی داخلی و سامانه‌های کنترل داخلی بر رابطه حاکمیت شرکتی و افشای سایبری.
- استفاده از مصاحبه‌های نیمه‌ساختاریافته با مدیران ارشد امنیت اطلاعات (CISO) و اعضای کمیته‌های ریسک به‌منظور واکاوی دلایل رفتاری در مهار درون‌سازمانی و احتراز از افشای عمومی.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع

کرمی، صیفی(۱۴۰۳). حاکمیت شرکتی، افشای ریسک و بازده سهام در شرکت‌های مالی ایران. *پژوهش‌های تجربی حسابداری*،۱۴(۵۳)۲۱۵-۲۳۸. https://doi. rg/10.22051/jera.2025.51375.3593

فصیحی، ستاره و برشد، رضوان (۱۴۰۲). افشای ریسک شرکت‌ها: تأثیر ویژگی‌های کمیته حسابرسی. *پژوهش‌های تجربی حسابداری*،۱۳(۱)، ۱۴۱-۱۶۰ https://doi. rg/10.22051/jera.2022.37494.2924

نمازی، محمد و ابراهیمی میمند، مهدی (۱۳۹۵). بررسی تأثیر سازوکارهای راهبری شرکتی بر افشای ریسک در شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران .*فصلنامه حسابداری مالی*،۸(۳۰)، ۲۷-۱. http://qfaj.mobarakeh.iau.ir/article-1-813-fa.html

هیئت وزیران(۱۴۰۴). سند ستاد توسعه علوم و فناوری افتا (امنیت سایبری) (تصویب‌نامه شماره ۳۶۶۰۸ مورخ ۱۴۰۴/۰۲/۳۱). پایگاه ملی اطلاع‌رسانی قوانین و مقررات کشور. https://qavanin. r

## References

Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Al Amosh, H. (2025). Board characteristics and cybersecurity disclosure: evidence from the UK. *Electronic Commerce Research*, 25(6), 1–32. https://doi.org/10.1007/s10660-024-09867-w

Al-Shaer, H., Albitar, K., Derouiche, I., & Hussainey, K. (2025). The role of CEO power and audit committees in cybersecurity risk management. *The International Journal of Accounting*, Advance online publication.

Alshira'h, A. F. (2024). Board of directors' characteristics, political connection and risk disclosure: Evidence from an emerging market context. *Risks*, 12(3), 54–73.

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. *Accounting Perspectives*, Advance online publication. https://doi.org/10.1111/1911-3838.12411

Council of Ministers. (2025). *Document of the High Council for Cyberspace and Cyber Security* Development *(AFTA)* (Resolution No. 36608 dated 2025/05/21). National Database of Laws and Regulations of the Islamic Republic of Iran. https://qavanin.ir (in Persian)

Fasihi, S., & Borshed, R. (2023). Corporate risk disclosure: The impact of audit committee characteristics. *Journal of Empirical Research in Accounting*, 13(1), 141–160. https://doi.org/10.22051/jera.2022.37494.2924 (in Persian)

Firoozi, M., & Mohsni, S. (2023). Cybersecurity disclosure in the banking industry: A comparative study. *Journal of Banking Regulation*, 25(2), 173–192. https://doi.org/10.1057/s41310-023-00190-8

Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. *Journal of Accounting and Public Policy*, 54(5), Article 107376. https://doi.org/10.1016/j.jaccpubpol.2025.107376

Héroux, S., & Fortin, A. (2024). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance*, 28(2), 527–562. DOI: 10.1007/s10997-022-09660-7

ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. Information Systems Audit and Control Association (ISACA).

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Karami, M., & Seyfi, A. (2024). Corporate governance, risk disclosure and stock returns in Iranian financial firms. *Journal of Empirical Research in Accounting*, 14(53), 215–238. https://doi.org/10.22051/jera.2025.51375.3593 (in Persian)

Ling, S., Liu, Z. F., & Xia, H. (2025). Code, control and cybersecurity: How board IT expertise shapes corporate risk management. Journal of Accounting Literature, 1–23. https://doi.org/10.1108/JAL-06-2025-0320

Elgammal, M. M., Hussainey, K., & Ahmed, F. (2018). Corporate governance and voluntary risk and forward-looking disclosures. Journal of Applied Accounting Research, 19(4), 592–607. https://doi.org/10.1108/JAAR-01-2017-0014

Matemane, R., Denhere, V., Mokabane, M., & Ojeyinka, T. A. (2024). Cybersecurity risk disclosure, board characteristics, and firm performance in the Fourth Industrial Revolution era: Evidence from an emerging economy. *African Finance Journal*, 26(1), 34–53. https://journals.co.za/doi/abs/10.10520/ejc-finj_v26_n1_a2

Namazi, M., & Ebrahimi Meimand, M. (2016). Investigating the effect of corporate governance mechanisms on risk disclosure in companies listed on Tehran Stock Exchange. *Financial Accounting Quarterly*, 8(30), 1–27. https://sid.ir/paper/517517/fa (in Persian)

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1299

Pfeffer, J., & Salancik, G. R. (2003). *The External Control of Organizations: A Resource Dependence Perspective*. Stanford University Press. https://www.sup.org/books/business/external-control-organizations

Trinh, V. Q., Elnahass, M., & Pasiouras, F. (2025). Personal traits of CEOs and cybersecurity-related disclosure. Journal of International Accounting, Auditing and Taxation, 58, Article 100680 https://doi.org/10.1016/j.intaccaudtax.2025.100680

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, 27(4), 1049–1071. https://doi.org/10.1007/s10997-022-09637-6

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Review Paper**

# The Synergy Between Artificial Intelligence and Agile Auditing in Small and Medium-Sized Enterprises: A Systematic Interpretive Literature Review [1]

**Saeed Alipour [*2] and Morteza Asadi [3]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 233 - 262

Received: 2026.04.23
Revised: 2026.07.15
Accepted: 2026.08.11

## Abstract

This study Aimed to explain the synergy between Artificial Intelligence (AI) and agile auditing in Small and Medium-sized Enterprises (SMEs) through an interpretive systematic review approach. Rapid changes in the business environment, increasing volume and complexity of financial data, and limitations in human and financial resources have challenged the effectiveness of traditional auditing models in SMEs. In this context, AI and agile auditing have emerged as complementary transformation pathways. However, previous studies have mainly examined these concepts separately and largely within large organizations. Addressing this gap, the present study analyzes their synergy as an integrated Framework for delivering auditing services in SMEs. The study was conducted based on the PRISMA 2020 guidelines. After identification, screening, and Full-text evaluation, 52 Persian and English studies published between 2019 and 2025 were selected for final analysis. Data were analyzed using interpretive thematic analysis with a context based approach. Findings indicate that the synergy between AI and agile auditing is a multilayered, gradual, and context dependent process rather than a simple causal relationship. At the first level, AI -based automation reduces repetitive tasks and enhances auditors' cognitive and time capacities. At the second level, advanced analytical algorithms strengthen risk based auditing, improve professional judgment, and generate analytical insights. At the third level, intelligent reporting technologies and natural language processing enhance transparency and continuous stakeholder interaction. The findings also reveal that achieving this synergy strongly depends on contextual factors such as data quality, auditors' hybrid skills, resource limitations, and organizational digital maturity.

**Keywords**: Artificial Intelligence, Agile Auditing; Small and Medium-sized Enterprises (SMEs), Synergy, Interpretive Systematic Literature Review, Digital Transformation.

**JEL classification:** *G32, L25, O33, M15, M42.*

---

[1] https://doi.org/10.22034/JISTA.2026.580880.1090
[2] Assistant Professor, Department of Accounting, Ard.C., Islamic Azad University, Ardabil, Iran. (Corresponding Author). Email: Saeed.Alipour@iau.ac.ir
[3] Master of Accounting, Management Faculty, University of Tehran, Tehran, Iran. Email: mortezaasadi4361@gmail.com

## 1. INTRODUCTION

The rapid advancement of digital technologies has fundamentally transformed organizational processes and professional services worldwide. Among these technologies, Artificial Intelligence (AI) has emerged as one of the most influential innovations capable of reshaping accounting and auditing practices. AI technologies—including machine learning, robotic process automation (RPA), natural language processing (NLP), and big data analytics—have significantly enhanced auditors' ability to process large volumes of financial information, detect anomalies, identify fraud risks, and improve audit quality. Simultaneously, Agile Auditing has attracted increasing attention as an adaptive auditing methodology emphasizing flexibility, continuous communication, rapid response to organizational changes, and iterative audit procedures.

Although numerous studies have independently examined AI applications in auditing and the principles of agile auditing, the interaction between these two concepts has received limited scholarly attention. Existing research has primarily focused on technological capabilities, implementation challenges, or individual auditing tools without providing an integrated understanding of how AI capabilities and agile auditing practices reinforce one another, particularly within Small and Medium-sized Enterprises (SMEs). SMEs operate under unique conditions characterized by limited financial resources, restricted technological infrastructure, fewer specialized personnel, and greater sensitivity to environmental uncertainty. Consequently, understanding how AI and agile auditing interact within such organizations requires a comprehensive conceptual framework that extends beyond purely technological explanations.

Furthermore, previous literature presents fragmented evidence regarding organizational, technological, and environmental factors influencing successful AI implementation in auditing. Most existing studies examine isolated dimensions such as automation, digital transformation, audit quality, or intelligent auditing, while the dynamic relationships among these dimensions remain insufficiently explored.

To address these research gaps, this study employs an Interpretive Systematic Literature Review (ISLR) to synthesize existing

international and Persian studies and develop an integrated conceptual understanding of AI–Agile Auditing synergy in SMEs. Rather than merely summarizing previous findings, the study seeks to interpret underlying mechanisms, identify major thematic relationships, and explain how organizational capabilities, technological readiness, and institutional conditions collectively shape successful digital transformation in auditing practices.

## 2. MATERIALS AND METHODS

This research adopts an Interpretive Systematic Literature Review (ISLR) methodology guided by the PRISMA 2020 statement for systematic evidence identification and selection. Unlike traditional narrative reviews or conventional meta-synthesis approaches, ISLR emphasizes conceptual interpretation, thematic integration, and theoretical development through critical analysis of previous studies.

Relevant publications were identified through comprehensive searches of major international databases; including Scopus, Web of Science, ScienceDirect, SpringerLink, Emerald Insight, IEEE Xplore, Taylor & Francis, Wiley Online Library, and Google Scholar; as well as Persian scientific databases including SID, Magiran, Noormags, and Ensani.ir. English- and Persian-language publications focusing on artificial intelligence, agile auditing, digital transformation, intelligent auditing, robotic process automation, machine learning, and SMEs were considered.

The selection process followed four sequential PRISMA stages: identification, screening, eligibility assessment, and final inclusion. After removing duplicate records and applying predefined inclusion and exclusion criteria, fifty-two high-quality studies (40 international and 12 Persian publications) were selected for detailed analysis.

To ensure methodological rigor, the quality of selected studies was assessed using CASP (Critical Appraisal Skills Programme) criteria. Studies lacking methodological transparency, conceptual relevance, or sufficient analytical quality were excluded.

Data analysis employed Braun and Clarke's thematic analysis framework. Through iterative coding, theme refinement, and interpretive comparison, the extracted concepts were synthesized

into broader conceptual themes representing the mechanisms underlying AI–Agile Auditing synergy.

## 3. RESULTS AND DISCUSSION

The findings demonstrate that the synergy between Artificial Intelligence and Agile Auditing represents a multidimensional organizational capability rather than a simple technological relationship. Three major thematic dimensions emerged from the interpretive synthesis.

The first dimension concerns operational automation. Technologies such as Robotic Process Automation substantially reduce repetitive audit activities including data extraction, reconciliation, documentation, and routine testing. By automating standardized procedures, auditors can devote greater attention to analytical reasoning, professional judgment, and value-added advisory activities. This operational improvement is particularly significant for SMEs where limited human resources and financial constraints intensify the need for efficient audit processes.

The second dimension involves analytical intelligence. Machine learning algorithms and big data analytics enable auditors to detect hidden patterns, identify complex anomalies, assess systematic risks, and improve predictive capabilities beyond traditional sampling approaches. However, the study indicates that AI-generated insights should complement—not replace—professional auditor judgment. Effective synergy emerges when technological capabilities and human expertise operate collaboratively.

The third dimension relates to communication and reporting enhancement. Natural language processing, intelligent dashboards, and interactive reporting systems facilitate continuous communication between auditors, managers, and stakeholders. Rather than producing static audit reports, AI supports dynamic reporting environments characterized by transparency, responsiveness, and continuous organizational learning.

Beyond these operational dimensions, the interpretive analysis highlights several contextual moderators affecting successful implementation. Organizational culture, technological maturity, professional competencies, financial constraints, and institutional support significantly influence both the speed and quality of AI

adoption. Consequently, AI implementation should not be viewed as an isolated technological project but as an organizational transformation requiring strategic alignment among technology, human resources, governance structures, and professional practices.

Comparative analysis with international literature confirms substantial consistency regarding AI's positive contribution to audit quality, decision-making, and risk assessment. However, this study extends previous research by demonstrating that sustainable AI adoption depends on dynamic interactions among technological, organizational, and environmental factors rather than technological sophistication alone.

Analysis of the twelve selected Persian studies similarly revealed that domestic research has generally examined artificial intelligence, digital transformation, intelligent auditing, or agile auditing independently. In contrast, this study integrates these fragmented perspectives into a unified interpretive framework explaining how AI and agile auditing mutually reinforce one another within SME environments.

From an Iranian perspective, the findings further indicate that successful implementation remains constrained by insufficient ERP infrastructure, fragmented accounting information systems, limited digital maturity, and inadequate institutional support. Therefore, organizations such as the Iranian Association of Certified Public Accountants and the Audit Organization play critical roles in facilitating professional guidance, educational programs, regulatory development, and technological standardization necessary for broader AI adoption.

## 4. CONCLUSION

This study provides a comprehensive interpretive explanation of how Artificial Intelligence and Agile Auditing jointly contribute to organizational transformation in Small and Medium-sized Enterprises. Rather than representing independent technological developments, AI and agile auditing form an integrated capability requiring continuous interaction among digital infrastructure, professional expertise, organizational culture, and institutional governance.

The primary contribution of this research lies in developing an integrated conceptual framework explaining the mechanisms through which AI-enabled auditing evolves from operational automation toward strategic organizational intelligence. The proposed framework offers valuable implications for researchers, audit professionals, policymakers, and SME managers seeking to implement effective digital auditing practices.

Despite its contributions, this study has several limitations. The review included only Persian and English publications, while additional evidence published in other languages or grey literature may provide complementary insights. Moreover, as an interpretive systematic review, the findings are based on synthesis of existing studies rather than empirical organizational data.

Future research is encouraged to empirically validate the proposed framework using data collected from SMEs and audit firms, investigate the influence of digital maturity and organizational culture on AI implementation success, and conduct comparative studies across different institutional and economic contexts.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ ترویجی**

# تبیین هم‌افزایی هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط: یک مرور نظام‌مند تفسیری[1]

**سعید علی‌پور*[2] و مرتضی اسدی[3]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۲۳۳ - ۲۶۲

تاریخ دریافت: ۱۴۰۵/۰۲/۰۳
تاریخ بازنگری: ۱۴۰۵/۰۴/۲۴
تاریخ پذیرش: ۱۴۰۵/۰۵/۲۰

## چکیده

*این پژوهش با هدف تبیین هم‌افزایی میان هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط، از رویکرد مرور نظام‌مند تفسیری استفاده می‌کند. تحولات سریع محیط کسب و کار، افزایش حجم و پیچیدگی داده‌های مالی و محدودیت منابع انسانی و مالی در SMEها، کارایی روش‌های سنتی حسابرسی را با چالش مواجه کرده است. در این شرایط، هوش مصنوعی و حسابرسی چابک به عنوان دو مسیر مکمل تحول مطرح شده‌اند، اما بیشتر پژوهش‌های پیشین این دو مفهوم را جداگانه و عمدتاً در سازمان‌های بزرگ بررسی کرده‌اند. پژوهش حاضر با تمرکز بر این خلأ، هم‌افزایی این دو رویکرد را به عنوان منطقی یکپارچه برای ارائه خدمات حسابرسی در SMEها تحلیل می‌کند. مطالعه بر اساس دستورالعمل PRISMA 2020 انجام شد و ۵۲ مقاله فارسی و انگلیسی منتشرشده در فاصله زمانی ۲۰۱۹ تا ۲۰۲۵، پس از مراحل شناسایی، غربالگری و ارزیابی نهایی، انتخاب شدند. داده‌ها با استفاده از تحلیل مضمون تفسیری و رویکردی زمینه محور بررسی شدند. یافته‌ها نشان می‌دهد هم‌افزایی هوش مصنوعی و حسابرسی چابک فرایندی چندلایه، تدریجی و وابسته به شرایط سازمانی است. در سطح نخست، اتوماسیون مبتنی بر هوش مصنوعی با کاهش فعالیت‌های تکراری، ظرفیت زمانی و شناختی حسابرسان را افزایش می‌دهد. در سطح دوم، الگوریتم‌های تحلیلی پیشرفته، کیفیت قضاوت حرفه‌ای و تحلیل مبتنی بر ریسک را تقویت می‌کنند. در سطح سوم، فناوری‌های گزارش‌دهی هوشمند و پردازش زبان طبیعی، شفافیت و تعامل مستمر با ذی‌نفعان را بهبود می‌بخشند. نتایج همچنین نشان می‌دهد تحقق این هم‌افزایی به عواملی مانند کیفیت داده‌ها، مهارت حسابرسان، محدودیت منابع و بلوغ دیجیتال سازمان وابسته است.*

**واژه‌های کلیدی:** *هوش مصنوعی، حسابرسی چابک، شرکت‌های کوچک و متوسط، هم‌افزایی، مرور نظام‌مند تفسیری، تحول دیجیتال.*

**طبقه‌بندی موضوعی:** *M42, M15, O33, L25, G32 .*

---

[1] https://doi.org/10.22034/JISTA.2026.580880.1090

[2] استادیار، گروه حسابداری، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران. (نویسنده مسئول). (saeed.alipour@iau.ac.ir)

[3] کارشناس ارشد، دانشکده مدیریت، گروه حسابداری ، دانشگاه تهران، تهران، ایران. (mortezaasadi4361@gmail.com)

**مقدمه**

تحولات شتابان در محیط کسب‌وکار، افزایش حجم و پیچیدگی داده‌های مالی، و فشار روزافزون ذی‌نفعان برای دریافت اطمینان‌بخشی با کیفیت بالاتر و هزینه کمتر، حرفه حسابرسی را با چالش‌های ساختاری عمیقی مواجه ساخته است. این چالش‌ها به ویژه در شرکت‌های کوچک و متوسط نمود پررنگ‌تری دارند؛ بنگاه‌هایی که از یک سو سهم قابل توجهی در اقتصاد ملی دارند و از سوی دیگر با محدودیت منابع انسانی، فناورانه و مالی روبه‌رو هستند. در چنین بستری، مدل‌های سنتی حسابرسی که مبتنی بر نمونه‌گیری محدود، فرآیندهای دستی که بیشتر متمرکز بر انطباق هستند، به تدریج کارایی و اثربخشی خود را از دست می‌دهند و پاسخگوی الزامات محیطی جدید نیستند (کاسار و جیزی[1]، ۲۰۲۵ : ۲۱۸). در واکنش به این وضعیت، هوش مصنوعی به عنوان یکی از مهم‌ترین محرک‌های تحول دیجیتال در حسابداری و حسابرسی مطرح شده است. ادبیات اخیر نشان می‌دهد که فناوری‌هایی مانند یادگیری ماشین، اتوماسیون فرآیندهای رباتیک و تحلیل پیشرفته داده‌ها، ظرفیت آن را دارند که فرآیند حسابرسی را از نظر سرعت، دقت و پوشش اطلاعاتی به شکل معناداری بهبود دهند (فدیک و همکاران[2]، ۲۰۲۲: ۹۳۹). برخلاف رویکردهای اولیه که هوش مصنوعی را صرفا ابزاری برای خودکارسازی وظایف تکراری تلقی می‌کردند، پژوهش‌های جدیدتر بر نقش آن در ارتقای قضاوت حرفه‌ای، شناسایی الگوهای پنهان ریسک و تولید بینش‌های ارزش‌آفرین تأکید دارند (لئوکادیو و همکاران[3]، ۲۰۲۴ : ۴). با این حال، شواهد موجود حاکی از آن است که اثرگذاری هوش مصنوعی در حسابرسی نه یک پدیده خطی و تضمین‌شده، بلکه فرآیندی وابسته به زمینه سازمانی و نحوه به‌کارگیری آن است. پژوهش فدیک و همکاران نشان می‌دهد که اگرچه استفاده از هوش مصنوعی می‌تواند کیفیت فرآیند حسابرسی را افزایش دهد، اما این بهبود زمانی محقق می‌شود که فناوری به عنوان مکمل توانمندی‌های انسانی حسابرسان عمل کند، نه جایگزین ساده آن‌ها (فدیک و همکاران، ۲۰۲۲: ۹۴۱). این دیدگاه با ادبیات نظری گسترده‌تری همسو است که از «پارادوکس اتوماسیون و ارتقا» سخن می‌گوید؛ بدین معنا که فناوری‌های هوشمند در عین کاهش برخی وظایف، نیاز به مهارت‌های تحلیلی و قضاوتی سطح بالاتر را تشدید می‌کنند

[1] Kassar and Jizi, 2025
[2] Fedyk et al., 2022
[3] Leocádio et al., 2024

(رایش و کراکوفسکی[1]، ۲۰۲۱ : ۱۹۳). در این میان، مفهوم حسابرسی چابک به عنوان پاسخی سازمانی و عملیاتی به عدم قطعیت، تغییرپذیری و محدودیت منابع مطرح شده است. حسابرسی چابک بر چرخه‌های کوتاه بازخورد، انعطاف‌پذیری در برنامه‌ریزی، تعامل مستمر با ذی‌نفعان و تمرکز بر خلق ارزش فراتر از انطباق تأکید دارد. پژوهش‌های اخیر نشان می‌دهند که تحقق عملی این اصول بدون تکیه بر زیرساخت‌های دیجیتال پیشرفته عملا دشوار است و هوش مصنوعی می‌تواند نقش بستر توانمندساز این رویکرد را ایفا کند (کاسار و جیزی، ۲۰۲۵ : ۲۱۸؛ لئوکادیو و همکاران، ۲۰۲۴ : ۸). با وجود رشد سریع ادبیات مرتبط با هوش مصنوعی در حسابرسی، هنوز شکاف‌های مفهومی و تحلیلی مهمی باقی مانده است. بخش قابل توجهی از پژوهش‌ها یا بر سازمان‌های بزرگ و مؤسسات حسابرسی بین‌المللی متمرکز بوده‌اند، یا هوش مصنوعی را به صورت منفک از رویکردهای نوین عملیاتی بررسی کرده‌اند. این در حالی است که شرکت‌های کوچک و متوسط شرایط نهادی، منابع و نیازهای متفاوتی دارند و هم‌افزایی میان هوش مصنوعی و حسابرسی چابک در این بستر می‌تواند ماهیتی متمایز و پیچیده‌تر داشته باشد (سوتن و همکاران[2]، ۲۰۱۶: ۶۲؛ کاسار و جیزی، ۲۰۲۵: ۲۲۱). از این رو، ضرورت دارد که این هم‌افزایی نه صرفا به عنوان استقرار یک فناوری جدید، بلکه به عنوان یک تحول یکپارچه در منطق ارائه خدمات حسابرسی مورد بررسی قرار گیرد. پژوهش حاضر با تمرکز بر این خلأ، می‌کوشد با تکیه بر مرور نظام‌مند تفسیری ادبیات، سازوکارها، پیامدها و شرایط تحقق هم‌افزایی میان هوش مصنوعی و حسابرسی چابک را در بستر شرکت‌های کوچک و متوسط تبیین کند و بدین ترتیب، زمینه‌ای نظری و تحلیلی برای توسعه پژوهش‌های تجربی آتی و تصمیم‌گیری حرفه‌ای فراهم آورد.

بر این اساس، پژوهش حاضر در پی پاسخ به پرسش‌های زیر است:

پرسش اول: هم‌افزایی میان هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط از چه سازوکارهایی شکل می‌گیرد؟

پرسش دوم: چه عوامل سازمانی، فناورانه و نهادی تحقق این هم‌افزایی را تسهیل یا محدود می‌کنند؟

[1] Raisch & Krakowski, 2021
[2] Sutton et al.,2016

پرسش سوم: هم‌افزایی میان هوش مصنوعی و حسابرسی چابک چه پیامدهایی برای ارتقای کیفیت و ارزش‌آفرینی خدمات حسابرسی در شرکت‌های کوچک و متوسط به همراه دارد؟

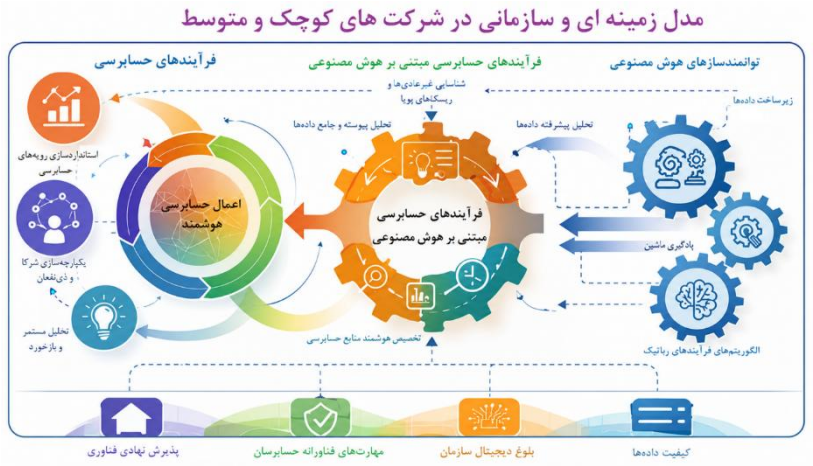
## چارچوب مفهومی

چارچوب مفهومی حسابرسی مبتنی بر هوش مصنوعی بر این پیش‌فرض استوار است که فناوری‌های هوشمند می‌توانند حسابرسی را از انجام وظایف تکراری و نمونه‌محور به سمت تحلیل پیوسته، جامع و داده‌محور سوق دهند. الگوریتم‌های هوشمند با شناسایی الگوهای غیرعادی، ارزیابی ریسک‌های پویا و تولید بینش‌های ارزش‌آفرین، نقش حسابرس را از ناظر انطباق به شریکی تحلیلی در فرایند تصمیم‌گیری ارتقا می‌دهند (لئوکادیو و همکاران، ۲۰۲۴ : ۶). در این میان، اتوماسیون فرایندهای رباتیک (RPA) با خودکارسازی فعالیت‌های تکراری، سرعت، دقت و مقیاس‌پذیری حسابرسی را افزایش داده و با آزادسازی زمان حسابرسان، زمینه تمرکز بیشتر بر قضاوت حرفه‌ای، تحلیل‌های پیچیده و تعامل با ذی‌نفعان را فراهم می‌کند؛ قابلیتی که با اصول حسابرسی چابک هم‌راستا است (کاسار و جیزی، ۲۰۲۵ : ۲۲۵). همچنین، یادگیری ماشین و تحلیل پیشرفته داده‌ها با پردازش حجم وسیعی از داده‌های مالی و غیرمالی، شناسایی نواحی پرریسک و تخصیص هدفمند منابع را تقویت کرده و انعطاف‌پذیری برنامه حسابرسی را افزایش می‌دهند (فدیک و همکاران، ۲۰۲۲ : ۹۴۲).

با این حال، تحقق این هم‌افزایی به قابلیت‌های فناورانه محدود نیست و تحت تأثیر شرایط سازمانی و نهادی قرار دارد. کیفیت داده‌ها، بلوغ دیجیتال سازمان، مهارت‌های فناورانه حسابرسان و پذیرش نهادی فناوری‌های هوشمند می‌توانند اثربخشی کاربرد هوش مصنوعی را تعدیل کنند (لئوکادیو و همکاران، ۲۰۲۴ : ۱۲). ازاین‌رو، در شرکت‌های کوچک و متوسط، حسابرسی چابک مبتنی بر هوش مصنوعی را می‌توان حاصل تعامل میان توانمندسازهای فناورانه، منطق تحلیلی حسابرسی چابک و عوامل زمینه‌ای سازمانی و نهادی دانست (کاسار و جیزی، ۲۰۲۵ : ۲۲۵؛ فدیک و همکاران، ۲۰۲۲: ۹۴۷).

بر این اساس، مدل مفهومی پژوهش در شکل ۱ ارائه شده است. در این مدل، توانمندسازهای فناورانه شامل RPA، یادگیری ماشین و تحلیل پیشرفته داده‌ها، زمینه تحول فرایندهای حسابرسی

را فراهم می‌کنند و از طریق تحلیل پیوسته داده‌ها، شناسایی ناهنجاری‌ها و ریسک‌های پویا و تخصیص هدفمند منابع، با اصول حسابرسی چابک شامل انعطاف‌پذیری، بازخورد سریع، قضاوت حرفه‌ای و تعامل مستمر با ذی‌نفعان همگرا می‌شوند. پیامد این هم‌افزایی، ارتقای کیفیت و پوشش حسابرسی، تقویت نقش تحلیلی حسابرس، افزایش کارایی در شرایط محدودیت منابع و خلق ارزش فراتر از الزامات قانونی است؛ درحالی‌که عوامل سازمانی و نهادی، اثربخشی این روابط را در بستر شرکت‌های کوچک و متوسط تحت تأثیر قرار می‌دهند.




**شکل ۱.** مدل مفهومی پژوهش

## روش‌شناسی مرور نظام‌مند

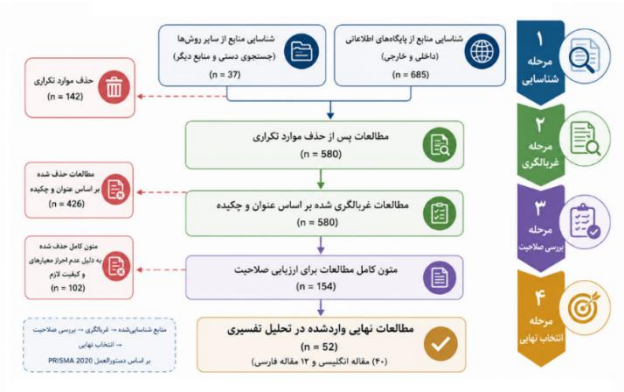
این مطالعه با هدف تبیین هم‌افزایی هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط، از رویکرد مرور نظام‌مند تفسیری بهره گرفته است. انتخاب این رویکرد ناشی از ماهیت مفهومی، میان‌رشته‌ای و تبیینی پرسش پژوهش است؛ به گونه‌ای که پاسخ به آن مستلزم فراتر رفتن از تجمیع توصیفی مطالعات و حرکت به سوی تفسیر، ترکیب مفهومی و بسط چارچوب‌های نظری است. برخلاف مرورهای تجمیعی یا متاآنالیزهای کمی که هدف اصلی آن‌ها برآورد اندازه اثر یا مقایسه فراوانی نتایج است، مرور نظام‌مند تفسیری بر فهم عمیق‌تر مفاهیم و تبیین سازوکارهای شکل‌گیری پدیده‌ها تمرکز دارد. در این پژوهش، مرور نظام‌مند

تفسیری به دلیل ماهیت تبیینی سؤال پژوهش انتخاب شد. برخلاف مرور روایتی (Narrative Review)که عمدتاً به توصیف و جمع‌بندی مطالعات موجود می‌پردازد، این رویکرد بر کشف روابط مفهومی میان یافته‌های مطالعات مختلف تمرکز دارد. همچنین، برخلاف فراترکیب (Meta-synthesis) که معمولاً به تلفیق نتایج پژوهش‌های کیفی با هدف تولید یک تفسیر جامع محدود می‌شود، مرور نظام‌مند تفسیری امکان بازاندیشی مستمر در مفاهیم، بازتعریف مضامین و توسعه یک چارچوب نظری جدید را فراهم می‌آورد. از سوی دیگر، این پژوهش از فراتحلیل (Meta-analysis) نیز متمایز است؛ زیرا هدف آن برآورد اندازه اثر یا ترکیب آماری نتایج مطالعات نیست، بلکه تبیین سازوکارهای شکل‌گیری هم‌افزایی میان هوش مصنوعی و حسابرسی چابک در بستر شرکت‌های کوچک و متوسط است. بر همین اساس، مطالعات منتخب صرفاً تجمیع یا خلاصه نشدند، بلکه از طریق مقایسه مستمر، بازتفسیر مفاهیم و تحلیل روابط میان مضامین، یک مدل تفسیری منسجم توسعه یافت. به بیان دیگر، هدف اصلی این نوع مرور پاسخ به پرسش‌های «چگونه» و «چرا» درباره یک پدیده است، نه صرفاً تعیین میزان اثر آن. به منظور اطمینان از شفافیت، جامعیت و قابلیت پیگیری فرآیند پژوهش، پروتکل مطالعه از دستورالعمل PRISMA 2020 تبعیت کرده است (پیج و همکاران[1]، ۲۰۲۱ : ۸). در این پژوهش، چارچوب PRISMA به عنوان ابزاری برای نظم‌دهی نظام‌مند به مراحل شناسایی، غربالگری و انتخاب مطالعات به کار رفته و نه به عنوان مبنای تحلیل معرفت‌شناختی. جستجوی نظام‌مند ادبیات در شش پایگاه داده معتبر بین‌المللی شاملScopus ، Web of Science، Core Collection، ScienceDirect، Emerald Insight، IEEE Xplore، SpringerLink و نیز سه پایگاه داده فارسی؛ پایگاه مرکز اطلاعات علمی جهاد دانشگاهی، بانک اطلاعات نشریات کشور و پرتال جامع علوم انسانی انجام شد. راهبرد جستجو سه محور اصلی پژوهش را پوشش داد: مفاهیم مرتبط با هوش مصنوعی و فناوری‌های داده‌محور، حسابرسی و ممیزی، و شرکت‌های کوچک و متوسط. بازه زمانی انتشار مطالعات از ابتدای سال ۲۰۱۹ تا پایان دسامبر ۲۰۲۵ تعیین شد تا ضمن پوشش مبانی نسبتاً تثبیت‌شده، تحولات اخیر حوزه هوش مصنوعی نیز لحاظ گردد. مطالعات بر اساس معیارهای از پیش تعریف‌شده غربالگری شدند. معیارهای ورود شامل تمرکز بر کاربردهای هوش مصنوعی در حسابرسی یا

[1] Page et al.,2021

مبانی مفهومی حسابرسی چابک، ارتباط مستقیم یا استنتاج‌پذیر با بستر شرکت‌های کوچک و متوسط، و انتشار در قالب مقاله علمی داوری‌شده یا پایان‌نامه دکتری با دسترسی کامل بود. کتاب‌ها، گزارش‌های حرفه‌ای عمومی، سرمقاله‌ها و مطالعات غیر فارسی یا غیر انگلیسی از دامنه پژوهش خارج شدند تا تمرکز بر شواهد علمی معتبر حفظ شود. فرآیند گزینش مطابق با نمودار جریان PRISMA 2020 (شکل ۲) در چهار مرحله شناسایی، غربالگری اولیه، ارزیابی متن کامل و انتخاب نهایی انجام گرفت. در نهایت، ۵۲ مطالعه شامل ۴۰ مقاله انگلیسی و ۱۲ مقاله فارسی برای تحلیل نهایی انتخاب شدند. علاوه بر معیارهای ورود و خروج، کیفیت روش‌شناختی مطالعات منتخب نیز پیش از ورود به مرحله تحلیل مورد بررسی قرار گرفت. برای این منظور، از معیارهای پیشنهادی برنامه CASP (Critical Appraisal Skills Programme) به‌عنوان چارچوب راهنما استفاده شد. در این ارزیابی، شفافیت هدف پژوهش، تناسب روش تحقیق، کفایت فرآیند گردآوری و تحلیل داده‌ها، استحکام یافته‌ها، انسجام نتایج و میزان ارتباط مستقیم هر مطالعه با موضوع هم‌افزایی هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط بررسی شد. مطالعاتی که فاقد شفافیت روش‌شناختی بودند یا ارتباط مستقیمی با سؤال پژوهش نداشتند، در مرحله بررسی متن کامل کنار گذاشته شدند و تنها مطالعات واجد شرایط وارد مرحله تحلیل مضمون شدند .

همان‌گونه که در شکل ۲ مشاهده می‌شود، فرآیند انتخاب مطالعات در چهار مرحله شامل شناسایی، غربالگری، بررسی صلاحیت و انتخاب نهایی انجام شد. پس از حذف منابع تکراری و مطالعات فاقد معیارهای ورود و کیفیت لازم، در نهایت ۵۲ مطالعه واجد شرایط برای تحلیل تفسیری انتخاب شدند.




**شکل ۲.** نمودار جریان انتخاب مطالعات بر اساس دستورالعمل PRISMA 2020

داده‌های کلیدی هر مطالعه در قالب جدولی از پیش طراحی‌شده شامل اطلاعاتی نظیر نویسنده، سال انتشار، هدف پژوهش، روش‌شناسی، بستر مطالعه و یافته‌های اصلی ثبت شد . تحلیل کیفی مطالعات منتخب با استفاده از روش تحلیل مضمون براساس چارچوب بازبینی‌شده براون و کلارک انجام گرفت. این فرآیند ماهیتی تفسیری داشته و با هدف بسط فهم نظری از هم‌افزایی میان هوش مصنوعی و حسابرسی چابک طراحی شده است. در مرحله نخست، کدگذاری به صورت باز و داده‌محور انجام شد و مضامین اولیه مستقیماً از محتوای مطالعات استخراج گردید. در مراحل بعد، این مضامین از طریق مقایسه مستمر، بازاندیشی تفسیری و تعامل انتقادی با مفاهیم نظری موجود، بازسازمان‌دهی شدند. چارچوب مفهومی اولیه پژوهش نه به عنوان قالبی تحمیلی، بلکه به عنوان ابزار تفسیری برای تعمیق و انسجام‌بخشی به مضامین در مراحل نهایی تحلیل مورد استفاده قرار گرفت. فرآیند تحلیل مضامین به‌صورت مرحله‌ای انجام شد. ابتدا متن کامل ۵۲ مطالعه منتخب چندین بار مطالعه و واحدهای معنایی مرتبط با هدف پژوهش استخراج شد. در مرحله نخست، کدگذاری باز بدون تحمیل چارچوب نظری از پیش تعیین‌شده انجام گرفت و کدهای اولیه مستقیماً از محتوای مطالعات استخراج شدند. سپس کدهای مشابه از طریق مقایسه مستمر، ادغام و در قالب خوشه‌های مفهومی سازمان‌دهی شدند. در ادامه، با بازبینی مکرر ارتباط میان خوشه‌های مفهومی و چارچوب نظری پژوهش، مضامین اولیه اصلاح، ادغام یا تفکیک شدند تا در نهایت چهار مضمون تفسیری شامل هم‌افزایی کارایی‌بخش، هم‌افزایی بینش‌ساز، هم‌افزایی ارتباطی و عوامل تعدیل‌گر استخراج شد. وجه

تمایز این پژوهش با یک فرایند صرفِ کدگذاری در آن بود که فرایند تحلیل به استخراج مضامین محدود نشد، بلکه روابط سلسله‌مراتبی و تعاملات میان مضامین نیز تحلیل شد. بر این اساس، الگوی تفسیری نهاییِ هم‌افزایی میان هوش مصنوعی و حسابرسی چابک توسعه یافت. این رویکرد امکان شناسایی مسیرهای هم‌افزایی، سازوکارهای کلیدی و عوامل زمینه‌ای مؤثر در بستر شرکت‌های کوچک و متوسط را فراهم ساخت.

**جدول ۱**

*فرایند اجرایی و تحلیلی مرور نظام‌مند تفسیری بر اساس PRISMA 2020*

| مرحله | ابزار و چارچوب مورد استفاده | منطق و هدف روش‌شناختی | خروجی و نتیجه هر مرحله |
|---|---|---|---|
| **۱. طراحی و تعیین رویکرد پژوهش** | انتخاب رویکرد مرور نظام‌مند تفسیری (Interpretive Systematic Review) | پاسخ به پرسش تبیینی و میان‌رشته‌ای؛ تمرکز بر ترکیب مفهومی و بسط نظری | تبیین الگوی مفهومی هم‌افزایی هوش مصنوعی و حسابرسی چابک |
| **۲. تدوین پروتکل و چارچوب اجرایی** | دستورالعمل PRISMA 2020 | اطمینان از شفافیت و قابلیت تکرار مراحل مرور | طراحی مراحل شناسایی، غربالگری، ارزیابی و تحلیل |
| **۳. جستجوی نظام‌مند منابع** | پایگاه‌های Scopus، WOS، ScienceDirect، Emerald، IEEE، Springer، SID و Noormags،Magiran | پوشش جامع ادبیات بین‌المللی و فارسی | احصای مطالعات مرتبط در بازه ۲۰۱۹–۲۰۲۵ |
| **٤. غربالگری و انتخاب مطالعات** | معیارهای ورود و خروج از پیش تعیین‌شده همراه با ارزیابی کیفیت مطالعات بر اساس معیارهای راهنمای CASP | تمرکز بر مطالعات علمی معتبر با ارتباط مستقیم با SMEs | گزینش نهایی ۵۲ مطالعه واجد معیارهای موضوعی و کیفیت روش‌شناختی |
| **۵. استخراج داده‌ها و متغیرها** | فرم از پیش طراحی‌شده استخراج داده | ایجاد انسجام در داده‌های کلیدی هر مطالعه | تشکیل پایگاه داده اولیه برای تحلیل مضمون |
| **٦. تحلیل کیفی و تفسیر داده‌ها** | روش تحلیل مضمون براون و کلارک (نسخه بازبینی‌شده) | شناسایی مضامین، سازوکارهای هم‌افزایی و عوامل زمینه‌ای | استخراج کدهای اولیه، تشکیل خوشه‌های مفهومی، توسعه مضامین تفسیری و طراحی الگوی نهایی هم‌افزایی. |

| مرحله | ابزار و چارچوب مورد استفاده | منطق و هدف روش‌شناختی | خروجی و نتیجه هر مرحله |
|---|---|---|---|
| **۷. تلفیق و بسط چارچوب مفهومی** | تعامل تفسیری با چارچوب مفهومی اولیه (نه تحمیلی) | تعمیق درک نظری و انسجام‌بخشی به نتایج | مدل تفسیری نهایی هم‌افزایی در بستر SMEs |
| **۸. اعتبارسنجی و اجماع پژوهشگران** | بررسی هم‌زمان توسط دو پژوهشگر و تطبیق نتایج | افزایش اعتمادپذیری و جلوگیری از سوگیری تفسیری | توافق نهایی در کدگذاری و توسعه مضامین نظری مبتنی بر تحلیل تفسیری |




**شکل ۳.** فرآیند استخراج مضامین در مرور نظام‌مند تفسیری

## یافته‌ها: تحلیل تفسیری منطق هم‌افزایی

تحلیل تفسیری ۵۲ مطالعه منتخب نشان می‌دهد که رابطه میان هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط، یک رابطه خطی یا صرفا علّی نیست. یافته‌ها حاکی از آن است که این تعامل، فرآیندی چندسطحی، تدریجی و به شدت وابسته به زمینه سازمانی و نهادی SMEهاست. نتایج به دست آمده، چارچوب مفهومی اولیه پژوهش را نتنها تأیید می‌کنند، بلکه آن را از طریق شناسایی سازوکارهای درونی هم‌افزایی، غنی‌سازند. هم‌افزایی مشاهده شده در ادبیات نشان نمی‌دهد که دو نوآوری فناورانه و روش‌شناختی به‌طور هم‌زمان رخ داده‌اند، بلکه بیانگر این است که شرکت‌های کوچک و متوسط به تدریج، شیوه ارائه خدمات حسابرسی خود را متناسب با محدودیت‌های ساختاری و فرصت‌های مقیاس‌پذیر فناوری‌های هوشمند تطبیق می‌دهند.بر اساس کدگذاری و خوشه‌بندی مفاهیم استخراج شده از مطالعات، چهار مضمون تفسیری به هم‌پیوسته و دارای رابطه سلسله‌مراتبی شناسایی شد. این مضامین نظری مبتنی بر تحلیل تفسیری مسیر شکل‌گیری هم‌افزایی را از سطح زیرساخت عملیاتی آغاز کرده و تا سطح قضاوت حرفه‌ای پیشرفته و تعامل با ذی‌نفعان را گسترش می‌دهند. تحلیل نشان می‌دهد که تحقق هر مضمون، پیش‌نیاز ظهور و اثربخشی مضمون بعدی است.

### هم‌افزایی کارایی‌بخش: اتوماسیون به مثابه بستر آزادسازی ظرفیت

یافته‌ها نشان می‌دهند که نقطه شروع هم‌افزایی در اغلبSME ها، استقرار اشکال مختلف اتوماسیون مبتنی بر هوش مصنوعی است. رباتیک فرآیندهای خودکار و الگوریتم‌های قاعده‌مند، به طور نظام‌مند برای انجام وظایف تکراری و پرحجم حسابرسی به کار گرفته شده‌اند. این وظایف شامل تطبیق‌های بانکی، آزمون‌های روتین کنترل، بررسی اقلام پرتکرار و تهیه پیش‌نویس‌های اولیه گزارش‌هاست. تحلیل مطالعات نشان می‌دهد که کاهش زمان اجرای این فعالیت‌ها در بسیاری از موارد قابل توجه بوده و در برخی گزارش‌ها به بیش از ۷۰ درصد می‌رسد. با این حال، یافته‌های تفسیری نشان می‌دهند که کارکرد اصلی اتوماسیون، صرفا افزایش سرعت یا کاهش هزینه نیست. بلکه مهم‌ترین پیامد آن، آزادسازی ظرفیت زمانی و شناختی حسابرسان است. در منطق حسابرسی چابک، کارایی به عنوان هدف نهایی تلقی نمی‌شود، بلکه به منزله شرط لازم برای حرکت به سطوح بالاتر ارزش‌آفرینی است. در بسترSME ها، این آزادسازی ظرفیت امکان انتقال نقش حسابرس از مجری رویه‌های از پیش تعریف شده به تحلیل‌گر ریسک و مشاور کسب‌وکار را فراهم می‌کند.

بنابراین، هم‌افزایی در این سطح، زیرساخت عملیاتی لازم برای تحول کیفی فرآیند حسابرسی را ایجاد می‌کند.

### هم‌افزایی بینش‌ساز: تقویت قضاوت حرفه‌ای در مقیاس و عمق نوین

پس از تحقق آزادسازی ظرفیت، هم‌افزایی به سطح کیفی‌تری ارتقا می‌یابد که در ادبیات به شکل تولید بینش تحلیلی منعکس شده است. یافته‌ها نشان می‌دهند که فناوری‌های پیشرفته هوش مصنوعی، به ویژه یادگیری ماشین، امکان تحلیل هم‌زمان حجم گسترده‌ای از داده‌های مالی و غیرمالی را فراهم می‌کنند. این قابلیت، شناسایی الگوهای غیرعادی، ناهنجاری‌های پیچیده و نشانه‌های بالقوه تقلب یا خطا را در سطحی فراتر از روش‌های سنتی ممکن می‌سازد. تحلیل تفسیری نشان می‌دهد که خروجی‌های هوش مصنوعی، در مطالعات موفق، به عنوان جایگزین قضاوت حرفه‌ای تلقی نشده‌اند، بلکه نقش شواهد تقویت‌کننده و جهت‌دهنده قضاوت حسابرس را ایفا می‌کنند. حسابرسان با اتکا به این خروجی‌ها، برنامه حسابرسی را به صورت پویا و مبتنی بر ریسک بازتنظیم می‌کنند، دامنه آزمون‌ها را هدفمندتر انتخاب کرده و تعاملات تحلیلی عمیق‌تری با مدیریت برقرار می‌سازند. یافته‌ها همچنین نشان می‌دهند که پیچیدگی بیشتر الگوریتم‌ها لزوما به بینش مؤثرتر منجر نمی‌شود. در بسیاری از SMEها، الگوریتم‌های ساده اما متناسب با مدل کسب‌وکار، اثربخشی بالاتری در حمایت از قضاوت حرفه‌ای داشته‌اند.

### هم‌افزایی ارتباطی: دگرگونی در پویایی گزارش‌دهی و تعامل با ذی‌نفعان

سطح سوم هم‌افزایی به تحول در گزارش‌دهی حسابرسی و تعامل با ذی‌نفعان اختصاص دارد. یافته‌ها نشان می‌دهند که فناوری‌های پردازش زبان طبیعی و ابزارهای هوشمند گزارش‌دهی، امکان بیان نتایج تحلیلی پیچیده به روایت‌های قابل فهم برای مدیران غیرمالی را فراهم کرده‌اند. داشبوردهای تعاملی، گزارش‌های مدیریتی پویا و بازخوردهای بلادرنگ، از جمله نمودهای این تحول است. تحلیل تفسیری نشان می‌دهد که این هم‌افزایی ارتباطی، حسابرسی را از یک رویداد دوره‌ای به یک فرآیند تعاملی و مستمر تبدیل می‌کند. چرخه‌های کوتاه بازخورد در حسابرسی چابک، شفافیت، اعتماد و مشارکت ذی‌نفعان را افزایش می‌دهد. با این حال، یافته‌ها به روشنی نشان می‌دهند که تحقق این سطح از هم‌افزایی، بدون دستیابی به دو مضمون پیشین یعنی آزادسازی ظرفیت و تولید بینش تحلیلی، امکان‌پذیر نیست و در غیر این صورت به گزارش‌دهی سطحی و نمایشی محدود می‌شود.

## عوامل تعدیل‌گر و مرزهای تحقق هم‌افزایی

یافته‌های تفسیری نشان می‌دهند که مسیر هم‌افزایی میان هوش مصنوعی و حسابرسی چابک، همواره یکنواخت و خطی نیست. شدت و جهت این هم‌افزایی تحت تأثیر مجموعه‌ای از عوامل تعدیل‌گر قرار دارد. محدودیت منابع مالی و انسانی، کیفیت پایین داده‌ها و فقدان مهارت‌های ترکیبی در حوزه حسابرسی، فناوری و تحلیل کسب‌وکار، از مهم‌ترین موانع شناسایی شده‌اند. علاوه بر این، موانع فرهنگی و شناختی مانند مقاومت در برابر تغییر، بی‌اعتمادی به خروجی‌های هوش مصنوعی و ضعف فرهنگ یادگیری سازمانی، نقش قابل توجهی در تضعیف هم‌افزایی دارند.

در سطح نهادی و حرفه‌ای نیز، نبود استانداردها و راهنماهای شفاف برای حسابرسی مبتنی بر هوش مصنوعی، ابهام در مسئولیت‌های قانونی و حرفه‌ای و فقدان مدل‌های قیمت‌گذاری متناسب با ارزش افزوده ایجاد شده، به عنوان مرزهای اصلی تحقق هم‌افزایی شناسایی شده‌اند. تحلیل نشان می‌دهد که در چنین شرایطی، استفاده از فناوری ممکن است صرفا ظاهری باشد، در حالی که منطق عملیاتی سنتی همچنان حاکم باقی بماند. هم‌افزایی پایدار، تنها زمانی محقق می‌شود که فناوری مناسب، توسعه قابلیت‌های انسانی و تطبیق چارچوب‌های راهبری به صورت همزمان مورد توجه قرار گیرند.

**جدول ۲**

*توصیف نظام‌مند مطالعات منتخب بر اساس سطح تحلیل، فناوری و نوع مطالعه*

| سطح تحلیل | فناوری محوری هوش مصنوعی | حوزه تمرکز | نوع مطالعه | مؤلف و سال |
|---|---|---|---|---|
| فرآیند حسابرسی | یادگیری ماشین | حسابرسی | تجربی کمی | فدیک و همکاران، ۲۰۲۲ |
| حرفه حسابرسی | چارچوب‌های AI | حسابرسی | مفهومی | لئوگادیو و همکاران، ۲۰۲۴ |
| سازمان و حرفه | RPA، ML، NLP | حسابداری و حسابرسی | مرور نظام‌مند | کسار و جیزی، ۲۰۲۵ |
| ... | ... | ... | ... | ... |
| مجموع | | | ۵۲ مطالعه | |

جدول ۲ تصویری نظام‌مند از نوع فناوری‌های هوش مصنوعی به کار رفته در مطالعات منتخب و کارکردهای حسابرسی متناظر با آن‌ها ارائه می‌دهد. این جدول نشان می‌دهد که تمرکز غالب ادبیات بر فناوری‌های اتوماسیون و الگوریتم‌های قاعده‌مند در مراحل ابتدایی حسابرسی است، در حالی که کاربردهای پیشرفته‌تر مانند یادگیری ماشین و تحلیل پیش‌بینانه سهم کمتری دارند. این الگو بیانگر آن است که در بستر شرکت‌های کوچک و متوسط، منطق پیاده‌سازی فناوری عمدتا مبتنی بر حل مسائل عملیاتی فوری و محدودیت منابع است. یافته‌های این جدول مبنای استنتاج مضمون «هم‌افزایی کارایی‌بخش» بوده و نشان می‌دهد که آزادسازی ظرفیت زمانی حسابرسان، نخستین گام تحقق هم‌افزایی میان هوش مصنوعی و حسابرسی چابک محسوب می‌شود.

**جدول ۳**

*مضامین نظری مبتنی بر تحلیل تفسیری اصلی و فرعی هم‌افزایی هوش مصنوعی و حسابرسی چابک*

| مضمون اصلی | مضمون فرعی | تبیین تفسیری | شواهد منتخب از ادبیات |
|---|---|---|---|
| هم‌افزایی کارایی‌بخش | اتوماسیون وظایف تکراری | خودکارسازی فعالیت‌های قاعده‌مند و پرحجم منجر به آزادسازی زمان حسابرس می‌شود | فدیک و همکاران، ۲۰۲۲؛ کسار و جیزی، ۲۰۲۵ |
| هم‌افزایی بینش‌ساز | کشف ناهنجاری‌ها | تحلیل جامع داده‌ها امکان شناسایی الگوهای پنهان ریسک را فراهم می‌کند | لئوگادیو و همکاران، ۲۰۲۴ |
| هم‌افزایی ارتباطی | گزارش‌دهی تعاملی | تبدیل گزارش ایستا به فرآیند ارتباط مستمر و مبتنی بر داده | کسار و جیزی، ۲۰۲۵ |
| عوامل تعدیل‌گر | بلوغ داده و مهارت | کیفیت داده و توانمندی انسانی شرط تحقق هم‌افزایی است | فدیک و همکاران، ۲۰۲۲ |

جدول ۳ نتایج کدگذاری تفسیری مطالعات را در قالب سطوح متمایز هم‌افزایی و پیامدهای حرفه‌ای هر سطح خلاصه می‌کند. این جدول نشان می‌دهد که هم‌افزایی میان هوش مصنوعی و حسابرسی چابک به صورت تدریجی و سلسله‌مراتبی شکل می‌گیرد و از کارایی عملیاتی به

تولید بینش تحلیلی و سپس تحول در تعاملات حرفه‌ای گسترش می‌یابد. تحلیل این جدول نشان می‌دهد که مطالعاتی که صرفا بر بهبود کارایی تمرکز دارند، به پیامدهای محدودتری دست یافته‌اند، در حالی که پژوهش‌هایی که به سطوح بالاتر هم‌افزایی پرداخته‌اند، نقش هوش مصنوعی را در تقویت قضاوت حرفه‌ای و ارزش‌آفرینی حسابرسی برجسته کرده‌اند. این جدول پشتوانه تجربی ساختار مضامین نظری مبتنی بر تحلیل تفسیری را فراهم می‌کند.

**جدول ٤**

*هم‌راستایی مضامین تفسیری با اصول حسابرسی چابک*

| مؤلفه حسابرسی چابک | فناوری پشتیبان | نقش در هم‌افزایی | پیامد برایSME ها |
|---|---|---|---|
| سرعت و کارایی | RPA | کاهش زمان اجرای رویه‌ها | کاهش هزینه حسابرسی |
| انعطاف‌پذیری | یادگیری ماشین | تنظیم پویای برنامه حسابرسی | تمرکز بر ریسک‌های واقعی |
| بینش‌محوری | تحلیل داده پیشرفته | ارتقای قضاوت حرفه‌ای | ارزش افزوده مدیریتی |
| شفافیت | NLPو داشبوردها | بهبود ارتباط با مدیریت | افزایش اعتماد |

جدول ۴ تغییر نقش حسابرس را در سطوح مختلف هم‌افزایی نشان داد. نتایج این جدول حاکی از آن بود که با افزایش سطح هم‌افزایی، نقش حسابرس از مجری رویه‌های استاندارد به تحلیل‌گر ریسک و در نهایت به مشاور راهبردی کسب‌وکار تغییر یافت. همچنین، این تحول نقش به‌طور مستقیم با میزان به‌کارگیری هدفمند ابزارهای هوش مصنوعی و منطق چابک در برنامه‌ریزی حسابرسی مرتبط شناخته شد. افزون بر این، جدول ۳ نشان داد که در بسیاری از مطالعات، عدم تحقق این تحول نقش به محدودیت‌های مهارتی و نهادی نسبت داده شد. در مجموع، این یافته‌ها اهمیت توسعه هم‌زمان قابلیت‌های انسانی و فناورانه را برای تحقق هم‌افزایی واقعی آشکار ساختند.

**جدول ۵**

*عوامل تعدیل‌گر زمینه‌ای در بستر SMEها*

| سطح عامل | شرح عامل | اثر بر هم‌افزایی | شواهد |
|---|---|---|---|
| فنی | کیفیت پایین داده | تضعیف خروجی الگوریتم‌ها | فدیک و همکاران، ۲۰۲۲ |
| انسانی | کمبود مهارت ترکیبی | استفاده سطحی ازAI | کسار و جیزی، ۲۰۲۵ |
| سازمانی | مقاومت فرهنگی | کندی پذیرش حسابرسی چابک | لئوگادیو و همکاران، ۲۰۲۴ |
| نهادی | ابهام مقرراتی | ریسک مسئولیت حرفه‌ای | فدیک و همکاران، ۲۰۲۲ |

جدول ۵ مجموعه‌ای از عوامل تعدیل‌گر شناسایی‌شده در مطالعات منتخب را که بر شدت و جهت هم‌افزایی تأثیر می‌گذارند، طبقه‌بندی می‌کند. این جدول نشان می‌دهد که محدودیت منابع، کیفیت داده‌ها، فرهنگ سازمانی و چارچوب‌های نهادی، نقش تعیین‌کننده‌ای در موفقیت یا شکست پیاده‌سازی هم‌افزایی دارند. تحلیل جدول نشان می‌دهد که حتی در حضور فناوری‌های پیشرفته، فقدان زیرساخت نهادی و مهارت‌های ترکیبی می‌تواند منجر به استفاده سطحی از هوش مصنوعی شود. این جدول مرزهای تحقق هم‌افزایی را مشخص کرده و نشان می‌دهد که هم‌افزایی پایدار نتیجه تعامل هم‌زمان فناوری، انسان و راهبری حرفه‌ای است، نه صرفا استقرار ابزارهای هوشمند.

## بحث

تحلیل تفسیری پژوهش حاضر نشان می‌دهد که تعامل میان هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط، ماهیتی چندلایه، پویا و زمینه‌محور دارد. یافته‌ها چارچوب مفهومی اولیه را تأیید کرده و آن را با برجسته‌سازی سه ویژگی تکمیل می‌کنند :سلسله‌مراتب قابلیت‌ها، غیرخطی بودن روابط و وابستگی تحقق هم‌افزایی به عوامل سازمانی و محیطی .بر این اساس، هم‌افزایی میان هوش مصنوعی و حسابرسی چابک نه حاصل هم‌زمانی دو نوآوری فناورانه و روش‌شناختی، بلکه نتیجه فرایندی تدریجی است که طی آن خدمات حسابرسی با فرصت‌ها و محدودیت‌های فناوری هوشمند سازگار می‌شوند.

در نخستین سطح، هم‌افزایی از اتوماسیون فعالیت‌های تکراری و قاعده‌مند آغاز می‌شود. فناوری‌هایی مانند رباتیک فرایندهای خودکار (RPA) می‌توانند استخراج و تطبیق داده‌ها، اجرای

آزمون‌های کنترلی پایه و تهیه پیش‌نویس گزارش‌ها را تسریع کنند و از این طریق، مؤلفه‌های سرعت و کارایی حسابرسی چابک را تقویت نمایند (براون و همکاران[1]، ۲۰۲۲). اهمیت این تحول صرفاً در بهبود کارایی نیست؛ بلکه اتوماسیون، امکان انتقال تمرکز حسابرسان از اجرای رویه‌های تکراری به تحلیل و قضاوت حرفه‌ای را فراهم می‌کند. این ظرفیت درSME ها، که معمولاً با محدودیت منابع انسانی و فشارهای زمانی مواجه‌اند، اهمیت بیشتری دارد.

در سطح بعد، توانمندسازی تحلیلی از طریق یادگیری ماشین و تحلیل داده‌های بزرگ، امکان شناسایی الگوهای پنهان، ناهنجاری‌های پیچیده و ریسک‌های سیستماتیک را فراهم می‌سازد؛ مواردی که ممکن است در روش‌های نمونه‌گیری سنتی کمتر شناسایی شوند (فام و همکاران[2]، ۲۰۲۵). در این سطح، خروجی‌های تحلیلی هوش مصنوعی مکمل قضاوت حرفه‌ای حسابرس هستند و با هدایت منابع به سمت حوزه‌های پرریسک‌تر، انعطاف‌پذیری و ارزش‌آفرینی حسابرسی چابک را افزایش می‌دهند. با این حال، اثربخشی این قابلیت بیش از آنکه به پیشرفته بودن ابزار وابسته باشد، به ادغام فناوری با منطق حسابرسی چابک و شناخت محیط کسب‌وکارSME ها بستگی دارد.

در سطح سوم، هم‌افزایی ارتباطی و گزارش‌دهی شکل می‌گیرد. فناوری‌های پردازش زبان طبیعی(NLP) ، داشبوردهای پویا و سیستم‌های گزارش‌دهی هوشمند می‌توانند یافته‌های پیچیده تحلیلی را به اطلاعات قابل فهم برای مدیران و سایر ذی‌نفعان تبدیل کنند. در نتیجه، حسابرسی از فرایندی عمدتاً یک‌طرفه و گزارش‌محور به تعاملی مستمر، مشارکتی و چرخه‌ای نزدیک می‌شود (کوکینا و همکاران[3]، ۲۰۲۵ : ۱۸). با این حال، تحقق این سطح از هم‌افزایی مستلزم وجود دو قابلیت پیشین، یعنی اتوماسیون کارا و تولید بینش معتبر، است.

این یافته‌ها نشان می‌دهند که هم‌افزایی هوش مصنوعی و حسابرسی چابک فرایندی خطی و خودکار نیست. محدودیت منابع مالی، کمبود مهارت‌های ترکیبی در حوزه فناوری، حسابرسی و کسب‌وکار، و چالش‌های فرهنگی مانند اعتماد، مقاومت در برابر تغییر و پذیرش فناوری می‌توانند شدت و مسیر این هم‌افزایی را تغییر دهند (مانال و همکاران[4]، ۲۰۲۴ : ۷؛ هانگ و ,واسرهلی[5]، ۲۰۱۹: ۹). ازاین‌رو، استفاده مؤثر از هوش مصنوعی نیازمند هم‌ترازی سه رکن اصلی، یعنی فناوری مناسب،

[1] Braun, & Clarke, 2022
[2] Pham et al., 2025
[3] Kokina et al., 2025
[4] Manal et al., 2024
[5] Huang & Vasarhelyi, 2019

سرمایه انسانی توانمند و فرهنگ سازمانی و حرفه‌ای پشتیبان است. در صورت نبود این هم‌ترازی، فناوری ممکن است صرفاً به اتوماسیون محدود فعالیت‌ها منجر شود و نتواند تحول مورد انتظار در کیفیت و ارزش خدمات حسابرسی را ایجاد کند.

یافته‌های پژوهش با مطالعات بین‌المللی که بر نقش هوش مصنوعی در ارتقای کیفیت تصمیم‌گیری، تحلیل ریسک و افزایش کارایی فرایندهای حسابرسی تأکید کرده‌اند، همسو است (فدیک و همکاران، ۲۰۲۲: ۹۸۰؛ لئوگادیو و همکاران، ۲۰۲۴: ۲۳۸؛ کسار و جیزی، ۲۰۲۵ : ۲۳۷). با این حال، تحلیل تفسیری حاضر نشان می‌دهد که ارزش هوش مصنوعی در محیط حسابرسی صرفاً به خودکارسازی فعالیت‌های تکراری محدود نمی‌شود، بلکه از تعامل میان فناوری، قضاوت حرفه‌ای و اصول حسابرسی چابک ناشی می‌شود. از این منظر، پژوهش حاضر تبیین تک‌بعدی فناوری‌محور مطالعات پیشین را به سوی تبیینی چندسطحی از سازوکارهای هم‌افزایی فناوری و فرایندهای حرفه‌ای توسعه می‌دهد.

در مطالعات داخلی نیز، دوازده مطالعه فارسی منتخب استخراج‌شده از پایگاه‌های SID ، مگیران، نورمگز و Ensani.ir عمدتاً هوش مصنوعی، تحول دیجیتال، حسابرسی هوشمند و حسابرسی چابک را به‌صورت مستقل بررسی کرده و بیشتر بر فرصت‌ها، چالش‌ها، الزامات استقرار فناوری و بهبود فرایندهای حسابرسی تمرکز داشته‌اند (رحمانی و همکاران، ۱۴۰۴ : ۹؛ زارع و همکاران، ۱۴۰۳: ۴۳؛ محمدی نوره و همکاران، ۱۴۰۰ : ۱۵۵؛ حمزه و رامشه، ۱۴۰۲: ۸۸؛ مطلبی کربکندی و همکاران، ۱۴۰۱ : ۱۱؛ سیرنگ و همکاران، ۱۴۰۳ : ۱۵۲). در مقابل، پژوهش حاضر با بهره‌گیری از مرور نظام‌مند تفسیری، یافته‌های مطالعات داخلی و بین‌المللی را در یک چارچوب مفهومی تلفیق کرده و روابط میان مضامین، سازوکارهای شکل‌گیری هم‌افزایی و شرایط تحقق آن را برای شرکت‌های کوچک و متوسط تبیین می‌کند. بنابراین، نوآوری پژوهش صرفاً در گردآوری مطالعات پیشین نیست، بلکه در بازترکیب و بازتفسیر نظام‌مند مضامین و ارائه یک چارچوب تفسیری یکپارچه است.

با وجود ظرفیت‌های شناسایی‌شده، تحقق این الگو در بستر شرکت‌ها و مؤسسات حسابرسی کوچک و متوسط ایران با محدودیت‌های ساختاری مواجه است. بخش قابل توجهی از شرکت‌های کوچک و متوسط ایران هنوز از سامانه‌های یکپارچه برنامه‌ریزی منابع سازمان (ERP) بهره‌مند نیستند و اطلاعات مالی آن‌ها در نرم‌افزارهای جزیره‌ای یا فرایندهای نیمه‌دستی نگهداری می‌شود. در چنین شرایطی، استفاده مؤثر از یادگیری ماشین، تحلیل داده‌های بزرگ و RPA ، که به داده‌های

استاندارد، یکپارچه و باکیفیت نیاز دارند، با چالش مواجه خواهد بود. از سوی دیگر، بسیاری از مؤسسات حسابرسی ایران، به‌ویژه مؤسسات کوچک و متوسط، نیز در مراحل اولیه تحول دیجیتال قرار دارند و استقرار اثربخش فناوری‌های هوش مصنوعی در آن‌ها مستلزم سرمایه‌گذاری در زیرساخت‌های دیجیتال و ارتقای شایستگی‌های فناورانه حسابرسان است.

افزون بر الزامات فناورانه، حمایت نهادی و حرفه‌ای نیز برای تحقق این هم‌افزایی ضروری است. جامعه حسابداران رسمی ایران و سازمان حسابرسی می‌توانند از طریق تدوین رهنمودهای حرفه‌ای، ارائه برنامه‌های آموزشی، بازنگری استانداردهای حسابرسی متناسب با فناوری‌های نوین و تبیین الزامات استفاده از هوش مصنوعی، به کاهش ریسک‌های حرفه‌ای و افزایش پذیرش این فناوری‌ها کمک کنند. بنابراین، تحقق هم‌افزایی میان هوش مصنوعی و حسابرسی چابک در ایران مستلزم ترکیبی از بلوغ دیجیتال بنگاه‌ها، یکپارچه‌سازی اطلاعات مالی، توسعه شایستگی‌های فناورانه حسابرسان و تقویت چارچوب‌های حرفه‌ای و نهادی است؛ در غیر این صورت، کاربرد هوش مصنوعی ممکن است در سطح اتوماسیون محدود باقی بماند و به بهبود واقعی کیفیت حسابرسی منجر نشود (رایش و کراکوفسکی، ۲۰۲۱ : ۱۹۸؛ لئوگادیو و همکاران، ۲۰۲۴ :۲۴۱ ؛ کسار و جیزی، ۲۰۲۵ : ۲۲۷).

**جدول ٦**

*سطح‌های هم‌افزایی هوش مصنوعی و حسابرسی چابک در SMEها*

| سطح هم‌افزایی | فناوری/ابزار کلیدی | اثر بر حسابرسی چابک | پیامد برای SME |
|---|---|---|---|
| **عملیاتی** | RPA، الگوریتم‌های قاعده‌مند | افزایش سرعت، کاهش خطا، آزادسازی ظرفیت حسابرس | تمرکز بر تحلیل و قضاوت حرفه‌ای، کاهش هزینه‌های نیروی انسانی |
| **بینش‌ساز** | یادگیری ماشین، شبکه‌های عصبی، تحلیل داده‌های بزرگ | شناسایی الگوهای پنهان و ناهنجاری‌ها، تقویت تصمیم‌گیری مبتنی بر ریسک | هدایت منابع به حوزه‌های با ریسک و فرصت بالاتر، انعطاف‌پذیری برنامه حسابرسی |
| **ارتباطی** | پردازش زبان طبیعی، داشبوردهای تعاملی، گزارش‌دهی هوشمند | افزایش شفافیت و مشارکت ذی‌نفعان، ارتباط مؤثر با مدیریت | ارزش ادراک‌شده بالاتر، همکاری مستمر، اعتماد متقابل |

## نتیجه‌گیری، محدودیت‌ها و پیشنهادها

این پژوهش با بهره‌گیری از مرور نظام‌مند تفسیری، سازوکارهای هم‌افزایی میان هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط را تبیین کرد. یافته‌ها نشان داد که این هم‌افزایی یک توانمندی سازمانی پویا و چندبعدی است که بر تعامل میان فناوری، سرمایه انسانی و بستر سازمانی استوار است. نتایج پژوهش بیانگر آن است که تحقق این هم‌افزایی از یک مسیر تکاملی شامل اتوماسیون فرآیندهای حسابرسی، تولید بینش‌های تحلیلی و ارتقای تعامل و گزارش‌دهی هوشمند شکل می‌گیرد و در تمامی این مراحل، کیفیت داده‌ها، قضاوت حرفه‌ای حسابرس و عوامل زمینه‌ای، نقش تعیین‌کننده‌ای در موفقیت استقرار فناوری‌های هوش مصنوعی دارند.

یافته‌های پژوهش همچنین نشان داد که بهره‌برداری اثربخش از هوش مصنوعی در حسابرسی، صرفاً به توسعه فناوری وابسته نیست، بلکه مستلزم هم‌ترازی راهبردی میان زیرساخت‌های دیجیتال، مهارت‌های حرفه‌ای حسابرسان، فرهنگ سازمانی و حمایت‌های نهادی است. از این‌رو، هوش مصنوعی زمانی می‌تواند ارزش‌آفرین باشد که در چارچوب اصول حسابرسی چابک و با حفظ نقش قضاوت حرفه‌ای حسابرس به‌کار گرفته شود. نوآوری اصلی پژوهش حاضر، ارائه یک چارچوب تفسیری یکپارچه برای تبیین سازوکارهای شکل‌گیری هم‌افزایی میان هوش مصنوعی و حسابرسی چابک در شرکت‌های کوچک و متوسط است؛ چارچوبی که روابط میان قابلیت‌های فناورانه، عوامل سازمانی و محیطی و پیامدهای حرفه‌ای حسابرسی را به‌صورت هم‌زمان تبیین می‌کند. این چارچوب می‌تواند مبنایی برای توسعه پژوهش‌های آتی و همچنین راهنمایی برای سیاست‌گذاران، نهادهای حرفه‌ای، مؤسسات حسابرسی و مدیران شرکت‌های کوچک و متوسط در برنامه‌ریزی تحول دیجیتال، توسعه زیرساخت‌های اطلاعاتی، تدوین استانداردهای حرفه‌ای و ارتقای مهارت‌های فناورانه حسابرسان باشد.

با وجود تلاش برای انجام یک مرور نظام‌مند و جامع، این پژوهش با محدودیت‌هایی نیز همراه است. نخست، دامنه پژوهش به مطالعات منتشرشده به زبان‌های فارسی و انگلیسی محدود بوده و احتمال دارد برخی مطالعات منتشرشده به سایر زبان‌ها یا منابع خاکستری (مانند گزارش‌های حرفه‌ای و اسناد سیاستی) در تحلیل نهایی لحاظ نشده باشند. دوم، پژوهش حاضر

بر مطالعات منتشرشده در بازه زمانی مورد بررسی متمرکز بوده و بنابراین، انتشار پژوهش‌های جدید می‌تواند به تکمیل یا بازنگری برخی یافته‌ها منجر شود. سوم، ماهیت مرور نظام‌مند تفسیری موجب می‌شود نتایج پژوهش بر پایه تحلیل و تفسیر مطالعات پیشین استوار باشد و نه داده‌های تجربی حاصل از شرکت‌ها یا مؤسسات حسابرسی؛ ازاین‌رو، تعمیم نتایج به سایر محیط‌های سازمانی باید با احتیاط انجام شود.

پیشنهاد می‌شود پژوهش‌های آینده با استفاده از داده‌های تجربی شرکت‌های کوچک و متوسط و مؤسسات حسابرسی ایران، چارچوب پیشنهادی این پژوهش را اعتبارسنجی کنند. همچنین، بررسی تأثیر سطح بلوغ دیجیتال، کیفیت زیرساخت‌های اطلاعاتی، فرهنگ سازمانی، سیاست‌های حرفه‌ای و الزامات مقرراتی بر موفقیت استقرار هوش مصنوعی در حسابرسی چابک، و نیز انجام مطالعات مقایسه‌ای میان کشورهای در حال توسعه و توسعه‌یافته، می‌تواند به توسعه و تعمیم ادبیات این حوزه کمک کند.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع

حمزه، احسان و رامشه، منیژه. (۱۴۰۲). حسابرسی در عصر دیجیتال: کاربست روش‌های دلفی فازی و ماباک در ایران. *نشریه پژوهش‌های حسابداری مالی*، ۱۵(۳)، ۷۵–۱۰۲. https://doi.org/10.22108/far.2024.140234.2028

رحمانی، علی، معنوی، سمیرا و حدادی، نفیسه. (۱۴۰۴). ادغام هوش مصنوعی در حسابرسی؛ چالش‌ها و مزایا. *حسابرسی سیستم‌ها و فناوری اطلاعات*، ۱(۱)، ۱–۲۷. https://doi.org/10.22034/jista.2025.528769.1051

زارع، حمید، حاجی‌ها، زهره و کیقبادی، امیررضا. (۱۴۰۳). بررسی تأثیر استفاده از هوش مصنوعی بر کیفیت فرایند حسابرسی صورت‌های مالی. *پژوهش‌های حسابرسی حرفه‌ای*، ۴(۱۶)، ۳۸–۶۵. https://doi.org/10.22034/jpar.2024.2011220.1224

زنگنه، مهدی، جمشیدی‌نوید، بابک، قنبری، مهرداد و محمدی یاریجانی، فروزان. (۱۴۰۵). ارائه الگویی برای فرصت‌ها و چالش‌های تصمیم‌گیری مبتنی بر هوش مصنوعی در فرآیند حسابرسی. *دانش حسابداری و حسابرسی مدیریت*، ۱۵(۶۰)، ۱۷۵–۱۹۰. https://doi.org/10.22034/jmaak.2026.23984

سیرنگ، بهروز، حجازی، رضوان، کنعانی، اکبر و محمدزاده سلطه، حیدر. (۱۴۰۳). ارائه الگوی حسابرسی داخلی چابک مبتنی بر حاکمیت فناوری داده و ارزیابی ریسک پویا. *نشریه اقتصاد و بانکداری اسلامی*، ۱۳(۴۹)، ۱۴۹–۱۷۳. https://mieaoi.ir/article-1-1610-fa.html

عدنان حمود، محمد، پیری، پرویز و آشتاب، علی. (۱۴۰۴). امکان‌سنجی بهره‌گیری از فناوری‌های نوین هوش مصنوعی در بهبود فرایندهای حسابرسی در کشور. *بررسی‌های حسابداری و حسابرسی*، ۳۲(۳)، ۵۳۵–۵۵۹. https://doi.org/10.22059/acctgrev.2025.391837.1009085

عبدی برآفتابی، عبدالله، صمدی، فاطمه، شاهوردیانی، شادی و حاجی‌ها، زهره. (۱۴۰۴). نقش چرخه حسابرسی داخلی مبتنی بر فنون یادگیرنده و هوش مصنوعی و تأثیرات آن در بهبود فرآیندهای حسابرسی. *دانش حسابداری و حسابرسی مدیریت*، ۱۶(۶۲)، ۴۴۳–۴۵۷. https://doi.org/10.22034/jmaak.2025.78407.4530

عاشوری اکبر، رحمانی محمود و جبارزاده کنگرلوئی، سعید. (۱۴۰۳). ارائه الگوی سلامت مالی در مؤسسات کوچک و متوسط با تأکید بر رویکرد ساختاری–تفسیری. *دانش حسابرسی*، ۲۴(۹۴)، ۱۸۸–۲۲۲. http://danesh.dmk.ir/article-1-3104-fa.html

مجلی حسن حسن، ازهار، محسنی، عبدالرضا، عبد موسی السعیری، ابراهیم و سروش‌یار، افسانه. (۱۴۰۴). ارائه مدل مفهومی آینده حرفه حسابداری در عصر دیجیتال با استفاده از روش گرند تئوری و مدل تحلیل فازی. *دانش حسابداری و حسابرسی مدیریت*، ۱۶(۶۱)، ۳۷۳–۳۸۵. https://doi.org/10.22034/jmaak.2025.24086

محمدی نوره، شاکر، رحیمیان، نظام‌الدین و احمدی دهرشید، جمیل. (۱۴۰۰). بررسی تأثیر دیجیتالی شدن بر حسابرسان مستقل و مؤسسات حسابرسی در ایران. پژوهش‌های حسابرسی حرفه‌ای، ۱(۳)، ۱۵۰–۱۷۶. https://doi.org/10.22034/arj.2021.247704

محمودی میمند، محمد و محسنی‌فرد، ندا. (۱۴۰۳). تأثیر پذیرش هوش مصنوعی مولد بر عملکرد سازمانی شرکت‌های کوچک و متوسط. *نشریه علمی رویکردهای پژوهشی نوین مدیریت و حسابداری*، ۸(۲۸)، ۲۴۴۹–۲۴۶۳. https://majournal.ir/index.php/ma/article/view/2662

مطلبی کربکندی، مصطفی، آذر، عادل، خدیور، آمنه و مقبل، عباس. (۱۴۰۱). طراحی مدل حسابرسی هوشمند در دیوان محاسبات کشور. *پژوهش‌های مدیریت عمومی*، ۱۵(۵۸)، ۵–۳۲. https://doi.org/10.22111/jmr.2022.43008.5818

## References

Abdi Baraftabi, A., Samadi, F., Shahvardiani, S., & Hajjiha, Z. (2025). The role of the internal audit cycle based on machine learning techniques and artificial intelligence and its effects on improving auditing processes. *Journal of Management Accounting and*

*Auditing Knowledge*, 16(62), 443–457. https://doi.org/10.22034/jmaak.2025.78407.4530 (in Persian)

Adnan Hamoud, M., Piri, P., & Ashtab, A. (2025). Feasibility of utilizing emerging artificial intelligence technologies to improve auditing processes in Iran. *Accounting and Auditing Reviews*, 32(3), 535–559. https://doi.org/10.22059/acctgrev.2025.391837.1009085 (in Persian)

Ashouri Akbar, R., Rahmani Mahmoud, M., & Jabbarzadeh Kangarlouei, S. (2024). Developing a financial health model for small and medium-sized enterprises with an emphasis on the structural–interpretive approach. *Audit Knowledge*, 24(94), 188–222. http://danesh.dmk.ir/article-1-3104-fa.html (in Persian)

Agustí, M., & Orta-Pérez, M. (2022). Big data and artificial intelligence in the fields of accounting and auditing: A bibliometric analysis. *REFC – Spanish Journal of Finance and Accounting*. Available at SSRN. https://ssrn.com/abstract=4155537

Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide. Sage Publications .

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*. https://doi.org/10.1007/s11142-022-09697-x

Hamzeh, E., & Ramsheh, M. (2024). Auditing in the digital era: Application of fuzzy Delphi and MABAC methods in Iran. *Financial Accounting Research*, 15(3), 75–102. https://doi.org/10.22108/far.2024.140234.2028 (in Persian)

Huang, F. Y., & Vasarhelyi, M. (2019). Applying robotic process automation (RPA) in auditing: A framework. *International Journal of Accounting Information Systems*, 35, 100433. https://doi.org/10.1016/j.accinf.2019.100433

Kassar, M., & Jizi, M. (2025). Artificial intelligence and robotic process automation in auditing and accounting: A systematic literature review. *Journal of Applied Accounting Research*. 27 (1): 217–241. https://doi.org/10.1108/JAAR-05-2024-0175

Kokina, J., Blanchette, S., Davenport, T. H., & Pachamanova, D. (2025). Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. *International Journal of Accounting Information Systems*, 56, 100734. https://doi.org/10.1016/j.accinf.2025.100734

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial intelligence in auditing: A conceptual framework for auditing practices. *Administrative Sciences*, 14(10), 238. https://doi.org/10.3390/admsci14100238

Manal, Y., Nawazish, M., Adnan, S., & Muhammad, U. (2024). Impact of audit quality and digital transformation on innovation efficiency: Role of financial risk-taking. *Global Finance Journal*, 62, 101026. 1-15 https://doi.org/10.1016/j.gfj.2024.101026

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, 10(1), 89. https://doi.org/10.1136/bmj.n71

Pham, V. A. T., Nguyen, L. A., Dellaportas, S., Phan, D. H. T., & Nguyen, Q. H. (2025). How does big data analytics impact accounting manipulation? *Accounting & Finance*, 65, 2918–2934. https://doi.org/10.1111/acfi.70024

Mahmoudi Meymand, M., & Mohseni-Fard, N. (2024). The impact of generative artificial intelligence adoption on the organizational performance of small and medium-sized enterprises. *Journal of Novel Research Approaches in Management and Accounting*, 8(28), 2449–2463. https://majournal.ir/index.php/ma/article/view/2662 (in Persian)

Majali Hassan Hassan, A., Mohseni, A., Abd Mousa Al-Saeeri, I., & Soroushyar, A. (2025). Developing a conceptual model for the future of the accounting profession in the digital era using grounded theory and fuzzy analysis. *Journal of Management Accounting and*

*Auditing Knowledge*, 16(61), 373–385. https://doi.org/10.22034/jmaak.2025.24086 (in Persian)

Matlabi Karbakandi, M., Azar, A., Khadivar, A., & Moqbel, A. (2022). Designing an intelligent auditing model for the Supreme Audit Court of Iran. *Public Management Research*, 15(58), 5–32. https://doi.org/10.22111/jmr.2022.43008.5818 (in Persian)

Mohammadi Noureh, S., Rahimian, N., & Ahmadi Dehrashid, J. (2021). Investigating the impact of digitalization on independent auditors and audit firms in Iran. *Journal of Professional Auditing Research*, 1(3), 150–176. https://doi.org/10.22034/arj.2021.247704 (in Persian)

Rahmani, A., Manavi, S., & Haddadi, N. (2025). Integration of artificial intelligence into auditing: Challenges and benefits. *Journal of Information Systems and Technology Auditing*, 1(1), 1–27. https://doi.org/10.22034/jista.2025.528769.1051 (in Persian)

Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review*, 46(1), 192–210. https://doi.org/10.5465/amr.2018.0072

Salijeni, G., Samsonova-Taddei, A., & Turley, S. (2021). Big data and changes in audit technology: Contemplating a research agenda. *Accounting and Business Research*, 51(3), 322–345. https://doi.org/10.1080/00014788.2018.1459458

Seethamraju, R., & Hecimovic, A. (2023). Adoption of artificial intelligence in auditing: An exploratory study. *Australian Journal of Management*, 48(4), 780–800. https://doi.org/10.1177/03128962221108440

Sirang, B., Hejazi, R., Kenaani, A., & Mohammadzadeh Soltah, H. (2024). Developing an agile internal auditing model based on data technology governance and dynamic risk assessment. *Journal of Islamic Economics and Banking*, 13(49), 149–173. https://mieaoi.ir/article-1-1610-fa.html (in Persian)

Sutton, S. G., Holt, M., & Arnold, V. (2016). The reports of my death are greatly exaggerated: Artificial intelligence research in accounting. *International Journal of Accounting Information Systems*, 22, 60–73. https://doi.org/10.1016/j.accinf.2016.07.005

Zangeneh, M., Jamshidi-Navid, B., Ghanbari, M., & Mohammadi Yarijani, F. (2026). Developing a model for the opportunities and challenges of artificial intelligence–based decision-making in the auditing process. *Journal of Management Accounting and Auditing Knowledge*, 15(60), 175–190. https://doi.org/10.22034/jmaak.2026.23984 (in Persian)

Zare, H., Hajiha, Z., & Keyghobadi, A. R. (2024). Investigating the impact of artificial intelligence on the quality of the financial statement auditing process. *Journal of Professional Auditing Research*, 4(16), 38–65. https://doi.org/10.22034/jpar.2024.2011220.1224 (in Persian)

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Research Paper**

# Design and Validation of an Organizational Cyber Resilience Governance Framework Based on Artificial Intelligence and Risk Management: A Mixed-methods Approach to Information Technology Governance [1]

**Amirhossein Kafi[*] [2], Mohammadali Soltanshahi [3], Mojtaba Reessafari[4] and Amirmohammad Kafi[5]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 263 - 302

Received: 2026.08.05
Revised: 2026.09.14
Accepted: 2026.10.17

## Abstract

With the rapid expansion of digital transformation and the growing sophistication of cyber threats, organizations require governance approaches that extend beyond traditional security controls to ensure business continuity and protect information assets. This study aims to design and validate an organizational cyber resilience governance framework based on artificial intelligence (AI) and risk management. The research is applied of purpose and adopts an exploratory mixed-methods design. In the qualitative phase, framework components were identified and refined through a systematic literature review of scientific publications published between 2020 to 2025, analysis of internationally recognized standards and frameworks—including The NIST Cybersecurity Framework (CSF) 2.0, NIST AI Risk Management Framework (AI RMF), COBIT 2019, ISO/IEC 27001:2022, ISO 31000, and COSO Enterprise Risk Management (ERM)—and a Delphi study involving experts in cybersecurity, risk management, and information technology governance. In the quantitative phase, the proposed framework was validated using a researcher-developed questionnaire and Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings Identified five core dimensions: Corporate Governance, Cyber Governance, Cyber Risk Management, Artificial Intelligence, and Continuous Learning. Their systematic integration strengthens organizational capabilities for predicting, preventing, detecting, responding to, recovering from, and adapting to cyber threats. The study contributes an integrated governance framework that combines corporate governance, risk management, and AI capabilities to enhance organizational cyber resilience and support strategic decision-making in an evolving cyber threat landscape.

**Keywords**: Cyber Resilience Governance, Artificial Intelligence, Cyber Risk Management, Corporate Governance, Cybersecurity.

**JEL classification:** *M15, M14, D81, O33, L86*

---

[1] https://doi.org/10.22034/JISTA.2026.595585.1093
[1] Selected paper of the 2nd National Conference on Corporate Governance and Information Technology Risk Management
[2] PhD in Information Technology, Expert in Technological Innovation and Smart Banking Strategies, Member of Bank Sepah Research Club, Tehran, Iran. (Corresponding Author). Email: amirhkafi@gmail.com
[3] PhD in Information Technology, Expert in Artificial Intelligence and Smart Systems Development, Member of Bank Sepah Research Club, Tehran, Iran. Email: ali.soltanshahi@gmail.com
[4] PhD in Information Technology, Expert in Digital Transformation and Smart Governance, Member of Bank Sepah Research Club, Tehran, Iran. Email: mgrd81@gmail.com
[5] PhD in Information Technology, Expert in Financial Technologies and Smart Systems Analysis, Member of Sky Innovation Core, Tehran, Iran. Email: amirmkafi@gmail.com.

## 1. INTRODUCTION

The rapid expansion of digital transformation, cloud-based services, interconnected information systems, and data-driven decision-making has fundamentally changed the operational environment of contemporary organizations. At the same time, the increasing frequency, complexity, and adaptability of cyber threats have exposed organizations to risks that cannot be effectively addressed through conventional information security controls alone. Cyber incidents can disrupt critical services, compromise information assets, damage organizational reputation, generate financial losses, and undermine strategic objectives. Consequently, organizations increasingly need to move from a predominantly preventive security perspective toward a broader concept of organizational cyber resilience that encompasses prediction, prevention, detection, response, recovery, and adaptation.

Cyber resilience is not solely a technical issue; rather, it is closely associated with organizational governance, risk management, decision-making, organizational learning, and the effective use of emerging technologies. In particular, artificial intelligence (AI) provides significant opportunities for identifying anomalous behavior, predicting cyber threats, supporting risk assessment, accelerating incident detection, and improving strategic decision-making. However, the use of AI also introduces new governance, security, ethical, and operational risks that must themselves be systematically managed.

Despite the growing literature on cybersecurity, cyber resilience, artificial intelligence, and risk management, these areas have often been examined separately. Existing approaches provide valuable guidance but do not necessarily offer an integrated organizational governance framework that simultaneously connects corporate governance, cyber governance, cyber risk management, AI capabilities, and continuous learning. This research therefore aims to design and validate an integrated organizational cyber resilience governance framework based on artificial intelligence and risk management. The study seeks to provide a governance-oriented approach capable of strengthening organizational resilience against evolving cyber threats while supporting effective strategic decision-making.

## 2. MATERIALS AND METHODS

This research is applied in terms of purpose and employs an exploratory mixed-methods design consisting of qualitative and quantitative phases. In the qualitative phase, the conceptual foundations and components of the proposed framework were identified through a systematic review of scientific publications published between 2020 and 2025. In addition, internationally recognized standards and frameworks relevant to cybersecurity, artificial intelligence, information technology governance, and risk management were examined.

The principal reference frameworks included the NIST Cybersecurity Framework (CSF) 2.0, NIST Artificial Intelligence Risk Management Framework (AI RMF), COBIT 2019, ISO/IEC 27001:2022, ISO 31000, and COSO Enterprise Risk Management (ERM). The identified concepts and components were subsequently refined and assessed using the Delphi method. A panel of experts with knowledge and professional experience in cybersecurity, risk management, and information technology governance participated in this phase.

Following the qualitative phase, a researcher-developed questionnaire was designed based on the validated conceptual components. The quantitative phase was conducted to assess and validate the proposed framework using Partial Least Squares Structural Equation Modeling (PLS-SEM). This approach enabled the relationships among the identified dimensions and the overall structure of the proposed organizational cyber resilience governance framework to be examined.

## 3. RESULTS AND DISCUSSION

The findings of the qualitative and quantitative phases indicate that organizational cyber resilience governance can be conceptualized through five core and interrelated dimensions: Corporate Governance, Cyber Governance, Cyber Risk Management, Artificial Intelligence, and Continuous Learning. Rather than functioning as independent components, these dimensions form an integrated governance mechanism in which organizational oversight, cyber governance, risk-based decision-making, AI-enabled capabilities, and organizational learning mutually reinforce one another.

**Table 1**

*Core Dimensions of the Proposed Organizational Cyber Resilience Governance Framework*

| No. | Core Dimension | Primary Role in Cyber Resilience |
|---|---|---|
| 1 | Corporate Governance | Strategic oversight, accountability, policies, and decision-making |
| 2 | Cyber Governance | Direction, control, coordination, and oversight of cybersecurity |
| 3 | Cyber Risk Management | Identification, assessment, treatment, monitoring, and control of cyber risks |
| 4 | Artificial Intelligence | Threat prediction, anomaly detection, analysis, automation, and decision support |
| 5 | Continuous Learning | Organizational learning, adaptation, improvement, and knowledge development |

The first dimension, **Corporate Governance**, establishes the strategic foundation of cyber resilience. It determines organizational accountability, management commitment, policies, decision-making structures, and alignment between cybersecurity objectives and broader organizational goals. Effective corporate governance ensures that cyber resilience is treated as an enterprise-level concern rather than being limited to the information technology function.

The second dimension, **Cyber Governance**, translates organizational governance principles into cybersecurity-related direction and control. It provides mechanisms for establishing cybersecurity responsibilities, monitoring cyber capabilities, coordinating security activities, and ensuring that cybersecurity initiatives are aligned with organizational priorities. The integration of cyber governance with corporate governance strengthens accountability and facilitates coordinated responses to cyber-related risks.

The third dimension, **Cyber Risk Management**, provides a systematic mechanism for identifying and assessing cyber threats and vulnerabilities, determining their potential organizational impacts, selecting appropriate risk responses, and continuously monitoring the risk environment. This dimension connects cybersecurity activities with enterprise risk management and enables organizations to prioritize resources according to the significance and potential consequences of cyber risks.

The fourth dimension, **Artificial Intelligence**, represents an enabling technological capability within the framework. AI can enhance the organization's ability to analyze large volumes of security-related data, identify patterns and anomalies, predict emerging threats, support risk analysis, and improve the speed and quality of response. Nevertheless, AI should not be viewed merely as a technological solution. Its implementation requires appropriate governance, risk controls, transparency, accountability, and continuous monitoring to ensure that AI-related risks do not undermine organizational resilience.

The fifth dimension, **Continuous Learning**, ensures that cyber resilience evolves in response to changes in the threat environment, organizational experience, technological developments, and lessons learned from incidents. Continuous learning enables organizations to transform experience and knowledge into improvements in policies, controls, processes, capabilities, and decision-making mechanisms.

**Table 2**

*Contribution of the Five Dimensions to the Cyber Resilience Lifecycle*

| Main Supporting Dimensions | Cyber Resilience Capability |
|---|---|
| Artificial Intelligence; Cyber Risk Management | Prediction |
| Cyber Governance; Cyber Risk Management | Prevention |
| Artificial Intelligence; Cyber Governance | Detection |
| Cyber Governance; Cyber Risk Management; Artificial Intelligence | Response |
| Corporate Governance; Cyber Risk Management | Recovery |
| Continuous Learning; Corporate Governance; Artificial Intelligence | Adaptation |

The integrated interaction among these five dimensions strengthens the organization's capabilities across the complete cyber resilience lifecycle. AI contributes particularly to prediction and detection, while risk management supports prioritization and appropriate responses. Governance provides the organizational authority and coordination necessary for effective prevention, response, and recovery. Continuous learning then enables the organization to adapt its capabilities based on emerging threats and previous experiences.

The proposed framework therefore extends conventional cybersecurity models by positioning cyber resilience within a broader governance architecture. Its primary value lies not in treating AI, risk management, and governance as separate mechanisms, but in establishing systematic relationships among them. This integration can improve the organization's ability to anticipate threats, make risk-informed decisions, respond effectively to incidents, recover critical operations, and continuously adapt to a changing cyber environment.

## 4. CONCLUSION

This study developed and validated an integrated organizational cyber resilience governance framework based on artificial intelligence and risk management using an exploratory mixed-methods approach. The findings identified five core dimensions: Corporate Governance, Cyber Governance, Cyber Risk Management, Artificial Intelligence, and Continuous Learning. The results demonstrate that effective cyber resilience requires more than the implementation of technical security controls; it depends on the coordinated interaction of governance structures, risk management practices, AI-enabled capabilities, and organizational learning.

The proposed framework provides an integrated perspective for embedding cyber resilience within organizational and information technology governance. By connecting strategic governance with cyber risk management and AI capabilities, organizations can improve their capacity to predict, prevent, detect, respond to, recover from, and adapt to cyber threats. The framework can therefore serve as a conceptual and practical foundation for organizations seeking to strengthen cyber resilience and improve strategic decision-making under conditions of increasing cyber uncertainty and technological change.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# طراحی و اعتبارسنجی چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک: رویکردی آمیخته در حاکمیت فناوری اطلاعات[1]

**امیرحسین کافی*[2]، محمدعلی سلطانشاهی[3]، مجتبی رئیس صفری[4] و امیرمحمد کافی[5]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۲۶۳ - ۳۰۲

تاریخ دریافت: ۱۴۰۵/۰۵/۱۴
تاریخ بازنگری: ۱۴۰۵/۰۶/۲۳
تاریخ پذیرش: ۱۴۰۵/۰۷/۲۵

## چکیده

*با گسترش تحول دیجیتال و افزایش پیچیدگی تهدیدهای سایبری، سازمان‌ها برای حفظ تداوم کسب‌وکار و حفاظت از دارایی‌های اطلاعاتی، نیازمند رویکردهایی فراتر از کنترل‌های سنتی امنیت اطلاعات هستند. پژوهش حاضر با هدف طراحی چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک انجام شده است. این پژوهش از نظر هدف کاربردی و از نظر روش، آمیخته اکتشافی است. در مرحله کیفی، با مرور نظام‌مند منابع علمی منتشرشده طی سال‌های ۲۰۲۰ تا ۲۰۲۵، تحلیل استانداردها و چارچوب‌های شامل NIST CSF 2.0، NIST AI RMF، COBIT 2019، ISO/IEC 27001:2022، ISO 31000 و COSO ERM و نیز بهره‌گیری از روش دلفی با مشارکت خبرگان حوزه امنیت سایبری، مدیریت ریسک و حاکمیت فناوری اطلاعات، مؤلفه‌های چارچوب استخراج و پالایش شد. در مرحله کمی نیز اعتبار چارچوب پیشنهادی از طریق پرسشنامه محقق‌ساخته و مدل‌یابی معادلات ساختاری مبتنی بر حداقل مربعات جزئی مورد ارزیابی قرار گرفت. یافته‌های پژوهش نشان داد که چارچوب پیشنهادی از پنج بُعد اصلی شامل حاکمیت شرکتی، حاکمیت سایبری، مدیریت ریسک سایبری، هوش مصنوعی و یادگیری مستمر تشکیل شده است که تعامل نظام‌مند آن‌ها موجب ارتقای پیش‌بینی، پیشگیری، تشخیص، پاسخ، بازیابی و انطباق سازمان در برابر تهدیدهای سایبری می‌شود. نوآوری پژوهش در ارائه چارچوبی یکپارچه است که با تلفیق اصول حاکمیت شرکتی، مدیریت ریسک و قابلیت‌های هوش مصنوعی، زمینه افزایش تاب‌آوری سایبری و بهبود کیفیت تصمیم‌گیری راهبردی سازمان‌ها را فراهم می‌سازد.*

**واژه‌های کلیدی:** *حاکمیت تاب‌آوری سایبری، هوش مصنوعی، مدیریت ریسک سایبری، حاکمیت شرکتی، امنیت سایبری.*

**طبقه‌بندی موضوعی:** *M15, M14, D81, O33, L86.*

---

[1] https://doi.org/10.22034/JISTA.2026.595585.1093

[1] مقاله منتخب دومین همایش ملی حاکمیت شرکتی و مدیریت ریسک‌های فناوری اطلاعات

[2] دانشجوی دکتری فناوری اطلاعات، متخصص نوآوری فناورانه و راهبردهای بانکداری هوشمند، عضو باشگاه پژوهان بانک سپه، تهران، ایران. (نویسنده مسئول). (amirhkafi@gmail.com)

[3] دکتری فناوری اطلاعات، متخصص هوش مصنوعی و توسعه سامانه‌های هوشمند، عضو باشگاه پژوهان بانک سپه، تهران، ایران. (ali.soltanshahi@gmail.com)

[4] دکتری فناوری اطلاعات، متخصص تحول دیجیتال و حکمرانی هوشمند، عضو باشگاه پژوهان بانک سپه، تهران، ایران. (mgrd81@gmail.com)

[5] دانشجوی دکتری فناوری اطلاعات، متخصص فناوری‌های مالی و تحلیل سامانه‌های هوشمند، عضو هسته نوآوری اسکای، تهران، ایران (amirmkafi@gmail.com)

**مقدمه**

تحول دیجیتال در سال‌های اخیر، سازمان‌ها را با فرصت‌های بی‌سابقه‌ای در زمینه افزایش بهره‌وری، توسعه خدمات هوشمند و بهبود فرایندهای تصمیم‌گیری مواجه کرده است؛ بااین‌حال، همین تحول موجب گسترش سطح حملات سایبری، پیچیده‌تر شدن تهدیدها و افزایش وابستگی سازمان‌ها به زیرساخت‌های دیجیتال شده است. امروزه دارایی‌های اطلاعاتی، سامانه‌های عملیاتی، خدمات برخط و زنجیره‌های تأمین دیجیتال، بخش جدایی‌ناپذیر ارزش‌آفرینی سازمان‌ها محسوب می‌شوند و هرگونه اختلال در امنیت یا دسترس‌پذیری آن‌ها می‌تواند پیامدهای مالی، عملیاتی، حقوقی و اعتباری گسترده‌ای به همراه داشته باشد. بر همین اساس، امنیت سایبری دیگر صرفاً یک موضوع فنی تلقی نمی‌شود، بلکه به یکی از ارکان اساسی حاکمیت سازمانی، مدیریت ریسک و تداوم کسب‌وکار تبدیل شده است (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴؛ آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۱-۲۰).

بررسی گزارش‌های بین‌المللی نشان می‌دهد که در سال‌های اخیر، حملات باج‌افزاری، حملات زنجیره تأمین، سوءاستفاده از هوش مصنوعی مولد، حملات مبتنی بر مهندسی اجتماعی و تهدیدات پیشرفته مداوم، از مهم‌ترین چالش‌های محیط امنیت سایبری بوده‌اند. این تهدیدها تنها زیرساخت‌های فناوری اطلاعات را هدف قرار نمی‌دهند، بلکه توان عملیاتی، اعتبار سازمان، اعتماد ذی‌نفعان و استمرار ارائه خدمات حیاتی را نیز تحت تأثیر قرار می‌دهند (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱؛ آی‌بی‌ام، ۱۴۰۳: ۹-۱۷؛ مجمع جهانی اقتصاد، ۱۴۰۳: ۶ ، ۱۲). ازاین‌رو، رویکردهای سنتی امنیت اطلاعات که عمدتاً بر پیشگیری از نفوذ متمرکز بودند، به‌تنهایی پاسخگوی محیط پیچیده و پویای تهدیدات سایبری نیستند.

در چنین شرایطی، مفهوم تاب‌آوری سایبری[1] به‌عنوان رویکردی مکمل برای مدیریت امنیت سایبری مطرح شده است. برخلاف رویکردهای سنتی امنیت سایبری که تمرکز اصلی آن‌ها بر پیشگیری و حفاظت در برابر حملات است، تاب‌آوری سایبری بر توانایی سازمان برای آمادگی و پیش‌بینی، مقاومت در برابر اختلال، پاسخ‌گویی مؤثر، بازیابی سریع و انطباق با شرایط پس از وقوع حوادث سایبری تأکید دارد. از این منظر، هدف تاب‌آوری صرفاً جلوگیری از وقوع حادثه

[1] Cyber Resilience

نیست، بلکه حفظ و تداوم قابلیت‌های حیاتی سازمان در شرایط اختلال و بازگشت مؤثر به وضعیت عملیاتی مطلوب است (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱، ۱۵،۱۰؛ مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

در کنار توسعه مفهوم تاب‌آوری سایبری، حاکمیت سازمانی نیز طی سال‌های اخیر دستخوش تحول قابل‌توجهی شده است. در گذشته، مسئولیت امنیت اطلاعات عمدتاً بر عهده واحد فناوری اطلاعات قرار داشت؛ اما امروزه هیئت‌مدیره، کمیته‌های ریسک، مدیران ارشد و سایر ذی‌نفعان نقش مستقیمی در سیاست‌گذاری، نظارت و مدیریت ریسک‌های سایبری بر عهده دارند. چارچوب‌های نوین حاکمیت و مدیریت فناوری اطلاعات، نظیر کوبیت ۲۰۱۹[1]، و چارچوب‌های مدیریت ریسک سازمانی، نظیر مدل مدیریت ریسک سازمانی کوزو[2] و استاندارد ایزو ۳۱۰۰۰[3]، بر همسوسازی تصمیمات راهبردی، مدیریت ریسک و سازوکارهای کنترلی سازمان تأکید دارند (ایساکا، ۱۳۹۹: ۱۰؛ کمیته سازمان‌های حامی کمیسیون تردوی، ۱۳۹۷: ۱۰، ۱۴؛ سازمان بین‌المللی استانداردسازی، ۱۳۹۷: ۱۴).

از سوی دیگر، گسترش حجم داده‌ها، پیچیدگی تهدیدها و سرعت تغییرات محیط سایبری موجب شده است که تحلیل انسانی به‌تنهایی برای شناسایی و مدیریت تمامی مخاطرات کافی نباشد. در چنین شرایطی، هوش مصنوعی به‌عنوان یکی از فناوری‌های تحول‌آفرین، ظرفیت قابل‌توجهی برای ارتقای امنیت سایبری و افزایش تاب‌آوری سازمانی ایجاد کرده است. الگوریتم‌های یادگیری ماشین، یادگیری عمیق، تحلیل رفتار کاربران، پردازش زبان طبیعی و تحلیل کلان‌داده‌ها می‌توانند در شناسایی الگوهای غیرعادی، تشخیص تهدیدها، کاهش هشدارهای کاذب و پشتیبانی از فرایند تصمیم‌گیری در مدیریت ریسک مورد استفاده قرار گیرند (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱؛ مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

در مقابل، استفاده از هوش مصنوعی نیز با چالش‌هایی نظیر سوگیری الگوریتمی، حملات خصمانه علیه مدل‌های یادگیری ماشین، نبود شفافیت و تبیین‌پذیری در برخی تصمیمات هوشمند و مخاطرات حاکمیتی همراه است. به همین دلیل، در سال‌های اخیر مفهوم حاکمیت هوش

[1] COBIT 2019 (Control Objectives for Information and Related Technologies)
[2] COSO Enterprise Risk Management (COSO ERM)
[3] ISO 31000:2018 (Risk Management—Guidelines)

مصنوعی[1] نیز مورد توجه نهادهای بین‌المللی قرار گرفته است. در همین راستا، مؤسسه ملی استانداردها و فناوری ایالات متحده در سال ۲۰۲۳ چارچوب مدیریت ریسک هوش مصنوعی را با هدف ارائه رویکردی نظام‌مند برای شناسایی، ارزیابی و مدیریت ریسک‌های مرتبط با سامانه‌های هوش مصنوعی منتشر کرد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۴-۳). بنابراین، استفاده مؤثر از هوش مصنوعی در امنیت سایبری مستلزم استقرار سازوکارهای حاکمیتی، کنترل‌های مدیریتی و فرایندهای منسجم ارزیابی و مدیریت ریسک است.

اگرچه مطالعات متعددی در زمینه امنیت سایبری، مدیریت ریسک، حاکمیت فناوری اطلاعات، تاب‌آوری سایبری و کاربرد هوش مصنوعی انجام شده است، بررسی ادبیات پژوهش نشان می‌دهد که بخش قابل‌توجهی از این مطالعات هر یک بر یکی از ابعاد مسئله تمرکز داشته‌اند. برخی پژوهش‌ها بر کاربرد هوش مصنوعی در تشخیص و مدیریت تهدیدات سایبری تمرکز کرده‌اند، برخی دیگر چارچوب‌های مدیریت ریسک و بلوغ امنیت سایبری را بررسی کرده‌اند و گروهی نیز به حاکمیت و مدیریت فناوری اطلاعات پرداخته‌اند. بااین‌حال، همچنان نیاز به چارچوب‌های یکپارچه‌ای وجود دارد که بتوانند ارتباط میان حاکمیت سازمانی، مدیریت ریسک، هوش مصنوعی و تاب‌آوری سایبری را در سطح سازمانی تبیین کنند (مک‌اینتاش و همکاران، ۱۴۰۳: ۱۱، ۱۴؛ آلهیدایفی و همکاران، ۱۴۰۳: ۱۱).

این خلأ پژوهشی به‌ویژه در سازمان‌های بزرگ، بانک‌ها، شرکت‌های زیرساختی و نهادهای دولتی اهمیت بیشتری پیدا می‌کند؛ زیرا این سازمان‌ها علاوه بر تهدیدهای سایبری، با الزامات قانونی و مقرراتی، الزامات حاکمیت سازمانی، انتظارات ذی‌نفعان و ضرورت تداوم ارائه خدمات نیز مواجه هستند. در چنین سازمان‌هایی، اتخاذ تصمیمات امنیتی صرفاً بر اساس شاخص‌های فنی کافی نیست و لازم است ابعاد مدیریتی، راهبردی، اقتصادی و حاکمیتی نیز به‌صورت همزمان مورد توجه قرار گیرد (سازمان همکاری و توسعه اقتصادی، ۱۴۰۲؛ مجمع جهانی اقتصاد، ۱۴۰۳: ۶، ۱۲).

بر این اساس، مسئله اصلی پژوهش حاضر آن است که چگونه می‌توان با تلفیق اصول حاکمیت شرکتی، مدیریت ریسک و قابلیت‌های هوش مصنوعی، چارچوبی جامع برای افزایش تاب‌آوری سایبری سازمان طراحی کرد؛ چارچوبی که علاوه بر ارتقای توان پیشگیری، قابلیت

[1] AI Governance

شناسایی سریع تهدیدها، پشتیبانی از تصمیم‌گیری مدیریتی، پاسخ‌گویی هوشمند به حوادث، بازیابی سریع خدمات و یادگیری مستمر از رخدادهای امنیتی را نیز فراهم سازد.

هدف اصلی این پژوهش، طراحی و تبیین یک چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک است که بتواند تعامل میان ساختارهای حاکمیتی، فرآیندهای مدیریت ریسک، فناوری‌های هوش مصنوعی و قابلیت‌های تاب‌آوری سایبری را به‌صورت نظام‌مند تشریح کند. همچنین این پژوهش درصدد است مؤلفه‌های اصلی این چارچوب، روابط میان آن‌ها و نقش هر یک در ارتقای تاب‌آوری سازمانی را مشخص کرده و زمینه لازم برای ارزیابی و پیاده‌سازی آن در سازمان‌های ایرانی را فراهم آورد.

اهمیت این پژوهش از دو جنبه نظری و کاربردی قابل تبیین است. از منظر نظری، پژوهش حاضر با یکپارچه‌سازی مفاهیم حاکمیت شرکتی، مدیریت ریسک، هوش مصنوعی و تاب‌آوری سایبری، مدلی مفهومی ارائه می‌کند که می‌تواند مبنای توسعه پژوهش‌های آینده قرار گیرد. از منظر کاربردی نیز چارچوب پیشنهادی می‌تواند به مدیران ارشد، اعضای هیئت‌مدیره، مدیران امنیت اطلاعات، مدیران فناوری اطلاعات و مدیران ریسک در طراحی سیاست‌های امنیتی، تخصیص منابع، اولویت‌بندی مخاطرات و افزایش آمادگی سازمان در برابر تهدیدهای سایبری کمک کند.

در این پژوهش، حاکمیت تاب‌آوری سایبری به مجموعه‌ای از ساختارها، سیاست‌ها، فرآیندها و سازوکارهای مدیریتی اطلاق می‌شود که با بهره‌گیری از اصول حاکمیت شرکتی، مدیریت ریسک و فناوری‌های هوش مصنوعی، توان سازمان را در پیش‌بینی، پیشگیری، مقاومت، پاسخ‌گویی، بازیابی و انطباق در برابر تهدیدهای سایبری افزایش می‌دهد. همچنین هوش مصنوعی به سامانه‌هایی اطلاق می‌شود که با استفاده از الگوریتم‌های یادگیری ماشین، یادگیری عمیق، تحلیل داده و استنتاج هوشمند، قابلیت شناسایی الگوهای تهدید، پیش‌بینی مخاطرات، تحلیل رفتار، اولویت‌بندی هشدارها و پشتیبانی از تصمیم‌گیری مدیران را فراهم می‌کنند. در این پژوهش، مدیریت ریسک سایبری نیز به فرآیند نظام‌مند شناسایی، تحلیل، ارزیابی، پاسخ و پایش مستمر مخاطرات سایبری بر اساس چارچوب‌های بین‌المللی مدیریت ریسک اطلاق می‌شود.

در نهایت، ساختار مقاله در پنج بخش تنظیم شده است. پس از مقدمه، در بخش دوم مبانی نظری و توسعه فرضیه‌ها با مرور و تحلیل یکپارچه پژوهش‌های داخلی و خارجی ارائه می‌شود. در بخش سوم روش‌شناسی پژوهش و نحوه طراحی چارچوب پیشنهادی تشریح خواهد شد. بخش چهارم به ارائه یافته‌های پژوهش و چارچوب نهایی اختصاص دارد و در پایان، نتایج، کاربردهای مدیریتی، محدودیت‌ها و پیشنهادهای پژوهشی در قالب بحث و نتیجه‌گیری ارائه می‌شود.




**شکل ۱.** روند تکامل رویکردهای امنیت سازمانی تا حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی

## مبانی نظری و توسعه فرضیه‌ها

### حاکمیت شرکتی و حاکمیت سایبری

افزایش وابستگی سازمان‌ها به فناوری‌های دیجیتال موجب شده است که ریسک‌های سایبری از سطح مخاطرات عملیاتی فراتر رفته و به یکی از مهم‌ترین ریسک‌های راهبردی سازمان‌ها تبدیل شوند. در چنین شرایطی، حاکمیت شرکتی دیگر تنها بر نظارت مالی، رعایت مقررات و پاسخگویی مدیریتی متمرکز نیست، بلکه مدیریت ریسک‌های فناوری اطلاعات، امنیت سایبری و تاب‌آوری دیجیتال نیز به بخشی جدایی‌ناپذیر از مسئولیت‌های هیئت‌مدیره و مدیران ارشد تبدیل شده است (سازمان همکاری و توسعه اقتصادی، ۱۴۰۲).

مطابق تعریف سازمان همکاری و توسعه اقتصادی، حاکمیت شرکتی مجموعه‌ای از روابط میان هیئت‌مدیره، مدیران اجرایی، سهامداران و سایر ذی‌نفعان است که چارچوب لازم برای

تعیین اهداف سازمان، نحوه دستیابی به این اهداف و نظارت بر عملکرد را فراهم می‌کند (سازمان همکاری و توسعه اقتصادی، ۱۴۰۲). در این چارچوب، مدیریت ریسک‌های سایبری دیگر یک مسئولیت صرفاً فنی محسوب نمی‌شود، بلکه بخشی از نظام تصمیم‌گیری کلان سازمان است.

در سال‌های اخیر مفهوم حاکمیت سایبری[1] به‌عنوان توسعه‌ای از حاکمیت فناوری اطلاعات مطرح شده است. حاکمیت سایبری بر تعیین مسئولیت‌ها، سیاست‌گذاری امنیتی، تخصیص منابع، نظارت مستمر، مدیریت ریسک و ارزیابی عملکرد امنیت سایبری در سطح هیئت‌مدیره تأکید دارد نیز بیان می‌کند که ارزش‌آفرینی از فناوری اطلاعات تنها زمانی امکان‌پذیر است که میان اهداف کسب‌وکار، مدیریت ریسک، امنیت اطلاعات و کنترل‌های حاکمیتی هماهنگی وجود داشته باشد (ایساکا، ۱۳۹۹).

مطالعات جدید نشان می‌دهد سازمان‌هایی که هیئت‌مدیره آن‌ها دارای کمیته تخصصی امنیت سایبری هستند، در مدیریت رخدادهای امنیتی، بازیابی خدمات و کاهش خسارات مالی عملکرد بهتری نسبت به سایر سازمان‌ها دارند (دیلویت، ۱۴۰۳).

## تاب‌آوری سایبری

مفهوم تاب‌آوری سایبری طی یک دهه گذشته به یکی از مهم‌ترین موضوعات پژوهش‌های امنیت اطلاعات تبدیل شده است. برخلاف رویکرد سنتی امنیت سایبری که هدف اصلی آن جلوگیری از وقوع حملات است، تاب‌آوری سایبری بر این فرض استوار است که هیچ سامانه‌ای مصون از نفوذ نیست و سازمان باید حتی در صورت موفقیت مهاجم نیز قادر به ادامه فعالیت‌های حیاتی خود باشد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

چارچوب جدید چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ایالات متحده ۲.۰[2] تاب‌آوری سایبری را مجموعه‌ای از قابلیت‌های سازمان در پنج مرحله اصلی معرفی می‌کند:

- شناسایی
- حفاظت
- کشف

[1] Cyber Governance
[2] National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0

- پاسخ
- بازیابی

در نسخه جدید این چارچوب، مؤلفه حاکمیت نیز به‌عنوان لایه راهبری به مدل اضافه شده است که نقش حاکمیت سازمانی را در امنیت سایبری برجسته می‌کند (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

از دیدگاه از دیدگاه استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲[1] نیز تاب‌آوری سایبری تنها با استقرار کنترل‌های امنیتی حاصل نمی‌شود، بلکه نیازمند مدیریت مستمر ریسک، بهبود فرآیندها، آموزش کارکنان، ارزیابی تهدیدها و آمادگی برای بازیابی است (سازمان بین‌المللی استانداردسازی، ۱۳۹۷: ۱۴).

در پژوهش‌های مرتبط با تاب‌آوری سایبری نیز بر ضرورت نگاه یکپارچه به امنیت، مدیریت ریسک و قابلیت‌های سازمانی تأکید شده است. در این چارچوب، تاب‌آوری سایبری را می‌توان به‌عنوان توانایی سازمان یا سامانه برای آمادگی در برابر تهدیدها، مقاومت در برابر اختلالات، پاسخ‌گویی مؤثر، بازیابی قابلیت‌های حیاتی و انطباق با شرایط پس از وقوع حادثه در نظر گرفت. همچنین، پژوهش‌های حوزه حاکمیت فناوری اطلاعات نشان می‌دهند که افزایش بلوغ سازوکارهای حاکمیتی می‌تواند به بهبود قابلیت سازمان در مدیریت ریسک‌های فناوری و افزایش ظرفیت پاسخ‌گویی و بازیابی در برابر اختلالات سایبری کمک کند (مک‌اینتاش و همکاران، ۱۴۰۳: ۱۱، ۱۴؛ آلهیدایفی و همکاران، ۱۴۰۳: ۱۱).

همچنین شارما[2] و همکاران (۲۰۲۳) بیان کردند که سازمان‌های دارای بلوغ بالاتر در حاکمیت فناوری اطلاعات، زمان بازیابی خدمات[3] را به‌طور معناداری کاهش داده‌اند.

## مدیریت ریسک سایبری

مدیریت ریسک یکی از ارکان اصلی تاب‌آوری سازمانی است. مطابق استاندارد ایزو ۳۱۰۰۰:۲۰۱۸[4]، مدیریت ریسک فرآیندی نظام‌مند برای شناسایی، تحلیل، ارزیابی، پاسخ و

[1] ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[2] Sharma
[3] Recovery Time Objective
[4] ISO 31000:2018 — Risk management — Guidelines

پایش ریسک‌ها است که باید در تمام سطوح سازمان جاری باشد (سازمان بین‌المللی استانداردسازی، ۱۳۹۷: ۱۴). اگرچه این استاندارد پیش از سال ۲۰۲۰ منتشر شده است، اما همچنان معتبرترین مرجع جهانی مدیریت ریسک بوده و در پژوهش‌های جدید نیز به‌طور گسترده مورد استناد قرار می‌گیرد.

در حوزه امنیت سایبری، مدیریت ریسک به فرآیند شناسایی دارایی‌های حیاتی، تهدیدها، آسیب‌پذیری‌ها، احتمال وقوع رخداد و میزان اثر آن بر اهداف سازمان اشاره دارد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

چارچوب مدیریت ریسک سازمانی کمیته سازمان‌های حامی کمیسیون تردوی[1] نیز بر یکپارچگی میان تصمیمات راهبردی، کنترل‌های داخلی، مدیریت ریسک و حاکمیت شرکتی تأکید دارد و معتقد است ریسک‌های سایبری باید همانند سایر ریسک‌های راهبردی در سطح هیئت‌مدیره مدیریت شوند (کمیته سازمان‌های حامی کمیسیون تردوی، ۱۳۹۷: ۱۰، ۱۴).

گزارش شرکت آی‌بی‌ام[2] در سال ۲۰۲۴ می‌دهد میانگین هزینه هر رخداد نشت اطلاعات در سال ۲۰۲۴ به بیش از ۸/۴ میلیون دلار رسیده است. همچنین سازمان‌هایی که از سامانه‌های هوشمند تشخیص تهدید و مدیریت ریسک استفاده می‌کنند، زمان شناسایی حمله را به‌طور متوسط بیش از ۳۰ درصد کاهش داده‌اند (آی‌بی‌ام، ۱۴۰۳: ۹-۱۷).

ازاین‌رو، مدیریت ریسک دیگر صرفاً ابزاری برای کاهش احتمال وقوع تهدید نیست، بلکه سازوکاری برای افزایش تاب‌آوری و تضمین تداوم خدمات سازمانی محسوب می‌شود.

## هوش مصنوعی در امنیت سایبری

رشد سریع حجم داده‌های امنیتی و پیچیدگی حملات سایبری موجب شده است که روش‌های سنتی تحلیل داده دیگر پاسخگوی نیاز سازمان‌ها نباشند. در چنین شرایطی، هوش مصنوعی به یکی از فناوری‌های کلیدی امنیت سایبری تبدیل شده است.

مطابق گزارش آژانس اتحادیه اروپا برای امنیت سایبری[3] در سال ۲۰۲۳، مهم‌ترین کاربردهای هوش مصنوعی در امنیت سایبری عبارت‌اند از:

[1] COSO Enterprise Risk Management (COSO ERM)
[2] IBM
[3] European Union Agency for Cybersecurity (ENISA)

- تشخیص ناهنجاری‌های رفتاری
- تحلیل ترافیک شبکه
- شناسایی بدافزارهای ناشناخته
- کشف حملات روز صفر[1]
- اولویت‌بندی هشدارهای امنیتی
- تحلیل رفتار کاربران
- پیش‌بینی تهدیدها

الگوریتم‌های یادگیری ماشین قادرند میلیون‌ها رویداد امنیتی را در مدت کوتاهی تحلیل کرده و الگوهایی را شناسایی کنند که برای تحلیل‌گران انسانی قابل مشاهده نیست.

علاوه بر این، هوش مصنوعی مولد نیز در سال‌های اخیر وارد حوزه امنیت سایبری شده است. این فناوری می‌تواند در تولید خودکار گزارش‌های امنیتی، تحلیل رخدادها، پاسخ‌گویی به حوادث و تولید سناریوهای حمله مورد استفاده قرار گیرد؛ هرچند همین فناوری می‌تواند توسط مهاجمان نیز برای طراحی حملات پیچیده‌تر مورد سوءاستفاده قرار گیرد (مجمع جهانی اقتصاد، ۱۴۰۳: ۶ ، ۱۲).

به همین دلیل، مؤسسه مؤسسه ملی استانداردها و فناوری در سال ۲۰۲۳ چارچوب چارچوب مدیریت ریسک هوش مصنوعی[2] را منتشر کرد که هدف آن مدیریت ریسک‌های مرتبط با سامانه‌های هوش مصنوعی از منظر اعتمادپذیری، شفافیت، عدالت، امنیت و پاسخگویی است (مؤسسه ملی استانداردها و فناوری، ۱۴۰۲: ۱۲).

[1] Zero-Day
[2] NIST Artificial Intelligence Risk Management Framework (AI RMF)

**جدول ۱**

*مقایسه رویکردهای سنتی امنیت سایبری با رویکرد حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی*

| شاخص | امنیت سایبری سنتی | حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی |
|---|---|---|
| هدف اصلی | جلوگیری از نفوذ | حفظ تداوم کسب‌وکار در زمان حمله |
| مسئول اصلی | واحد فناوری اطلاعات | هیئت‌مدیره، مدیران ارشد و واحدهای تخصصی |
| تصمیم‌گیری | واکنشی | پیش‌بینانه و هوشمند |
| تحلیل داده | دستی و مبتنی بر قوانین | یادگیری ماشین و تحلیل بلادرنگ |
| مدیریت ریسک | دوره‌ای | مستمر و پویا |
| پاسخ به رخداد | پس از وقوع | پیش‌بینی، پاسخ خودکار و بازیابی هوشمند |
| یادگیری | محدود | یادگیری مستمر مبتنی بر داده |

## تحلیل یکپارچه پژوهش‌های پیشین

مرور پژوهش‌های انجام‌شده در سال‌های اخیر نشان می‌دهد که اگرچه ادبیات پژوهش در حوزه امنیت سایبری، مدیریت ریسک، حاکمیت فناوری اطلاعات و هوش مصنوعی به‌طور مستقل توسعه قابل‌توجهی یافته است، اما هنوز یک چارچوب جامع که این چهار حوزه را به‌صورت یکپارچه و از منظر حاکمیت سازمانی تلفیق کند، کمتر ارائه شده است. بخش عمده‌ای از مطالعات بر توسعه الگوریتم‌های هوش مصنوعی برای تشخیص نفوذ، شناسایی بدافزار یا تحلیل رفتار کاربران متمرکز بوده‌اند، در حالی که ابعاد مدیریتی، نقش هیئت‌مدیره، فرآیندهای

تصمیم‌گیری راهبردی و تعامل میان هوش مصنوعی و مدیریت ریسک کمتر مورد توجه قرار گرفته است (کور، اسلام و رضاق، ۲۰۲۲: ۷؛ شارما، ۲۰۲۳: ۹).

در پژوهش‌های داخلی نیز تمرکز عمدتاً بر ارزیابی بلوغ امنیت اطلاعات، مدیریت ریسک فناوری اطلاعات یا پیاده‌سازی استانداردهایی نظیر ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲ بوده و کمتر پژوهشی به طراحی چارچوبی یکپارچه برای حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی پرداخته است. این خلأ پژوهشی، ضرورت توسعه مدلی بومی و در عین حال منطبق با استانداردهای بین‌المللی را برجسته می‌سازد. بر همین اساس، پژوهش حاضر با تلفیق چارچوب‌های امنیت سایبری مؤسسه ملی استانداردها و فناوری ایالات متحده ۲.۰، چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری، اهداف حاکمیت و مدیریت فناوری اطلاعات ۲۰۱۹، استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲ و استاندارد ایزو ۳۱۰۰۰:۲۰۱۸ در پی ارائه یک چارچوب حاکمیتی جامع است که بتواند نقش هوش مصنوعی را در تمامی مراحل چرخه مدیریت ریسک و ارتقای تاب‌آوری سایبری تبیین کند.

## توسعه چارچوب مفهومی پژوهش

با توجه به مبانی نظری ارائه‌شده، بررسی پژوهش‌های پیشین و تحلیل استانداردهای بین‌المللی، می‌توان دریافت که هیچ‌یک از چارچوب‌های موجود به‌تنهایی قادر به پوشش هم‌زمان ابعاد حاکمیت شرکتی، مدیریت ریسک سایبری، هوش مصنوعی و تاب‌آوری سازمانی نیستند. برای نمونه، چارچوب چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ایالات متحده ۲.۰ بر چرخه مدیریت امنیت سایبری و حاکمیت تمرکز دارد، اما به نحوه بهره‌گیری از هوش مصنوعی در تصمیم‌گیری مدیریتی نمی‌پردازد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴). همچنین چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری بر مدیریت ریسک سامانه‌های هوش مصنوعی متمرکز است و ارتباط مستقیمی با فرآیندهای حاکمیت سایبری سازمانی ارائه نمی‌کند. از سوی دیگر، چارچوب کوبیت ۲۰۱۹[1] سازوکارهای حاکمیتی فناوری اطلاعات را تبیین می‌کند، اما معماری عملیاتی مشخصی برای افزایش تاب‌آوری سایبری مبتنی بر هوش مصنوعی پیشنهاد نمی‌دهد (انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی، ۱۳۹۸: ۱۰، ۱۳، ۱۷).

[1] COBIT 2019

بر همین اساس، پژوهش حاضر با تلفیق نقاط قوت این چارچوب‌ها، مدلی مفهومی برای حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک ارائه می‌کند. در این مدل، تاب‌آوری سایبری نتیجه تعامل پویا میان پنج مؤلفه اصلی است:

- حاکمیت شرکتی
- حاکمیت سایبری
- مدیریت ریسک سایبری
- هوش مصنوعی
- بهبود مستمر و یادگیری سازمانی

در چارچوب پیشنهادی، حاکمیت شرکتی به‌عنوان لایه راهبردی، سیاست‌ها، اهداف، حدود مسئولیت‌ها و میزان ریسک‌پذیری سازمان را تعیین می‌کند. در سطح بعد، حاکمیت سایبری وظیفه تبدیل سیاست‌های کلان به سازوکارهای اجرایی، کنترل‌های امنیتی، پایش عملکرد و تخصیص منابع را بر عهده دارد. این لایه، ارتباط میان هیئت‌مدیره، مدیران ارشد، مدیران فناوری اطلاعات و واحدهای امنیت اطلاعات را برقرار می‌کند.

در ادامه، مدیریت ریسک سایبری به‌عنوان هسته تصمیم‌گیری عمل می‌کند و با شناسایی دارایی‌های حیاتی، تحلیل تهدیدها، ارزیابی آسیب‌پذیری‌ها، تعیین احتمال وقوع و برآورد پیامدهای حملات، اولویت‌های امنیتی سازمان را مشخص می‌سازد. داده‌های حاصل از این فرآیند به موتور هوش مصنوعی منتقل می‌شود تا تحلیل‌های پیشرفته و پیش‌بینی‌های لازم انجام گیرد.

در این چارچوب، هوش مصنوعی صرفاً ابزار تشخیص نفوذ نیست، بلکه نقش یک سامانه تصمیم‌یار مدیریتی را ایفا می‌کند. این سامانه با استفاده از الگوریتم‌های یادگیری ماشین، یادگیری عمیق و تحلیل داده‌های بلادرنگ، الگوهای تهدید را شناسایی کرده، احتمال وقوع رخدادهای امنیتی را پیش‌بینی می‌کند، هشدارها را اولویت‌بندی کرده و سناریوهای پاسخ مناسب را پیشنهاد می‌دهد. همچنین خروجی‌های این سامانه می‌تواند مبنای تصمیم‌گیری مدیران در تخصیص منابع، اصلاح سیاست‌ها و بازنگری کنترل‌های امنیتی قرار گیرد (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱؛ مایکروسافت، ۱۴۰۳: ۸۱).

ویژگی متمایز چارچوب پیشنهادی، وجود چرخه بازخورد و یادگیری مستمر است. برخلاف مدل‌های خطی مدیریت ریسک، در این پژوهش نتایج حاصل از هر رخداد سایبری، داده‌های جدیدی برای آموزش مجدد مدل‌های هوش مصنوعی و بهبود سیاست‌های حاکمیتی فراهم می‌کند. به این ترتیب، چارچوب پیشنهادی از یک سامانه ایستا به یک سامانه یادگیرنده و تطبیق‌پذیر تبدیل می‌شود که می‌تواند همگام با تغییرات محیط تهدید تکامل یابد. این ویژگی با مفهوم «تاب‌آوری پویا» همسو است که در پژوهش‌های جدید به‌عنوان یکی از شاخص‌های بلوغ امنیت سایبری مطرح شده است (مجمع جهانی اقتصاد، ۱۴۰۳: ۱۸).

از منظر مدیریتی، چارچوب پیشنهادی سه مزیت اساسی دارد. نخست، ارتباط مستقیم میان تصمیمات هیئت‌مدیره و شاخص‌های عملیاتی امنیت سایبری را برقرار می‌کند. دوم، استفاده از هوش مصنوعی موجب افزایش سرعت و دقت تحلیل ریسک و کاهش زمان کشف و پاسخ به رخدادها می‌شود. سوم، با ایجاد چرخه یادگیری مستمر، زمینه بهبود مداوم سطح تاب‌آوری سازمان را فراهم می‌سازد. این سه ویژگی سبب می‌شود چارچوب پیشنهادی علاوه بر سازمان‌های تجاری، برای بانک‌ها، شرکت‌های زیرساختی، سازمان‌های دولتی و ارائه‌دهندگان خدمات حیاتی نیز قابل استفاده باشد.




**شکل ۲.** چارچوب پیشنهادی حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک

## فرضیه‌های پژوهش

با توجه به مدل مفهومی پژوهش و مبانی نظری ارائه‌شده، فرضیه‌های زیر تدوین می‌شوند:

**فرضیه ۱.** حاکمیت شرکتی اثر مثبت و معناداری بر استقرار حاکمیت سایبری در سازمان دارد.

**فرضیه ۲.** حاکمیت سایبری اثر مثبت و معناداری بر اثربخشی مدیریت ریسک سایبری دارد.

**فرضیه ۳.** مدیریت ریسک سایبری اثر مثبت و معناداری بر به‌کارگیری هوش مصنوعی در تصمیم‌گیری‌های امنیتی دارد.

**فرضیه ٤.** به‌کارگیری هوش مصنوعی اثر مثبت و معناداری بر افزایش تاب‌آوری سایبری سازمان دارد.

**فرضیه ۵.** مدیریت ریسک سایبری به‌صورت مستقیم بر تاب‌آوری سایبری سازمان اثر مثبت و معناداری دارد.

**فرضیه ٦.** هوش مصنوعی نقش میانجی در رابطه بین مدیریت ریسک سایبری و تاب‌آوری سایبری سازمان ایفا می‌کند.

**فرضیه ۷.** حاکمیت سایبری نقش میانجی در رابطه بین حاکمیت شرکتی و مدیریت ریسک سایبری ایفا می‌کند.

بر اساس مبانی نظری و چارچوب مفهومی ارائه‌شده، پژوهش حاضر استدلال می‌کند که دستیابی به تاب‌آوری سایبری پایدار صرفاً از طریق استقرار کنترل‌های امنیتی امکان‌پذیر نیست، بلکه مستلزم یکپارچه‌سازی حاکمیت شرکتی، مدیریت ریسک و هوش مصنوعی در قالب یک نظام تصمیم‌گیری هوشمند است. چارچوب پیشنهادی با ایجاد پیوند میان این مؤلفه‌ها، نه‌تنها قابلیت پیش‌بینی و پاسخ‌گویی به تهدیدهای سایبری را ارتقا می‌دهد، بلکه از طریق چرخه بازخورد و یادگیری مستمر، زمینه بهبود مستمر تاب‌آوری سازمان را نیز فراهم می‌سازد.

## روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، کاربردی و از نظر شیوه اجرا، آمیخته اکتشافی است. در این رویکرد، ابتدا با بهره‌گیری از مطالعات کتابخانه‌ای، مرور نظام‌مند ادبیات و اخذ نظر خبرگان، چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک طراحی شد و سپس در مرحله کمی، اعتبار و روابط میان مؤلفه‌های چارچوب از طریق مدل‌یابی معادلات ساختاری مورد ارزیابی قرار گرفت.

استفاده از روش آمیخته به این دلیل انتخاب شد که طراحی یک چارچوب مفهومی، علاوه بر پشتوانه نظری، نیازمند بهره‌گیری از تجربیات متخصصان و ارزیابی تجربی روابط میان سازه‌ها است. این رویکرد در پژوهش‌های طراحی مدل و چارچوب‌های مدیریتی به‌طور گسترده مورد استفاده قرار گرفته و امکان افزایش اعتبار علمی یافته‌ها را فراهم می‌کند (کرسول و پلانو کلارک، ۲۰۲۱: ۲۰).

## مرحله کیفی پژوهش

در بخش کیفی، ابتدا مرور نظام‌مند منابع علمی منتشرشده بین سال‌های ۲۰۲۰ تا ۲۰۲۵ انجام شد. منابع مورد بررسی شامل مقالات نمایه‌شده در پایگاه‌های اسکوپوس[1]، وب آو ساینس[2]، آی‌تریپل‌ایکسپلور[3]، اشپرینگر[4]، ساینس‌دایرکت[5] و کتابخانه دیجیتال ای‌سی‌ام[6] بودند. همچنین استانداردها و چارچوب‌های معتبر بین‌المللی شامل چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ۲.۰، چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری، اهداف حاکمیت و مدیریت فناوری اطلاعات ۲۰۱۹، استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲، استاندارد ایزو ۳۱۰۰۰ و مدیریت ریسک سازمانی کمیته سازمان‌های حامی کمیسیون تردوی نیز تحلیل شدند.

پس از استخراج مؤلفه‌های اولیه، چارچوب پیشنهادی با استفاده از روش دلفی مورد ارزیابی قرار گرفت. جامعه خبرگان شامل استادان دانشگاه در حوزه امنیت اطلاعات، مدیران ارشد فناوری اطلاعات، مدیران امنیت اطلاعات، متخصصان مدیریت ریسک و مشاوران حاکمیت فناوری اطلاعات بود.

نمونه‌گیری در این مرحله به‌صورت هدفمند انجام شد و تعداد ۱۸ نفر از خبرگان که حداقل دارای مدرک کارشناسی ارشد، بیش از ده سال سابقه حرفه‌ای و تجربه عملی در حوزه امنیت سایبری یا مدیریت ریسک بودند، در پژوهش مشارکت کردند.

فرآیند دلفی طی سه دور انجام شد. در دور نخست، خبرگان درباره مؤلفه‌های پیشنهادی اظهار نظر کردند. در دور دوم، پیشنهادهای اصلاحی بررسی و چارچوب بازنگری شد. در دور سوم، میزان

[1] Scopus
[2] Web of Science
[3] IEEE Xplore
[4] Springer
[5] ScienceDirect
[6] ACM Digital Library

توافق خبرگان درباره هر مؤلفه اندازه‌گیری شد و تنها مؤلفه‌هایی که میانگین امتیاز آن‌ها بیش از ۴ از ۵ بود در مدل نهایی باقی ماندند.

## مرحله کمی پژوهش

در مرحله کمی، مدل مفهومی استخراج‌شده از مرحله کیفی از طریق پرسشنامه استاندارد محقق‌ساخته مورد ارزیابی قرار گرفت.

جامعه آماری شامل مدیران فناوری اطلاعات، مدیران امنیت اطلاعات، مدیران ریسک، کارشناسان امنیت سایبری و مدیران تحول دیجیتال سازمان‌های بزرگ، بانک‌ها، شرکت‌های بیمه، اپراتورهای مخابراتی و سازمان‌های دولتی ایران بود.

با توجه به تعداد متغیرهای پژوهش و استفاده از مدل‌یابی معادلات ساختاری، حجم نمونه بر اساس روش هیر و همکاران[1] در سال ۱۴۰۳ حداقل ۲۰۰ نفر تعیین شد. در نهایت ۲۲۸ پرسشنامه جمع‌آوری شد که پس از حذف پرسشنامه‌های ناقص، ۲۱۲ پرسشنامه برای تحلیل نهایی مورد استفاده قرار گرفت.

نمونه‌گیری به روش در دسترس همراه با قضاوتی انجام شد؛ زیرا جامعه متخصصان امنیت سایبری جامعه‌ای تخصصی و محدود است.

### جدول ۲

*مقایسه مشخصات جامعه آماری و نمونه پژوهش*

| مرحله پژوهش | جامعه آماری | روش نمونه‌گیری | حجم نمونه |
|---|---|---|---|
| کیفی | خبرگان امنیت سایبری، مدیریت ریسک و حاکمیت فناوری اطلاعات | هدفمند | ۱۸ نفر |
| کمی | مدیران و کارشناسان امنیت اطلاعات، فناوری اطلاعات و مدیریت ریسک | در دسترس و قضاوتی | ۲۱۲ نفر |

[1] Hair et al

### ابزار گردآوری داده‌ها

در مرحله کیفی، ابزار گردآوری اطلاعات شامل چک‌لیست استخراج مفاهیم از ادبیات پژوهش و پرسشنامه دلفی بود.

در مرحله کمی، پرسشنامه‌ای محقق‌ساخته بر اساس مؤلفه‌های استخراج‌شده طراحی شد. پرسشنامه شامل دو بخش بود:

- اطلاعات جمعیت‌شناختی پاسخ‌دهندگان
- گویه‌های مربوط به سازه‌های پژوهش

پاسخ‌ها بر اساس طیف پنج‌درجه‌ای لیکرت از «کاملاً مخالفم» تا «کاملاً موافقم» اندازه‌گیری شدند.

سازه‌های اصلی پرسشنامه عبارت بودند از:

- حاکمیت شرکتی
- حاکمیت سایبری
- مدیریت ریسک سایبری
- هوش مصنوعی
- تاب‌آوری سایبری

در مجموع ۳۴ گویه برای اندازه‌گیری متغیرهای پژوهش طراحی شد.

### روایی و پایایی ابزار پژوهش

برای ارزیابی روایی محتوا، پرسشنامه در اختیار خبرگان قرار گرفت و پس از اعمال اصلاحات لازم، نسخه نهایی تهیه شد.

در مرحله کمی، روایی همگرا با استفاده از میانگین واریانس استخراج‌شده[1] و روایی واگرا با معیار فورنل و لارکر و نسبت هتروتریت ـ مونوتریت[2] بررسی شد.

پایایی ابزار نیز از طریق شاخص‌های زیر اندازه‌گیری شد:

- آلفای کرونباخ
- پایایی ترکیبی

[1] Average Variance Extracted (AVE)
[2] Heterotrait–Monotrait Ratio (HTMT)

- شاخص rho_A

مطابق معیارهای هیر و همکاران، مقادیر آلفای کرونباخ و پایایی ترکیبی بزرگ‌تر از ۰/۷ و مقدار میانگین بزرگ‌تر از ۰/۵ نشان‌دهنده مطلوب بودن ابزار اندازه‌گیری است.

## روش تجزیه و تحلیل داده‌ها

داده‌های جمع‌آوری‌شده در دو سطح توصیفی و استنباطی تحلیل شدند.

در بخش توصیفی از شاخص‌هایی مانند فراوانی، درصد، میانگین و انحراف معیار استفاده شد.

در بخش استنباطی، برای آزمون مدل مفهومی پژوهش از مدل‌یابی معادلات ساختاری مبتنی بر حداقل مربعات جزئی[1] استفاده شد.

تحلیل مدل در دو مرحله انجام شد:

۱. ارزیابی مدل اندازه‌گیری شامل:

- پایایی
- روایی همگرا
- روایی واگرا

۲. ارزیابی مدل ساختاری شامل:

- ضرایب مسیر
- آماره t
- مقدار p
- ضریب تعیین ($R^2$)
- اندازه اثر ($f^2$)
- شاخص پیش‌بینی ($Q^2$)

برای تحلیل داده‌ها از نرم‌افزارهای اس‌پی‌اس‌اس[2] نسخه ۲۷ و نرم‌افزار اسمارت‌پی‌ال‌اس[3] نسخه ۴ استفاده شد.

---

[1] Partial Least Squares Structural Equation Modeling
[2] SPSS
[3] SmartPLS

## متغیرهای پژوهش و تعریف عملیاتی آن‌ها

در پژوهش حاضر، تاب‌آوری سایبری سازمانی به‌عنوان متغیر وابسته در نظر گرفته شد و میزان توانایی سازمان در پیش‌بینی، مقاومت، پاسخ، بازیابی و یادگیری از رخدادهای سایبری را اندازه‌گیری می‌کند.

هوش مصنوعی و مدیریت ریسک سایبری به‌عنوان متغیرهای مستقل اصلی تعریف شدند و میزان استفاده سازمان از فناوری‌های هوشمند در شناسایی تهدیدها، تحلیل ریسک و تصمیم‌گیری امنیتی را می‌سنجند.

حاکمیت شرکتی و حاکمیت سایبری نیز به‌عنوان سازه‌های راهبردی مدل در نظر گرفته شدند که نقش آن‌ها در ایجاد ساختارهای تصمیم‌گیری، سیاست‌گذاری و نظارت بر امنیت سایبری ارزیابی می‌شود.

## یافته‌های پژوهش

### استخراج و پالایش مؤلفه‌های چارچوب پیشنهادی

در مرحله نخست پژوهش، با مرور نظام‌مند منابع علمی منتشرشده بین سال‌های ۲۰۲۰ تا ۲۰۲۵ و تحلیل چارچوب‌های معتبر بین‌المللی شامل چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ۲.۰، چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری، اهداف حاکمیت و مدیریت فناوری اطلاعات ۲۰۱۹، استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲، استاندارد ایزو ۳۱۰۰۰ و مدیریت ریسک سازمانی کمیته سازمان‌های حامی کمیسیون تردوی، مجموعه‌ای از مؤلفه‌های اولیه مرتبط با حاکمیت تاب‌آوری سایبری استخراج شد. این مؤلفه‌ها پس از حذف موارد تکراری و ادغام مفاهیم مشابه، در قالب پنج بُعد اصلی و بیست‌ویک مؤلفه فرعی سازمان‌دهی شدند.

در ادامه، مؤلفه‌های استخراج‌شده در اختیار خبرگان قرار گرفت و طی سه دور اجرای روش دلفی، میزان اهمیت، شفافیت مفهومی، قابلیت اجرا و ارتباط هر مؤلفه با هدف پژوهش ارزیابی شد. نتایج این مرحله نشان داد که تمامی ابعاد اصلی چارچوب از نظر خبرگان دارای اهمیت بالا بوده و میانگین امتیاز آن‌ها از حد آستانه تعیین‌شده فراتر است. همچنین برخی مؤلفه‌ها با نظر خبرگان ادغام یا بازتعریف شدند تا از همپوشانی مفهومی جلوگیری شود.

فرآیند پالایش نشان داد که تاب‌آوری سایبری تنها حاصل استقرار کنترل‌های امنیتی نیست، بلکه پیامد تعامل نظام‌مند میان ساختارهای حاکمیتی، فرآیندهای مدیریت ریسک، فناوری‌های هوش مصنوعی و سازوکارهای یادگیری سازمانی است. این یافته با نتایج پژوهش‌های اخیر در حوزه حاکمیت سایبری و مدیریت ریسک همسو است که بر ضرورت نگاه فرابخشی به امنیت سایبری تأکید دارند.

**ابعاد اصلی چارچوب حاکمیت تاب‌آوری سایبری**

بر اساس تحلیل داده‌های کیفی، چارچوب پیشنهادی از پنج بُعد اصلی تشکیل شده است که هر یک نقش مشخصی در ارتقای تاب‌آوری سایبری سازمان ایفا می‌کنند.

حاکمیت شرکتی به‌عنوان لایه راهبردی، مسئول تعیین سیاست‌های کلان، میزان ریسک‌پذیری، تخصیص منابع و نظارت بر عملکرد امنیت سایبری است. در این سطح، هیئت‌مدیره و کمیته‌های تخصصی مسئولیت اصلی هدایت و پایش ریسک‌های سایبری را بر عهده دارند.

حاکمیت سایبری لایه‌ای است که سیاست‌های کلان را به فرآیندهای اجرایی تبدیل می‌کند. این بُعد شامل مدیریت کنترل‌های امنیتی، پایش انطباق، مدیریت دارایی‌های اطلاعاتی، تعیین مسئولیت‌ها و نظارت بر اجرای الزامات امنیتی است.

مدیریت ریسک سایبری هسته تصمیم‌گیری چارچوب محسوب می‌شود. در این بخش، دارایی‌های حیاتی، تهدیدها، آسیب‌پذیری‌ها و پیامدهای بالقوه شناسایی و ارزیابی شده و اولویت اقدامات امنیتی مشخص می‌شود.

هوش مصنوعی نقش تصمیم‌یار را در چارچوب پیشنهادی ایفا می‌کند. سامانه‌های هوشمند با تحلیل داده‌های امنیتی، شناسایی الگوهای غیرعادی، پیش‌بینی حملات، اولویت‌بندی هشدارها و ارائه پیشنهادهای تصمیم‌گیری، سرعت و دقت مدیریت ریسک را افزایش می‌دهند.

در نهایت، یادگیری مستمر و بهبود مداوم به‌عنوان مؤلفه‌ای میان‌بخشی، نتایج حاصل از رخدادهای امنیتی، تحلیل‌های هوش مصنوعی و بازخوردهای مدیریتی را به چرخه حاکمیت بازمی‌گرداند تا سیاست‌ها، کنترل‌ها و مدل‌های تحلیلی به‌صورت مستمر بهبود یابند.

**جدول ۳**

*ابعاد و مؤلفه‌های چارچوب پیشنهادی حاکمیت تاب‌آوری سایبری*

| بُعد اصلی | مؤلفه‌های کلیدی | نقش در چارچوب |
|---|---|---|
| حاکمیت شرکتی | سیاست‌گذاری، راهبری، نظارت، تعیین ریسک‌پذیری | تعیین جهت‌گیری راهبردی |
| حاکمیت سایبری | مدیریت کنترل‌ها، انطباق، تخصیص مسئولیت، پایش | اجرای سیاست‌های امنیتی |
| مدیریت ریسک سایبری | شناسایی، تحلیل، ارزیابی، پاسخ و پایش ریسک | اولویت‌بندی تصمیمات امنیتی |
| هوش مصنوعی | تحلیل داده، پیش‌بینی تهدید، تشخیص ناهنجاری، تصمیم‌یار | افزایش دقت و سرعت تصمیم‌گیری |
| یادگیری مستمر | بازخورد، بهبود کنترل‌ها، آموزش مدل‌ها، بازنگری سیاست‌ها | ارتقای مستمر تاب‌آوری |

## تحلیل تعامل میان ابعاد چارچوب

تحلیل خبرگان نشان داد که اثربخشی هر یک از ابعاد چارچوب وابسته به تعامل آن با سایر ابعاد است و هیچ‌یک از آن‌ها به‌تنهایی قادر به ایجاد تاب‌آوری سایبری پایدار نیست. برای مثال، استقرار سامانه‌های هوش مصنوعی بدون وجود سیاست‌های حاکمیتی و فرآیندهای نظام‌مند مدیریت ریسک، ممکن است به تصمیم‌های غیرشفاف یا ناهماهنگ منجر شود. همچنین مدیریت ریسک بدون بهره‌گیری از تحلیل‌های هوشمند، در مواجهه با حجم بالای داده‌های امنیتی و تهدیدهای پیچیده، کارایی لازم را نخواهد داشت.

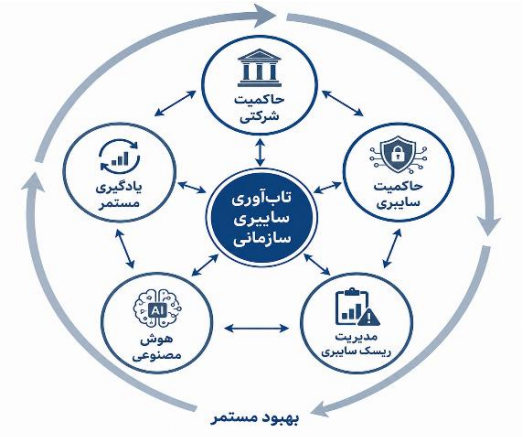
از سوی دیگر، خبرگان تأکید کردند که نقش هیئت‌مدیره در تعیین ریسک‌پذیری سازمان، تخصیص منابع و نظارت بر اجرای سیاست‌های امنیتی، عامل کلیدی موفقیت چارچوب است. این یافته با توصیه‌های سازمان همکاری و توسعه اقتصادی، انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی و مؤسسه ملی استانداردها و فناوری ایالات متحده مبنی بر ضرورت مشارکت فعال هیئت‌مدیره در حاکمیت سایبری همخوانی دارد.

همچنین، به‌کارگیری هوش مصنوعی در چارچوب پیشنهادی صرفاً به اتوماسیون فرآیندها محدود نیست، بلکه به‌عنوان ابزاری برای ارتقای کیفیت تصمیم‌گیری مدیریتی، کاهش زمان کشف تهدید، افزایش دقت ارزیابی ریسک و تسهیل یادگیری سازمانی در نظر گرفته شده است. این موضوع یکی از وجوه تمایز چارچوب حاضر نسبت به بسیاری از مدل‌های موجود است که هوش مصنوعی را صرفاً در سطح عملیاتی بررسی کرده‌اند.

## تبیین نوآوری چارچوب پیشنهادی

یافته‌های پژوهش نشان می‌دهد که نوآوری اصلی چارچوب پیشنهادی در یکپارچه‌سازی چهار حوزه راهبردی شامل حاکمیت شرکتی، حاکمیت سایبری، مدیریت ریسک و هوش مصنوعی در قالب یک چرخه یادگیرنده است. در این چارچوب، اطلاعات حاصل از پایش امنیتی و تحلیل‌های هوشمند، به‌صورت مستمر به فرآیندهای مدیریت ریسک و سطوح حاکمیتی بازخورد داده می‌شود و مبنای اصلاح سیاست‌ها و تصمیمات آینده قرار می‌گیرد.

این چرخه یادگیری موجب می‌شود که سازمان در برابر تغییرات محیط تهدید، فناوری‌های نوظهور و الگوهای جدید حملات، توان انطباق و بازآرایی خود را حفظ کند. به همین دلیل، چارچوب پیشنهادی تنها یک مدل مدیریتی نیست، بلکه یک سامانه حاکمیتی پویا برای ارتقای تاب‌آوری سایبری محسوب می‌شود.




**شکل ۳.** چرخه تعامل مؤلفه‌های چارچوب حاکمیت تاب‌آوری سایبری سازمانی

### ارزیابی مدل اندازه‌گیری

پس از نهایی‌شدن چارچوب در مرحله کیفی و دلفی، مدل اندازه‌گیری با استفاده از روش حداقل مربعات جزئی ارزیابی شد. در این مرحله، پایایی سازه‌ها با استفاده از آلفای کرونباخ، rho_Aو پایایی ترکیبی و روایی همگرا با استفاده از میانگین واریانس استخراج‌شده بررسی شد. نتایج نشان داد که مقادیر شاخص‌های پایایی برای تمامی سازه‌ها در محدوده قابل قبول قرار دارد و مقادیر میانگین واریانس استخراج‌شده نیز از حداقل معیار قابل قبول ۵۰/۰ بالاتر است. بنابراین، سازه‌های مورد استفاده از پایایی درونی و روایی همگرای مطلوب برخوردارند.

### جدول ٤

*نتایج ارزیابی پایایی و روایی همگرای سازه‌ها*

| سازه | تعداد گویه | آلفای کرونباخ | rho_A | پایایی ترکیبی (CR) | AVE |
|---|---|---|---|---|---|
| حاکمیت شرکتی | ۷ | ۰/۸۹۲ | ۰/۸۹۶ | ۰/۹۱۵ | ۰/۶۰۵ |
| حاکمیت سایبری | ۷ | ۰/۸۸۴ | ۰/۸۸۹ | ۰/۹۱۰ | ۰/۵۹۳ |
| مدیریت ریسک سایبری | ۷ | ۰/۹۰۱ | ۰/۹۰۵ | ۰/۹۲۲ | ۰/۶۲۹ |
| هوش مصنوعی | ۶ | ۰/۸۷۶ | ۰/۸۸۲ | ۰/۹۰۷ | ۰/۶۱۹ |
| تاب‌آوری سایبری | ۷ | ۰/۹۱۳ | ۰/۹۱۶ | ۰/۹۳۰ | ۰/۶۵۲ |

همان‌گونه که در جدول ۴ مشاهده می‌شود، مقدار آلفای کرونباخ سازه‌ها بین ۰/۸۷۶ و ۰/۹۱۳، مقدار rho_A بین ۰/۸۸۲ و ۰/۹۱۶ و مقدار پایایی ترکیبی بین ۰/۹۰۷ و ۰/۹۳۰ قرار دارد. همچنین مقدار میانگین واریانس استخراج‌شده تمامی سازه‌ها بیش از ۰/۵۰ است. بنابراین، پایایی درونی و روایی همگرای مدل اندازه‌گیری در سطح مطلوب ارزیابی می‌شود.

### ارزیابی روایی واگرا

برای بررسی تمایز سازه‌های مدل از یکدیگر، روایی واگرا با استفاده از معیار فورنل–لارکر و نسبت هتروتریت – مونوتریت ارزیابی شد. نتایج نشان داد که جذر میانگین واریانس استخراج‌شده هر سازه از همبستگی آن سازه با سایر سازه‌ها بیشتر بوده و مقادیر هتروتریت –

مونوتریت نیز در محدوده قابل قبول قرار دارند. بنابراین، سازه‌های مدل از تمایز مفهومی و آماری مناسبی برخوردارند.

**جدول ۵**

*نتایج معیار فورنل–لارکر*

| سازه | حاکمیت شرکتی | حاکمیت سایبری | مدیریت ریسک سایبری | هوش مصنوعی | تاب‌آوری سایبری |
|---|---|---|---|---|---|
| حاکمیت شرکتی | ۰/۷۷۸ | ۰/۶۲۴ | ۰/۵۸۱ | ۰/۵۴۸ | ۰/۵۳۲ |
| حاکمیت سایبری | ۰/۶۲۴ | ۰/۷۷۰ | ۰/۶۷۱ | ۰/۶۰۲ | ۰/۵۸۷ |
| مدیریت ریسک سایبری | ۰/۵۸۱ | ۰/۶۷۱ | ۰/۷۹۳ | ۰/۷۸۷ | ۰/۷۱۱ |
| هوش مصنوعی | ۰/۵۴۸ | ۰/۶۰۲ | ۰/۶۴۸ | ۰/۷۸۷ | ۰/۷۱۱ |
| تاب‌آوری سایبری | ۰/۵۳۲ | ۰/۵۸۷ | ۰/۶۹۲ | ۰/۷۱۱ | ۰/۸۰۸ |

مقادیر قطری جدول نشان‌دهنده جذر میانگین واریانس استخراج‌شده هستند. همان‌طور که مشاهده می‌شود، مقدار جذر میانگین واریانس استخراج‌شده هر سازه از ضرایب همبستگی آن با سایر سازه‌ها بیشتر است؛ بنابراین شرط فورنل–لارکر برقرار است.

**جدول ٦**

*نتایج آزمون هتروتریت ـ مونوتریت*

| رابطه سازه‌ها | هتروتریت ـ مونوتریت |
|---|---|
| حاکمیت شرکتی – حاکمیت سایبری | ۰/۷۰۶ |
| حاکمیت شرکتی – مدیریت ریسک سایبری | ۰/۶۵۸ |
| حاکمیت شرکتی – هوش مصنوعی | ۰/۶۲۱ |
| حاکمیت شرکتی – تاب‌آوری سایبری | ۰/۶۰۳ |
| حاکمیت سایبری – مدیریت ریسک سایبری | ۰/۷۵۲ |
| حاکمیت سایبری – هوش مصنوعی | ۰/۶۹۱ |
| حاکمیت سایبری – تاب‌آوری سایبری | ۰/۶۷۴ |
| مدیریت ریسک سایبری – هوش مصنوعی | ۰/۷۳۱ |
| مدیریت ریسک سایبری – تاب‌آوری سایبری | ۰/۷۸۴ |
| هوش مصنوعی – تاب‌آوری سایبری | ۰/۸۱۲ |

بیشترین مقدار نسبت هتروتریت - مونوتریت مربوط به رابطه هوش مصنوعی و تاب‌آوری سایبری و برابر با ۰/۸۱۲ است که در محدوده قابل قبول قرار دارد. بنابراین، نتایج دو آزمون فورنل–لارکر و نسبت هتروتریت - مونوتریت ، روایی واگرای مدل اندازه‌گیری را تأیید می‌کنند.

## ارزیابی مدل ساختاری و آزمون فرضیه‌ها

پس از تأیید مدل اندازه‌گیری، مدل ساختاری پژوهش مورد ارزیابی قرار گرفت. برای بررسی معناداری روابط، از ضرایب مسیر، آماره t و مقدار p استفاده شد. نتایج نشان داد که تمامی مسیرهای مستقیم پیشنهادی دارای اثر مثبت و معنادار هستند. همچنین، اثرهای غیرمستقیم مربوط به فرضیه‌های میانجی نیز مورد بررسی قرار گرفت.

**جدول ۷**

*نتایج آزمون فرضیه‌های پژوهش*

| فرضیه | مسیر | β | t | p | نتیجه |
|---|---|---|---|---|---|
| H1 | حاکمیت شرکتی ← حاکمیت سایبری | ۰/۶۲۴ | ۱۰/۸۴۷ | <۰/۰۰۱ | تأیید |
| H2 | حاکمیت سایبری ← مدیریت ریسک سایبری | ۰/۶۷۱ | ۱۳/۱۲۶ | <۰/۰۰۱ | تأیید |
| H3 | مدیریت ریسک سایبری ← هوش مصنوعی | ۰/۶۴۸ | ۱۱/۹۳۲ | <۰/۰۰۱ | تأیید |
| H4 | هوش مصنوعی ← تاب‌آوری سایبری | ۰/۵۶۳ | ۹/۶۸۴ | <۰/۰۰۱ | تأیید |
| H5 | مدیریت ریسک سایبری ← تاب‌آوری سایبری | ۰/۳۲۸ | ۵/۴۱۷ | <۰/۰۰۱ | تأیید |
| H6 | مدیریت ریسک سایبری ← هوش مصنوعی ← تاب‌آوری سایبری | ۰/۳۶۵ | ۷/۱۲۶ | <۰/۰۰۱ | تأیید |
| H7 | حاکمیت شرکتی ← حاکمیت سایبری ← مدیریت ریسک سایبری | ۰/۴۱۹ | ۸/۵۰۳ | <۰/۰۰۱ | تأیید |

نتایج جدول ۷ نشان می‌دهد که حاکمیت شرکتی تأثیر مثبت و معناداری بر حاکمیت سایبری دارد (ضریب مسیر: ۰/۶۲۴؛ آماره تی: ۱۰/۸۴۷؛ سطح معناداری: کمتر از ۰/۰۰۱). همچنین، حاکمیت سایبری تأثیر مثبت و معناداری بر مدیریت ریسک سایبری دارد (ضریب مسیر: ۰/۶۷۱؛ آماره تی: ۱۳/۱۲۶؛ سطح معناداری: کمتر از ۰/۰۰۱). تأثیر مدیریت ریسک سایبری بر به‌کارگیری هوش مصنوعی نیز مثبت و معنادار است (ضریب مسیر: ۰/۶۴۸؛ آماره تی: ۱۱/۹۳۲؛ سطح معناداری: کمتر از ۰/۰۰۱). افزون بر این، به‌کارگیری هوش مصنوعی تأثیر مثبت و معناداری بر تاب‌آوری سایبری دارد (ضریب مسیر: ۰/۵۶۳؛ آماره تی: ۹/۶۸۴؛ سطح معناداری: کمتر از ۰/۰۰۱). اثر مستقیم مدیریت ریسک سایبری بر تاب‌آوری سایبری نیز مثبت و معنادار است (ضریب مسیر: ۰/۳۲۸؛ آماره تی: ۵/۴۱۷؛ سطح معناداری: کمتر از ۰/۰۰۱).

بررسی اثرهای غیرمستقیم نشان می‌دهد که به‌کارگیری هوش مصنوعی در رابطه میان مدیریت ریسک سایبری و تاب‌آوری سایبری نقش میانجی معناداری دارد (ضریب اثر غیرمستقیم: ۰/۳۶۵؛ آماره تی: ۷/۱۲۶؛ سطح معناداری: کمتر از ۰/۰۰۱). همچنین، نقش میانجی حاکمیت سایبری در رابطه میان حاکمیت شرکتی و مدیریت ریسک سایبری معنادار است

(ضریب اثر غیرمستقیم: ۰/۴۱۹؛ آماره تی: ۸/۵۰۳؛ سطح معناداری: کمتر از ۰/۰۰۱). بر اساس نتایج گزارش‌شده، هر هفت فرضیه پژوهش تأیید شدند.

## قدرت تبیین مدل

برای ارزیابی قدرت تبیین مدل ساختاری، ضریب تعیین ($R^2$) برای سازه‌های درون‌زا محاسبه شد. نتایج نشان می‌دهد که مدل پیشنهادی بخش قابل توجهی از تغییرات سازه‌های درون‌زا را تبیین می‌کند.

### جدول ۸

شاخص‌های قدرت تبیین مدل ساختاری پژوهش

| سازه درون‌زا | $R^2$ | $R^2$ تعدیل‌شده |
|---|---|---|
| حاکمیت سایبری | ۰/۳۹۰ | ۰/۳۸۷ |
| مدیریت ریسک سایبری | ۰/۴۵۰ | ۰/۴۴۷ |
| هوش مصنوعی | ۰/۴۲۰ | ۰/۴۱۷ |
| تاب‌آوری سایبری | ۰/۶۷۲ | ۰/۶۶۹ |

بیشترین قدرت تبیین مدل مربوط به سازه تاب‌آوری سایبری است که ضریب تعیین آن برابر با ۰/۶۷۲ به دست آمد؛ بنابراین، متغیرهای پیش‌بین این سازه در مدل، ۶۷/۲ درصد از واریانس آن را تبیین می‌کنند. همچنین، ضرایب تعیین حاکمیت سایبری، مدیریت ریسک سایبری و هوش مصنوعی به‌ترتیب برابر با ۰/۳۹۰، ۰/۴۵۰ و ۰/۴۲۰ است؛ به این معنا که متغیرهای پیش‌بین هر یک از این سازه‌ها، به‌ترتیب ۳۹، ۴۵ و ۴۲ درصد از واریانس آن‌ها را تبیین می‌کنند. ضرایب تعیین تعدیل‌شده نیز برای حاکمیت سایبری، مدیریت ریسک سایبری، هوش مصنوعی و تاب‌آوری سایبری به‌ترتیب برابر با ۰/۳۸۷، ۰/۴۴۷، ۰/۴۱۷ و ۰/۶۶۹ به دست آمد.

### اندازه اثر و قدرت پیش‌بینی

در ادامه، اندازه اثر روابط با استفاده از شاخص $f^2$ و قدرت پیش‌بینی مدل با استفاده از شاخص $Q^2$ بررسی شد. نتایج نشان داد که مسیرهای اصلی مدل دارای اندازه اثر قابل قبول بوده و مقادیر $Q^2$ برای سازه‌های درون‌زا مثبت است؛ بنابراین، مدل علاوه بر قدرت تبیین، از قدرت پیش‌بینی قابل قبول نیز برخوردار است.

**جدول ۹**

*شاخص‌های قدرت پیش‌بینی مدل ساختاری پژوهش*

| سازه درون‌زا | $Q^2$ |
|---|---|
| حاکمیت سایبری | ۰/۳۵۲ |
| مدیریت ریسک سایبری | ۰/۴۰۱ |
| هوش مصنوعی | ۰/۳۶۸ |
| تاب‌آوری سایبری | ۰/۵۱۷ |

و:

**جدول ۱۰**

*اندازه اثر مسیرهای مدل ساختاری پژوهش*

| مسیر | $f^2$ |
|---|---|
| حاکمیت شرکتی ← حاکمیت سایبری | ۰/۶۳۷ |
| حاکمیت سایبری ← مدیریت ریسک سایبری | ۰/۸۱۸ |
| مدیریت ریسک سایبری ← هوش مصنوعی | ۰/۷۲۱ |
| هوش مصنوعی ← تاب‌آوری سایبری | ۰/۳۹۸ |
| مدیریت ریسک سایبری ← تاب‌آوری سایبری | ۰/۱۲۶ |

## بحث و نتیجه‌گیری

تحول دیجیتال، گسترش زیرساخت‌های مبتنی بر فناوری اطلاعات و افزایش وابستگی سازمان‌ها به خدمات دیجیتال، موجب شده است که امنیت سایبری از یک مسئله صرفاً فنی به یکی از مهم‌ترین موضوعات راهبردی در حاکمیت سازمانی تبدیل شود. در چنین شرایطی،

سازمان‌ها علاوه بر حفاظت از دارایی‌های اطلاعاتی، باید توانایی حفظ تداوم فعالیت، پاسخ‌گویی مؤثر به رخدادهای سایبری و بازگشت سریع به وضعیت عادی را نیز داشته باشند. از این رو، مفهوم تاب‌آوری سایبری طی سال‌های اخیر به یکی از ارکان اصلی مدیریت ریسک سازمانی تبدیل شده است.

هدف اصلی پژوهش حاضر، طراحی چارچوبی جامع برای حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک بود. بر اساس مرور نظام‌مند ادبیات، تحلیل استانداردهای بین‌المللی و تلفیق دیدگاه‌های خبرگان، چارچوبی پنج‌بعدی شامل حاکمیت شرکتی، حاکمیت سایبری، مدیریت ریسک سایبری، هوش مصنوعی و یادگیری مستمر ارائه شد. این چارچوب با ایجاد ارتباط میان لایه‌های راهبردی، مدیریتی و عملیاتی، زمینه ارتقای توان سازمان در پیش‌بینی، پیشگیری، تشخیص، پاسخ، بازیابی و انطباق با تهدیدهای سایبری را فراهم می‌کند.

یافته‌های پژوهش نشان داد که حاکمیت شرکتی نقطه آغاز شکل‌گیری تاب‌آوری سایبری است. بدون مشارکت فعال هیئت‌مدیره، تعیین سطح ریسک‌پذیری، تصویب سیاست‌های امنیتی و تخصیص منابع، ایجاد سازوکارهای پایدار مدیریت ریسک و امنیت سایبری امکان‌پذیر نخواهد بود. این نتیجه با گزارش‌های سازمان همکاری و توسعه اقتصادی و چارچوب کوبیت ۲۰۱۹ همسو است که بر مسئولیت مستقیم هیئت‌مدیره در مدیریت ریسک‌های سایبری تأکید می‌کنند. همچنین یافته‌های پژوهش حاضر نشان می‌دهد که حاکمیت سایبری باید به‌عنوان حلقه واسط میان سیاست‌های کلان و فرآیندهای اجرایی عمل کند و از طریق نظارت مستمر، ارزیابی انطباق و مدیریت کنترل‌ها، تحقق اهداف امنیتی سازمان را تضمین نماید.

یکی دیگر از یافته‌های مهم پژوهش، نقش محوری مدیریت ریسک سایبری در چارچوب پیشنهادی است. برخلاف رویکردهای سنتی که مدیریت ریسک را فرآیندی دوره‌ای و عمدتاً مبتنی بر ارزیابی‌های دستی می‌دانند، چارچوب حاضر بر مدیریت ریسک پویا و داده‌محور تأکید دارد. در این رویکرد، اطلاعات حاصل از سامانه‌های پایش امنیتی، تحلیل‌های هوشمند و بازخوردهای عملیاتی به‌صورت مستمر در فرآیند ارزیابی ریسک وارد شده و موجب به‌روزرسانی اولویت‌های امنیتی سازمان می‌شود. این نتیجه با یافته‌های پژوهش‌های کور و

همکاران و شارما و همکاران همخوانی دارد که مدیریت ریسک پویا را یکی از پیش‌نیازهای تاب‌آوری سایبری معرفی کرده‌اند.

پژوهش حاضر همچنین نشان داد که هوش مصنوعی تنها یک ابزار فناورانه برای تشخیص نفوذ یا تحلیل داده نیست، بلکه می‌تواند به‌عنوان یک سامانه تصمیم‌یار مدیریتی در تمام مراحل چرخه مدیریت ریسک ایفای نقش کند. به‌کارگیری الگوریتم‌های یادگیری ماشین، تحلیل رفتار، کشف ناهنجاری، پیش‌بینی تهدید و اولویت‌بندی هشدارها، امکان تصمیم‌گیری سریع‌تر و دقیق‌تر را برای مدیران فراهم می‌کند. علاوه بر این، استفاده از تحلیل‌های هوشمند موجب کاهش زمان کشف حملات، بهبود کیفیت ارزیابی ریسک و افزایش سرعت پاسخ‌گویی به رخدادهای امنیتی می‌شود. این یافته با چارچوب چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری و گزارش‌های اخیر آژانس اتحادیه اروپا برای امنیت سایبری در سال ۱۴۰۳ و مایکروسافت در سال ۱۴۰۴ مبنی بر نقش هوش مصنوعی در ارتقای امنیت سایبری سازگار است.

از مهم‌ترین نوآوری‌های چارچوب پیشنهادی، ایجاد چرخه یادگیری مستمر میان تمامی ابعاد مدل است. در بسیاری از چارچوب‌های موجود، فرآیند مدیریت ریسک به ارزیابی و پاسخ ختم می‌شود؛ اما در مدل حاضر، نتایج حاصل از هر رخداد سایبری، تحلیل‌های هوش مصنوعی و بازخوردهای مدیریتی، مجدداً وارد فرآیندهای حاکمیتی شده و مبنای اصلاح سیاست‌ها، بازنگری کنترل‌ها و آموزش مجدد مدل‌های هوش مصنوعی قرار می‌گیرد. این چرخه موجب افزایش توان انطباق سازمان در برابر تهدیدهای نوظهور و کاهش آسیب‌پذیری در بلندمدت می‌شود.

از منظر نظری، پژوهش حاضر با یکپارچه‌سازی مفاهیم حاکمیت شرکتی، مدیریت ریسک، امنیت سایبری، هوش مصنوعی و تاب‌آوری سازمانی، مدلی مفهومی ارائه می‌کند که می‌تواند مبنای توسعه پژوهش‌های آینده قرار گیرد. بسیاری از مطالعات پیشین این حوزه را به‌صورت مجزا بررسی کرده‌اند؛ در حالی که پژوهش حاضر ارتباط میان این مؤلفه‌ها را در قالب یک نظام حاکمیتی منسجم تبیین کرده است. از این رو، چارچوب پیشنهادی می‌تواند به غنای ادبیات پژوهش در حوزه حاکمیت سایبری و مدیریت ریسک فناوری اطلاعات کمک کند.

از منظر کاربردی، نتایج پژوهش برای سازمان‌هایی که با ریسک‌های سایبری گسترده مواجه هستند، از جمله بانک‌ها، شرکت‌های بیمه، اپراتورهای مخابراتی، سازمان‌های دولتی، شرکت‌های زیرساختی و صنایع حیاتی، قابل استفاده است. استقرار چارچوب پیشنهادی می‌تواند به مدیران ارشد در تعیین سیاست‌های امنیتی، تخصیص بهینه منابع، اولویت‌بندی سرمایه‌گذاری‌های امنیتی، ارتقای هماهنگی میان واحدهای سازمانی و افزایش آمادگی در برابر رخدادهای سایبری کمک کند. همچنین، استفاده از هوش مصنوعی در فرآیندهای مدیریت ریسک می‌تواند موجب کاهش هزینه‌های ناشی از رخدادهای امنیتی، افزایش سرعت بازیابی خدمات و بهبود کیفیت تصمیم‌گیری مدیریتی شود.

با وجود دستاوردهای پژوهش، محدودیت‌هایی نیز وجود دارد. نخست، چارچوب پیشنهادی بر پایه مرور ادبیات، استانداردهای بین‌المللی و دیدگاه خبرگان تدوین شده و برای تعمیم نتایج به تمامی سازمان‌ها، لازم است در محیط‌های عملیاتی مختلف اعتبارسنجی شود. دوم، سرعت بالای تحول فناوری‌های هوش مصنوعی و ظهور تهدیدهای جدید سایبری ممکن است در آینده نیازمند بازنگری و به‌روزرسانی برخی مؤلفه‌های چارچوب باشد. سوم، تفاوت در ساختار حاکمیتی، الزامات قانونی و سطح بلوغ امنیت سایبری سازمان‌ها می‌تواند بر نحوه استقرار و اثربخشی چارچوب تأثیرگذار باشد.

بر این اساس، پیشنهاد می‌شود در پژوهش‌های آینده، چارچوب ارائه‌شده در صنایع مختلف از جمله بانکداری، سلامت، انرژی، حمل‌ونقل و خدمات دولت الکترونیک به‌صورت تجربی اعتبارسنجی شود. همچنین بررسی نقش فناوری‌های نوظهوری مانند سامانه‌های چندعاملی هوش مصنوعی، هوش مصنوعی مولد، رایانش لبه، معماری اعتماد صفر و رایانش کوانتومی در توسعه تاب‌آوری سایبری می‌تواند زمینه‌های ارزشمندی برای پژوهش‌های آینده فراهم آورد. علاوه بر این، توسعه شاخص‌های بلوغ حاکمیت تاب‌آوری سایبری و طراحی مدل‌های ارزیابی عملکرد مبتنی بر هوش مصنوعی نیز از دیگر حوزه‌های پژوهشی قابل پیشنهاد است.

در مجموع، نتایج این پژوهش نشان می‌دهد که دستیابی به تاب‌آوری سایبری پایدار مستلزم عبور از رویکردهای سنتی امنیت اطلاعات و حرکت به سمت نظام‌های هوشمند حاکمیتی است. چارچوب پیشنهادی با تلفیق اصول حاکمیت شرکتی، مدیریت ریسک، هوش

مصنوعی و یادگیری مستمر، زمینه ایجاد سازمان‌هایی را فراهم می‌کند که نه‌تنها توانایی مقابله با تهدیدهای سایبری را دارند، بلکه قادرند از رخدادهای امنیتی بیاموزند، خود را با شرایط جدید تطبیق دهند و در بلندمدت مزیت رقابتی پایدارتری در فضای دیجیتال کسب کنند.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع


احمدی، م.، و رضایی، ع. (۱۴۰۲). ارائه چارچوب مدیریت ریسک امنیت سایبری در سازمان‌های مالی ایران. *فصلنامه مدیریت فناوری اطلاعات*، ۱۵(۳)، ۵۵–۷۸.

جعفری، س.، محمدی، ع.، و کریمی، ح. (۱۴۰۱). ارزیابی بلوغ امنیت سایبری در سازمان‌های ایرانی با رویکرد COBIT 2019. *پژوهش‌های مدیریت فناوری اطلاعات*، ۱۴(۲)، ۹۱–۱۱۲.

حسینی، م.، و همکاران. (۱۴۰۳). نقش هوش مصنوعی در مدیریت ریسک امنیت اطلاعات. *فصلنامه پژوهش‌های فناوری اطلاعات*، ۱۸(۱)، ۲۵–۴۸.


## References


Ahmadi, M., & Rezaei, A. (2023). A framework for cybersecurity risk management in Iranian financial organizations. *Journal of Information Technology Management*, 15(3), 55–78. (in Persian).

Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Computing Surveys*, *56*(8), 196, 1–48. https://doi.org/10.1145/3649218

Committee of Sponsoring Organizations of the Treadway Commission (COSO), & World Business Council for Sustainable Development (WBCSD). (2018). *Enterprise risk management: Applying enterprise risk management to environmental, social and governance-related risks*.

Creswell, J. W., & Plano Clark, V. L. (2021). *Designing and conducting mixed methods research* (3rd ed.). SAGE.

Deloitte. (2024). *Global Future of Cyber Survey 2024*. Deloitte.

ENISA. (2023). *Artificial intelligence and cybersecurity: Challenges and opportunities*. European Union Agency for Cybersecurity.

ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. https://doi.org/10.2824/0710888

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE.

Hosseini, M., et al. (2024). Artificial intelligence in information security risk management. *Information Technology Research Journal, 18*(1), 25–48. (in Persian).

IBM. (2024). *Cost of a data breach report 2024*. IBM Security.

ISACA. (2020). *COBIT 2019 framework: Governance and management objectives*. ISACA.

ISACA. (2023). *State of Cybersecurity 2023*. ISACA.

ISO. (2018). *ISO 31000:2018 Risk management—Guidelines*. International Organization for Standardization.

ISO. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*. International Organization for Standardization.

ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. International Organization for Standardization.

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Jafari, S., Mohammadi, A., & Karimi, H. (2022). Cybersecurity maturity assessment in Iranian organizations based on COBIT 2019. *Information Technology Management Studies, 14*(2), 91–112. (in Persian).

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P. A., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security*, *144*, 103964. https://doi.org/10.1016/j.cose.2024.103964

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. Microsoft.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

Organisation for Economic Co-operation and Development (OECD). (2023). *G20/OECD principles of corporate governance*. OECD Publishing.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. https://doi.org/10.6028/NIST.CSWP.29

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum.

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. World Economic Forum.

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Research Paper**

# Emerging Digital Technologies in the Auditing Industry: Challenges and New Opportunities [1]

**Kaveh Parandin[2], Kaveh Ghaderi[3] and Avan Jamshidi[*4]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 303-332

Received: 2025.12.14
Revised: 2026.04.06
Accepted: 2026.05.09

## Abstract

The auditing profession is undergoing a fundamental transformation in the digital age, driven by emerging technologies such as artificial intelligence and robotic process automation. This study aims to analyze the impact of these technologies on the efficiency, effectiveness, human resource structure, and competitive gap within auditing firms in Iran, employing a mixed-methods (qualitative-quantitative) approach. In the qualitative phase, 14 semi-structured interviews with experts were conducted to identify the key dimensions of technological impact and extract a preliminary conceptual model. In the quantitative phase, data collected from 300 valid questionnaires completed by auditors in large, medium, and small firms analyzed using covariance-based structural equation modeling in Amos software. The findings revealed that emerging technologies significantly enhance audit process efficiency by automating repetitive tasks. Furthermore, these technologies improve decision-making effectiveness and professional judgment quality by facilitating the analysis of complex data. Additionally, technology implementation has led to a reduction in low-level staff and a significant increase in demand for auditors with IT and data analytics skills. The environmental factor of client digitalization level was identified as the most decisive determinant of technology adoption by audit firms. The overall conclusion suggests that emerging technologies are transforming auditing into a data-driven and technology-based profession. While this transformation brings challenges such as a widening competitive gap between firms, the need for extensive retraining, and new ethical considerations, it also creates unparalleled opportunities for enhancing the quality, transparency, and efficiency of audit services.

**Keywords**: Artificial Intelligence; Auditing Profession; Digital Transformation; Efficiency and Effectiveness; Robotic Process Automation.

**JEL classification:** *M42, C88, O33.*

---

[1] https://doi.org/10.22034/JISTA.2026.566170.1075
[2] Department of Accounting, Payame Noor University, Tehran, Iran. Email: kparandin@pnu.ac.ir
[3] Department of Accounting, Payame Noor University, Tehran, Iran. Email: tekosh.gh@pnu.ac.ir
[4] Ph.D. Department of Accounting, Faculty of Social and Economic Sciences, AlZahra University, Tehran, Iran, Lecturer at National Skill University. (Corresponding Author). Email: jamshidi@alzahra.ac.ir

## 1. INTRODUCTION

Emerging digital technologies are reshaping global markets and providing opportunities for businesses and society to adopt them. These technologies offer innovators and business managers the chance to leverage them in the digital world to create and transform their organizations. Emerging technologies include artificial intelligence, blockchain, cloud computing, and big data. These technologies, whether independently or in combinations such as AI and IoT, possess disruptive potential and can fundamentally transform the performance of specific industries, education, and society. They act as catalysts for digital transformation, creating new opportunities and business models. Digital technologies have led to a "transformation in the auditing process," where auditing procedures are recognized as a "direct result of existing technologies." Some auditors believe that several auditing procedures can be automated, with a 94% probability that automation could replace accountants and auditors, as modern technologies enable a wide range of routine and non-routine cognitive tasks to be performed automatically. According to a report from the World Economic Forum (2015), 75.4% of 816 managers and experts in the field of information and communication technology believe that AI will perform 30% of corporate audits by 2025. Therefore, it is expected that emerging digital technologies will create new opportunities and risks in the accounting and auditing profession. Emerging technologies are rapidly changing the auditing field, compelling auditors to adopt new technologies to increase efficiency and maintain competitiveness. However, the adoption of technology by auditors is influenced by various factors, including technological readiness, perceived ease of use, and perceived usefulness. Auditors have significantly lagged behind their clients in adopting new technologies. This delay can be attributed to various reasons, including the conservatism and rigidity of the profession, as well as the gradual tightening of procedures. If auditing firms do not adopt modern tools, companies like Google or fintech startups may begin to offer similar services. Therefore, the

skills, tools, and activities of auditors are rapidly changing. Based on these considerations, this paper analyzes the impacts of new technologies such as robotic process automation and artificial intelligence on auditing firms. It also focuses on the following research question: How can emerging digital technologies improve the quality and efficiency of auditing processes, and what challenges do they pose in this regard?

## 2. MATERIALS AND METHODS

This research investigates the impact of emerging digital technologies, such as artificial intelligence and robotic process automation, on the efficiency, effectiveness, human resource structure, and competitive gap of auditing firms in Iran, employing a mixed exploratory-explanatory approach. In the first phase, qualitative data were gathered through semi-structured interviews with 14 auditors and specialists from various firms, focusing on key concepts and dimensions of the technology's impact. The qualitative analysis utilized open, axial, and selective coding to develop an initial model of the main research variables. In the second phase, a quantitative study was conducted to test hypotheses and generalize findings across a larger population of auditors in Iran. Stratified random sampling was used to collect data from 300 auditors, ensuring representation from large, medium, and small firms. A researcher-designed questionnaire measured variables related to efficiency, effectiveness, digitalization levels, and the use of AI and automation. The questionnaire's validity and reliability were confirmed through expert opinions and statistical analyses. Quantitative data were analyzed using structural equation modeling and supplementary tests to explore causal relationships among variables. Finally, qualitative and quantitative results were integrated to provide a comprehensive understanding of the effects of emerging technologies on the auditing profession in Iran, offering valuable insights for professional policymaking and decision-making.

## 3. RESULTS AND DISCUSSION

The findings indicate that emerging technologies significantly enhance the efficiency of the auditing process by automating repetitive tasks and reducing errors. These technologies also improve decision-making effectiveness and the quality of auditors' professional judgment by facilitating the analysis of complex data. The implementation of technology has led to a reduction in low-level staff within auditing firms and has directed the human resource structure towards specialization, while the demand for auditors with IT and data analysis skills has markedly increased.

Moreover, the level of client digitalization is a key factor in the adoption of emerging technologies by auditing firms, with a strong relationship between technological advancements in the client environment and the speed of auditors' digital transformation. The final conclusion suggests that emerging technologies are transforming auditing into a data-driven and technology-based profession. This transformation brings challenges such as the need for retraining auditors, managing ethical issues, and increasing the competitive gap between large and small firms, while also providing significant opportunities for enhancing the quality, transparency, and efficiency of auditing.

## 4. CONCLUSION

The research findings indicate that emerging technologies, particularly artificial intelligence (AI) and robotic process automation, have transformed the auditing profession from merely being auxiliary tools to essential elements that redefine its nature. These technologies have changed how data is collected, processed, risks are assessed, and judgments are made, transitioning the auditing process from a limited sampling model to a comprehensive, data-driven approach. This shift has significant implications for auditing quality, workforce structure, and operational efficiency, confirming that digital transformation in auditing is a strategic necessity rather than a temporary trend. The study reveals that emerging technologies enhance efficiency by speeding up

information processing, reducing human error, and eliminating repetitive tasks. The transition of auditors' focus from mechanical to judgment-oriented activities significantly boosts their productivity. Furthermore, the demand for auditors with IT and data analysis skills has increased, necessitating a transformation in workforce capabilities. The research also highlights that higher client digitalization compels auditing firms to adopt emerging technologies. The findings show that technology impacts auditing at operational, analytical, and strategic levels, enhancing efficiency, decision-making quality, and competitive advantage. The study concludes that technology complements rather than replaces human expertise, emphasizing the need for a balance between human and artificial intelligence in the auditing process. Ethical issues related to emerging technologies require human oversight and new standards in digital auditing education. Overall, the profession is evolving towards a technologically-driven ecosystem, necessitating significant adaptations in education and practice. The results align with global literature, confirming the transformative impact of emerging technologies on auditing.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ پژوهشی**

# فناوری‌های دیجیتال نوظهور در صنعت حسابرسی: چالش‌ها و فرصت‌های جدید[1]

**کاوه پرندین[2]، کاوه قادری[3] و آوان جمشیدی *[4]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۳۰۳ - ۳۳۲

تاریخ دریافت: ۱۴۰۴/۰۹/۲۳
تاریخ بازنگری: ۱۴۰۵/۰۱/۱۷
تاریخ پذیرش: ۱۴۰۵/۰۲/۱۹

## چکیده

*حرفه حسابرسی در عصر دیجیتال، شاهد تحولی بنیادین تحت تأثیر فناوری‌های نوظهوری چون هوش مصنوعی و اتوماسیون فرآیند رباتیک است. این پژوهش با هدف تحلیل تأثیر این فناوری‌ها بر کارایی، اثربخشی، ساختار نیروی انسانی و شکاف رقابتی در مؤسسات حسابرسی ایران، با رویکردی ترکیبی (کیفی-کمی) انجام شد. در فاز کیفی، با انجام ۱۴ مصاحبه نیمه‌ساختاریافته با خبرگان، ابعاد کلیدی تأثیر فناوری شناسایی و مدل مفهومی اولیه استخراج گردید. در فاز کمی، داده‌های حاصل از ۳۰۰ پرسشنامه معتبر از حسابرسان مؤسسات بزرگ، متوسط و کوچک، با استفاده از مدل‌سازی معادلات ساختاری مبتنی بر کوواریانس در نرم‌افزار Amos تحلیل شد. یافته‌ها نشان داد که فناوری‌های نوظهور از طریق خودکارسازی وظایف تکراری، کارایی فرآیند حسابرسی را به‌طور معناداری افزایش می‌دهند. همچنین، این فناوری‌ها با تسهیل تحلیل داده‌های پیچیده، اثربخشی تصمیم‌گیری و قضاوت حرفه‌ای حسابرسان را ارتقاء می‌بخشند. از سوی دیگر، استقرار فناوری منجر به کاهش کارکنان سطح پایین و افزایش تقاضا برای حسابرسان دارای مهارت‌های فناوری اطلاعات و تحلیل داده شده است. عامل محیطی سطح دیجیتالی‌شدن مشتریان نیز با ضریب مسیر ۰/۷۹ به عنوان تعیین‌کننده‌ترین عامل در پذیرش فناوری توسط مؤسسات حسابرسی شناسایی شد. نتیجه کلی حاکی از آن است که فناوری‌های نوظهور در حال تبدیل حسابرسی به یک حرفه داده‌محور و فناورانه هستند. این تحول اگرچه چالش‌هایی چون افزایش شکاف رقابتی بین مؤسسات، نیاز به بازآموزی گسترده و ملاحظات اخلاقی جدید را به همراه دارد، ولی فرصت‌های بی‌بدیلی برای ارتقای کیفیت، شفافیت و کارایی در ارائه خدمات حسابرسی ایجاد می‌کند.*

**واژه‌های کلیدی:** *هوش مصنوعی، اتوماسیون فرآیند رباتیک، حرفه حسابرسی، کارایی و اثربخشی، تحول دیجیتال.*

**طبقه‌بندی موضوعی:** *M42, C88, O33* .

---

[1] https://doi.org/10.22034/JISTA.2026.566170.1075

[2] گروه حسابداری، دانشگاه پیام نور، تهران، ایران. (kparandin@pnu.ac.ir)

[3] گروه حسابداری، دانشگاه پیام نور، تهران، ایران. (tekosh.gh@pnu.ac.ir)

[4] دکترا، گروه حسابداری، دانشکده علوم اجتماعی و اقتصادی دانشگاه الزهراء، تهران، ایران. مدرس مدعو دانشگاه ملی مهارت. (نویسنده مسئول). (jamshidi@alzahra.ac.ir)

## مقدمه

فناوری‌های دیجیتال نوظهور در حال بازسازی بازارهای جهانی هستند و فرصت‌هایی را برای کسب‌وکارها و جامعه به منظور پذیرش این فناوری‌ها فراهم می‌آورند. این فناوری‌ها به نوآوران و مدیران کسب‌وکار فرصتی می‌دهند تا از این فناوری‌ها در دنیای دیجیتال برای ایجاد و تغییر سازمان‌های خود بهره‌برداری کنند (تته و همکاران[1]، ۲۰۲۵: ۵۶). فناوری‌های نوظهور شامل هوش مصنوعی، بلاک‌چین، رایانش ابری و داده‌های کلان هستند (بوزتاش و همکاران[2]، ۲۰۲۵: ۱). این فناوری‌ها، چه به‌صورت مستقل و چه در ترکیب‌هایی مانند هوش مصنوعی T و IIT[3]، دارای پتانسیل تخریبی هستند و می‌توانند به‌طور بنیادین عملکرد صنایع خاص، آموزش و جامعه را متحول کنند. این فناوری‌ها به‌عنوان کاتالیزوری برای تحول دیجیتال عمل می‌کنند و فرصت‌ها و مدل‌های کسب‌وکار جدیدی را ایجاد می‌کنند (فلورئا[4]، ۲۰۲۴: ۲۱۵). فناوری‌های دیجیتال به «تحول در فرآیند حسابرسی» منجر شده‌اند که در آن رویه‌های حسابرسی به‌عنوان «نتیجه‌ای مستقیم از فناوری‌های موجود» شناخته می‌شوند (عیسی و همکاران[5]، ۲۰۱۶: ۵).

برخی از حسابرسان بر این باورند که تعدادی از رویه‌های حسابرسی قابلیت خودکارسازی دارند (موفیت و همکاران[6]، ۲۰۱۸: ۱)؛ به طوری که احتمال ۹۴ درصدی وجود دارد که خودکارسازی بتواند جایگزین حسابداران و حسابرسان شود، زیرا فناوری‌های مدرن این امکان را فراهم می‌آورند که طیف وسیعی از وظایف شناختی روتین و غیر روتین به‌طور خودکار انجام شوند (فری و آزبورن[7]، ۲۰۱۷: ۱). طبق گزارشی از مجمع جهانی اقتصاد (۲۰۱۵)، ۷۵/۴ درصد از ۸۱۶ مدیر و کارشناس در حوزه فناوری اطلاعات و ارتباطات اعتقاد دارند که هوش مصنوعی تا سال ۲۰۲۵، ۳۰ درصد از حسابرسی‌های شرکتی را انجام خواهد داد. بنابراین، انتظار می‌رود که فناوری‌های دیجیتال نوظهور، فرصت‌ها و ریسک‌های جدیدی را در حرفه حسابداری و حسابرسی به وجود آورند (دیبال و سیثامراجو[8]، ۲۰۲۱: ۷-۵). فناوری‌های نوظهور به‌سرعت در

1. Tetteh et al.
2. Bztaş et al.
3. Industrial Internet of Things (IIoT)
4. Florea
5. Issa et al.
6. Mffitt et al.
7. Frey & Osborne
8. Dyball & Seethamraju

حال تغییر حوزه حسابرسی هستند و حسابرسان را وادار به پذیرش فناوری‌های جدید برای افزایش کارایی و حفظ رقابت‌پذیری می‌کنند (آفسای و همکاران[1]، ۲۰۲۳: ۱). با این حال، پذیرش فناوری توسط حسابرسان تحت تأثیر عوامل متعددی قرار دارد، از جمله آمادگی فناوری، ادراک آسانی استفاده و ادراک مفید بودن (دامرچی و سلیمی[2]، ۲۰۲۱: ۱۰۷). این تأخیر می‌تواند به دلایل مختلفی، از جمله «سنت‌گرایی و سخت‌گیری حرفه و همچنین تأثیر سخت‌شدن تدریجی رویه‌ها» باشد. اگر شرکت‌های حسابرسی به استفاده از ابزارهای مدرن نپردازند، شرکت‌هایی مانند گوگل یا استارتاپ‌های فین‌تک ممکن است شروع به ارائه خدمات مشابه کنند (ریچینز و همکاران[3]، ۲۰۱۷: ۶۸-۶۵). بر اساس این ملاحظات، این مقاله به تحلیل تأثیرات فناوری‌های جدیدی مانند اتوماسیون فرآیند رباتیک و هوش مصنوعی بر شرکت‌های حسابرسی می‌پردازد. همچنین، بر روی سوال پژوهش زیر تمرکز می‌شود: فناوری‌های دیجیتال نوظهور چگونه می‌توانند کیفیت و کارایی فرایندهای حسابرسی را بهبود بخشند و چه چالش‌هایی را در این راستا به وجود می‌آورند؟

## مبانی نظری

دیجیتالی‌سازی به عنوان یکی از تغییرات و چالش‌های مهم در جامعه امروزی به‌دلیل تأثیر آن بر زندگی روزمره در نظر گرفته می‌شود. «دیجیتالی‌سازی» اصطلاحی است که برای توصیف طیف گسترده و پیچیده‌ای از فناوری‌ها و پدیده‌ها استفاده می‌شود (وارنر و واگر[4]، ۲۰۱۹: ۳۲۷). دیجیتالی‌سازی در حال تغییر روش‌های عملیاتی کسب‌وکارها است و با استفاده از فناوری‌های نوظهور، به ساده‌سازی عملیات، بهبود تصمیم‌گیری و افزایش کارایی کمک می‌کند (پات‌جوشی و همکاران[5]، ۲۰۲۵: ۱). دیجیتالی‌سازی شامل انتقال فرآیندهای سازمانی به راه‌حل‌های فناوری اطلاعات است که تغییرات قابل توجهی در جنبه‌های مختلف سازمان ایجاد

1. Afsay et al.
2. Damerji & Salimi
3. Richins et al.
4. Warner & Wager
5. Patjsh et al.

می‌کند (سعید و همکاران[1]، ۲۰۲۳: ۱). این موضوع فرصتی را برای کسب‌وکارها فراهم می‌آورد تا با استفاده از فناوری، سازمان خود را در دنیای دیجیتال ایجاد و متحول کنند (تتّه و همکاران، ۲۰۲۵: ۵۸). برخی از حسابرسان بر این باورند که مجموعه‌ای گسترده از فناوری‌ها می‌تواند از فعالیت‌های متنوعی که انجام می‌دهند، پشتیبانی کند. برای هر نوع وظیفه، ابزاری مناسب وجود دارد. در این راستا، عبدالمحمدی[2] (۱۹۹۹: ۵۱) به بررسی ۳۳۲ وظیفه حسابرسی پرداخته و اشاره کرده است که ۸۰ درصد از این وظایف ساختارمند یا نیمه‌ساختارمند هستند.

## روباتیک فرآیند اتوماسیون در بخش حسابرسی

در حوزه حسابرسی، استفاده از اتوماسیون فرآیند رباتیک به‌طور فزاینده‌ای رایج شده است. این فناوری با تقلید از انسان‌ها در انجام وظایف تکراری، به افزایش کارایی و دقت کمک می‌کند. اتوماسیون فرآیند رباتیک به‌ویژه برای وظایفی که دارای حجم زیاد و تکراری هستند، مناسب است و می‌تواند هزینه‌ها را کاهش و کارایی را افزایش دهد (هازار و توپلو[3]، ۲۰۲۳: ۴۶). استفاده از اتوماسیون فرآیند رباتیک در حسابرسی می‌تواند به‌طور قابل توجهی کیفیت حسابرسی را افزایش دهد. با اتوماسیون وظایفی مانند جمع‌آوری و ورود داده‌ها، حسابرسان می‌توانند انرژی بیشتری را به کارهایی که نیاز به تفکر سطح بالاتری دارند، اختصاص دهند(موفیت و همکاران، ۲۰۱۸: ۲). به‌طور خاص، اتوماسیون فرآیند رباتیک در چندین زمینه نقش‌آفرینی می‌کند:

- افزایش کارایی: اتوماسیون فرآیند رباتیک می‌تواند وظایف تکراری زیادی مانند پردازش فاکتورها، تأیید داده‌ها و تولید گزارش‌ها را خودکار کند و به این ترتیب زمان و منابع را صرفه‌جویی کند (هازار و توپلو، ۲۰۲۳: ۴۵).
- کاهش خطا: با کاهش دخالت انسانی، اتوماسیون فرآیند رباتیک خطر خطاهای انسانی را کاهش داده و دقت داده‌ها را افزایش می‌دهد (گاجار و همکاران[4]، ۲۰۲۲: ۱).

1 .Saeed et al.
2. Abdolmohammadi
3. Hazar & Toplu
4. Gajjar et al.

- تقویت کیفیت حسابرسی: اتوماسیون فرآیند رباتیک به حسابرسان این امکان را می‌دهد که بیشتر بر روی وظایفی که نیاز به قضاوت حرفه‌ای دارند، مانند ارزیابی ریسک و ارزیابی کنترل‌های داخلی، تمرکز کنند (موفیت و همکاران، ۲۰۱۸: ۲).
- بهبود انطباق: اتوماسیون فرآیند رباتیک می‌تواند به شرکت‌ها در رعایت بهتر مقررات و استانداردها کمک کند، زیرا می‌تواند به‌طور خودکار بررسی‌ها و گزارش‌های انطباق را انجام دهد (لاکورزینو و همکاران[1]، ۲۰۲۰: ۷۵۵).

اتوماسیون فرآیند رباتیک به حسابرسان این امکان را می‌دهد که وظایف حسابرسی ساختارمند، تکراری و مبتنی بر قواعد را اتوماسیون کنند، مانند تطبیق حساب‌ها، آزمون‌های کنترل داخلی و آزمون‌های تفصیلی (موفیت و همکاران، ۲۰۱۸: ۴). این ابزار به‌ویژه برای اتوماسیون وظایف در شرایطی مناسب است که فرآیندها در محیطی پایدار، با قواعد مشخص و پیچیدگی پایین انجام می‌شوند و شامل حجم بالای معاملات و داده‌های ساختارمند هستند. این وظایف باید به‌طور مکرر تکرار شوند و نیاز به دسترسی به سیستم‌های متعدد داشته باشند. همچنین، درک واضح از هزینه‌های دستی و وجود داده‌های دیجیتال از دیگر ویژگی‌های مهم این فرآیندها به شمار می‌رود. در نهایت، اتوماسیون فرآیند رباتیک برای فرآیندهایی که مستعد خطاهای انسانی هستند نیز بسیار مناسب است (اوریلیچ و همکاران[2]، ۲۰۲۲: ۶۹۱-۶۹۲). با وجود مزایای بسیار، اجرای فرآیند رباتیک به حسابرسان در حسابرسی با چالش‌هایی نیز مواجه است. یکی از چالش‌های اصلی، نرخ بالای شکست پروژه‌های فرآیند رباتیک به حسابرسان است. برای مقابله با این چالش‌ها، حسابرسان نیاز به اتخاذ اقداماتی فعال دارند. رویکرد سیستم‌های اجتماعی-فنی: استفاده از نظریه سیستم‌های اجتماعی-فنی، با در نظر گرفتن تعاملات بین فناوری، افراد و سازمان، می‌تواند به شناسایی و حل مشکلات احتمالی در فرآیند اجرای فرآیند رباتیک به حسابرسان کمک کند (دهبیه و موافی[3]، ۲۰۲۳: ۷۸). مدیریت ریسک: اتوماسیون فرآیندهای رباتیک مزایای گوناگونی ارائه می‌دهد؛ با این حال، پیاده‌سازی این فناوری بدون ریسک نیست. ریسک‌های متعددی وجود دارند که می‌توانند به شکست پیاده‌سازی یا استفاده بعدی از فناوری

1. Lacurezeanu et al.
2. Eulerich et al.
3. Dahabiyeh & Mwafi

اتوماسیون فرآیندهای رباتیک منجر شوند، از جمله ریسک‌های فناورانه، عامل انسانی، ریسک‌های مالی، و ریسک خودکارسازی فرآیندهای تجاری که برای اتوماسیون مناسب نیستند(هوروات و همکاران، ۲۰۲۴: ۹). تقویت مهارت‌ها: برنامه‌های آموزشی حسابداری نیاز به به‌روزرسانی دارند تا مهارت‌های استفاده از ابزارهای فرآیند رباتیک به حسابرسان را به حسابداران آینده آموزش دهند (وینسنت و همکاران[1]، ۲۰۲۰: ۷۸).

## هوش مصنوعی در بخش حسابرسی

اگرچه اتوماسیون فرآیند رباتیک تنها می‌تواند وظایف ساختاریافته را محاسبه کند، اما هوش مصنوعی قادر به انجام وظایف نیمه‌ساختاریافته و غیرساختاریافته است (ژانگ و همکاران[2]، ۲۰۲۲: ۱). هوش مصنوعی به سرعت در حال تغییر حوزه حسابرسی است و از طریق افزایش کارایی، دقت و بینش، فرآیندهای حسابرسی را بهبود می‌بخشد (موکتاش و همکاران[3]، ۲۰۲۴: ۱۳۲). برخی از کاربردها و تأثیرات کلیدی هوش مصنوعی در حوزه حسابرسی آورده شده است:

۱. اتوماسیون و افزایش کارایی: اتوماسیون فرآیند رباتیک (اتوماسیون فرآیند رباتیک): اتوماسیون فرآیند رباتیک یک تکنولوژی اتوماسیون است که می‌تواند رفتار انسان را در فرآیندهای تجاری شبیه‌سازی کند و به ویژه برای وظایف تکراری مناسب است (هازار و توپلو، ۲۰۲۳: ۴۸). در حسابرسی، اتوماسیون فرآیند رباتیک می‌تواند تعداد زیادی از وظایف تکراری مانند جمع‌آوری داده‌ها، پردازش فاکتورها و تولید گزارش‌ها را به‌طور خودکار انجام دهد و بدین ترتیب زمان و منابع را صرفه‌جویی کند (هوانگ و واسارلی[4]، ۲۰۱۹: ۱). استخراج و تأیید داده‌ها: هوش مصنوعی می‌تواند به‌طور خودکار از منابع مختلف داده استخراج کند و دقت و جامعیت آن‌ها را تأیید کند و بدین ترتیب نیاز به دخالت انسانی و اشتباهات را کاهش دهد. حسابرسی صورت‌های مالی: مدل‌های زبانی بزرگ می‌توانند برای اتوماسیون حسابرسی

1. Vincent et al.
2. Zhang & Vasarhelyi
3. Muqattash et al.
4. Huang & Vasarhelyi

صورت‌های مالی استفاده شوند و کارایی و دقت حسابرسی را افزایش دهند (وانگ و همکاران[1]، ۲۰۲۵: ۱).

۲. ارزیابی ریسک و تشخیص تقلب: ارزیابی ریسک: هوش مصنوعی می‌تواند حجم زیادی از داده‌ها را تحلیل کرده و حوزه‌های بالقوه ریسک را شناسایی کند و به حسابرسان کمک کند تا ارزیابی ریسک را به‌طور مؤثرتری انجام دهند. تشخیص تقلب: با تحلیل الگوهای معاملاتی و شناسایی رفتارهای غیرعادی، هوش مصنوعی می‌تواند به شناسایی تقلب کمک کند و اثر بخشی حسابرسی را افزایش دهد (موکتاش و همکاران، ۲۰۲۴: ۱۳۵).

۳. بهبود کیفیت حسابرسی: تمرکز بر قضاوت حرفه‌ای: با اتوماسیون وظایف تکراری، هوش مصنوعی به حسابرسان این امکان را می‌دهد که بیشتر بر روی وظایفی تمرکز کنند که نیاز به قضاوت حرفه‌ای دارند، مانند ارزیابی ریسک و ارزیابی کنترل‌های داخلی (هوانگ و واسارلی، ۲۰۱۹: ۳). افزایش کیفیت حسابرسی: استفاده از هوش مصنوعی می‌تواند کیفیت کلی حسابرسی را افزایش داده و اشتباهات و کاستی‌ها را کاهش دهد (لیو[2]، ۲۰۲۲: ۲۳).

۴. ترکیب هوش مصنوعی با سایر فناوری‌ها: اتوماسیون هوشمند: ترکیب اتوماسیون فرآیند رباتیک با هوش مصنوعی می‌تواند به اتوماسیون سیستم‌های قضاوتی کمک کند و وظایف پیچیده‌تری را مدیریت کند (العسولی[3]، ۲۰۲۵: ۱۲۲). به عنوان مثال، نرم‌افزار اتوماسیون فرآیند رباتیک مبتنی بر هوش مصنوعی می‌تواند به‌طور خودکار فاکتورها را پردازش کرده، داده‌ها را تأیید کند و گزارش‌ها را تولید کند. فناوری بلاک‌چین: ترکیب اتوماسیون فرآیند رباتیک با فناوری بلاک‌چین می‌تواند به اتوماسیون فرآیندهای حسابرسی و ایجاد اعتماد کمک کند و به حسابرسان اجازه دهد بر روی حساب‌های قابل‌اختصاص بیشتری تمرکز کنند تا تقلب را بهتر شناسایی و پیشگیری کنند.

۵. چالش‌های پیاده‌سازی: نرخ شکست اتوماسیون فرآیند رباتیک: با وجود مزایای اتوماسیون فرآیند رباتیک، پیاده‌سازی آن در حسابرسی با چالش‌هایی نیز مواجه است، از جمله نرخ بالای شکست پروژه‌های اتوماسیون فرآیند رباتیک. رویکرد سیستم‌های اجتماعی-فنی:

1. Wang et al.
2. Liu
3. Alassuli

استفاده از نظریه سیستم‌های اجتماعی-فنی، که به تعاملات بین فناوری، افراد و سازمان توجه دارد، می‌تواند به شناسایی و حل مشکلات احتمالی در فرآیند پیاده‌سازی اتوماسیون فرآیند رباتیک کمک کند (دهبیه و موافی، ۲۰۲۳: ۸۱-۷۸). ارتقاء مهارت‌ها: برنامه‌های آموزشی حسابداری نیاز به به‌روزرسانی دارند تا مهارت‌های استفاده از ابزارهای اتوماسیون فرآیند رباتیک را به حسابداران آینده آموزش دهند. به‌طور کلی، کاربردهای هوش مصنوعی در حوزه حسابرسی دارای پتانسیل زیادی هستند که می‌توانند کارایی، دقت و کیفیت حسابرسی را افزایش دهند (موکتاش و همکاران، ۲۰۲۴: ۱۳۳). با این حال، در فرآیند پیاده‌سازی هوش مصنوعی، نیاز است که چالش‌های مختلف به‌دقت مورد توجه قرار گیرد و اقدامات لازم برای تضمین موفقیت پروژه اتخاذ شود (دهبیه و موافی، ۲۰۲۳: ۷۷). با پیشرفت‌های تکنولوژیکی مداوم، هوش مصنوعی نقش فزاینده‌ای در حوزه حسابرسی ایفا خواهد کرد.

## تأثیرات چندگانه اتوماسیون فرآیند رباتیک بر فعالیت‌های حسابرسان و شرکت‌های حسابرسی

تأثیرات اتوماسیون فرآیندهای رباتیک بر حسابرسان و شرکت‌های حسابرسی: اتوماسیون فرآیندهای رباتیک تأثیرات متعددی بر فعالیت‌های حسابرسان و شرکت‌های حسابرسی دارد. این تأثیرات شامل افزایش بهره‌وری، کاهش خطاهای انسانی، بهبود دقت در تحلیل داده‌ها، و افزایش توانایی انجام وظایف تکراری و فرآیندهای استاندارد شده است (ویتالی و جولیانی[1]، ۲۰۲۴: ۱). علاوه بر این، اتوماسیون فرآیندهای رباتیک می‌تواند به حسابرسان کمک کند تا زمان بیشتری را به فعالیت‌های تحلیلی و ارزیابی ریسک اختصاص دهند، که منجر به تولید گزارش‌های با کیفیت بهتر می‌شود (موفیت و همکاران، ۲۰۱۸: ۴). از سوی دیگر، اتوماسیون فرآیندهای رباتیک ممکن است نیاز به مهارت‌های فنی جدید را افزایش دهد، که این امر می‌تواند چالش‌هایی برای حسابرسان و شرکت‌های حسابرسی کوچک و متوسط ایجاد کند (ویتالی و جولیانی، ۲۰۲۴: ۲).

1. Vitali & Giuliani

اتوماسیون فرآیندهای رباتیک تأثیرات مثبت قابل توجهی بر حسابرسان و شرکت‌های حسابرسی دارد. اولاً، اتوماسیون فرآیندهای رباتیک می‌تواند وظایف روتین و تکراری را اتوماسیون کند، که این امر زمان حسابرسان را صرفه‌جویی کرده و به آن‌ها اجازه می‌دهد بر وظایفی که به مهارت‌های تحلیلی و قضاوت شخصی نیاز دارند، تمرکز کنند. به عنوان مثال، اتوماسیون فرآیندهای رباتیک می‌تواند داده‌ها را از منابع مختلف جمع‌آوری کرده، گزارش‌ها را تهیه کند، داده‌ها را اعتبارسنجی کند و حساب‌ها را تسویه کند (پردانا و همکاران[1]، ۲۰۲۳: ۲)، که منجر به تکمیل سریع‌تر و کارآمدتر فرآیندهای حسابرسی می‌شود (لاکیورزانو و همکاران، ۲۰۲۰: ۷۶۰). ثانیاً، اتوماسیون فرآیندهای رباتیک می‌تواند خطاهای انسانی را که معمولاً در هنگام وارد کردن داده‌ها یا انجام محاسبات به صورت دستی رخ می‌دهد، کاهش دهد (سولانکی و همکاران[2]، ۲۰۲۴: ۱) و ربات‌ها می‌توانند وظایف را با دقت ثابت انجام دهند، که این امر خطر داده‌های نادرست یا گمراه‌کننده را کاهش می‌دهد. علاوه بر این، با اتوماسیون وظایف روتین و کاهش خطاها، اتوماسیون فرآیندهای رباتیک می‌تواند کیفیت حسابرسی را بهبود بخشد (اشرف[3]، ۲۰۲۴: ۴۳۷) و حسابرسان می‌توانند بیشتر بر ارزیابی ریسک، شناسایی تقلب‌های احتمالی و ارائه توصیه‌هایی برای بهبود فرآیندهای داخلی تمرکز کنند (موفیت و همکاران، ۲۰۱۸: ۶). در نهایت، اتوماسیون فرآیندهای رباتیک می‌تواند به شرکت‌های حسابرسی در رعایت مقررات و استانداردهای مختلف کمک کند (لاکیورزانو و همکاران، ۲۰۲۰: ۷۵۹) و ربات‌ها می‌توانند فرآیندهای نظارت و بررسی انطباق را اتوماسیون کنند، که این امر اطمینان می‌دهد که تمام الزامات قانونی رعایت می‌شود (داهیات[4]، ۲۰۲۲: ۱۶۰).

چالش‌ها و خطرات بالقوه اتوماسیون فرآیندهای رباتیک بر حسابرسان و شرکت‌های حسابرسی شامل موارد متعددی است. اولاً، اجرای اتوماسیون فرآیندهای رباتیک ممکن است در ابتدا هزینه‌بر باشد، به ویژه برای شرکت‌های حسابرسی کوچک و متوسط، زیرا هزینه‌ها شامل خرید نرم‌افزار، آموزش کارکنان و ادغام اتوماسیون فرآیندهای رباتیک با سیستم‌های موجود

1. Perdana et al.
2. Solanki et al.
3. Ashraf
4. Dahiyat

است. ثانیاً، استفاده از اتوماسیون فرآیندهای رباتیک نیاز به مهارت‌های جدیدی از حسابرسان دارد، مانند توانایی طراحی، اجرا و نگهداری ربات‌ها، که ممکن است شرکت‌های حسابرسی را مجبور کند تا در آموزش کارکنان خود سرمایه‌گذاری کرده یا متخصصان اتوماسیون فرآیندهای رباتیک را استخدام کنند (ویتالی و جولیانی، ۲۰۲۴: ۵-۴). همچنین، اتوماسیون فرآیندهای رباتیک می‌تواند خطرات امنیت سایبری را افزایش دهد اگر ربات‌ها به درستی ایمن نشوند؛ هکرها می‌توانند از ربات‌ها برای دسترسی به داده‌های حساس یا مختل کردن فرآیندهای حسابرسی استفاده کنند (اوریلیچ و همکاران، ۲۰۲۴: ۱۴۴). در نهایت، اتوماسیون فرآیندهای رباتیک ممکن است منجر به از دست دادن شغل در برخی زمینه‌ها شود، به ویژه برای کارکنانی که وظایف روتین و تکراری انجام می‌دهند، هرچند که اتوماسیون فرآیندهای رباتیک همچنین می‌تواند فرصت‌های شغلی جدیدی در زمینه‌هایی مانند طراحی و نگهداری ربات‌ها ایجاد کند (ویتاراناج و تیبوتووا[1]، ۲۰۲۱: ۱۰). ملاحظات اضافی در زمینه اتوماسیون فرآیندهای رباتیک شامل چند نکته کلیدی است. اولاً، استانداردسازی وظایف حسابداری و مالی می‌تواند به تسهیل فرایند اتوماسیون کمک کند و امکان استفاده گسترده‌تر از اتوماسیون فرآیندهای رباتیک را فراهم کند (اشرف، ۲۰۲۴: ۴۳۹). ثانیاً، اهمیت دارد که اطمینان حاصل شود داده‌های استفاده‌شده برای آموزش ربات‌ها عاری از تعصبات هستند، زیرا ربات‌ها می‌توانند تعصبات موجود در داده‌ها را تکرار کنند. همچنین، باید نظارت انسانی بر ربات‌ها وجود داشته باشد تا اطمینان حاصل شود که آن‌ها به درستی کار می‌کنند و تصمیمات نادرستی اتخاذ نمی‌کنند (مونوکو و همکاران[2]، ۲۰۲۰: ۲۱۵). در نهایت، ضروری است که توسعه مداوم توانایی‌های کارکنان برای هماهنگی با تغییرات فناوری وجود داشته باشد (ژنگ و همکاران، ۲۰۲۳: ۲). به طور کلی، اتوماسیون فرآیندهای رباتیک می‌تواند تأثیر قابل توجهی بر فعالیت‌های حسابرسان و شرکت‌های حسابرسی داشته باشد. با درک مزایا و چالش‌های بالقوه، شرکت‌های حسابرسی می‌توانند تصمیمات آگاهانه‌ای درباره اجرای اتوماسیون فرآیندهای رباتیک اتخاذ کنند (ویتالی و جولیانی، ۲۰۲۴: ۵).

1. Vitharanage & Thibbotuwawa
2. Munoko et al.

### تأثیرات چندگانه هوش مصنوعی بر فعالیت‌های حسابرسان و شرکت‌های حسابرسی

هوش مصنوعی تأثیرات متعددی بر فعالیت‌های حسابرسان و شرکت‌های حسابرسی دارد که فرصت‌ها و چالش‌های بزرگی را به همراه می‌آورد. هوش مصنوعی می‌تواند به اتوماسیون وظایف تکراری، بهبود کیفیت حسابرسی و افزایش کارایی کمک کند، اما همچنین چالش‌هایی را در زمینه تعصبات بالقوه در داده‌ها و نیاز به مهارت‌های جدید به وجود می‌آورد. هوش مصنوعی تأثیرات مثبت قابل توجهی بر حسابرسان و شرکت‌های حسابرسی دارد که می‌تواند به بهبود کیفیت حسابرسی، افزایش تجربه مشتری، بهبود کارایی و ایجاد تمایز کمک کند. به عنوان مثال، هوش مصنوعی می‌تواند کیفیت حسابرسی را از طریق اتوماسیون و استانداردسازی فرآیندها بهبود بخشد و با تحلیل حجم بالایی از داده‌ها، موارد غیرطبیعی یا الگوهایی را شناسایی کند که ممکن است به تقلب اشاره کنند. همچنین، با کاهش کارهای روتین برای حسابرسان و مشتریان، هوش مصنوعی می‌تواند تجربه مشتری را بهبود بخشد. علاوه بر این، هوش مصنوعی می‌تواند کارایی را با بازگشت زمان به حوزه‌های قضاوت و ریسک‌های بالا در حسابرسی ارتقاء دهد و به عنوان ابزاری برای تمایز شرکت‌ها از شرکت‌های سنتی دیگر عمل کند. هوش مصنوعی چالش‌ها و خطرات بالقوه‌ای برای حسابرسان و شرکت‌های حسابرسی به همراه دارد که شامل مشکلات متعددی است. یکی از این چالش‌ها، مشکل جعبه سیاه است که حسابرسان ممکن است در درک نحوه تصمیم‌گیری هوش مصنوعی با دشواری مواجه شوند، که این امر می‌تواند منجر به عدم اعتماد به نتایج گردد. همچنین، تعصب در تصمیمات مبتنی بر داده یکی دیگر از خطرات است، زیرا داده‌های استفاده‌شده برای آموزش هوش مصنوعی ممکن است متعصب باشند و این امر به تصمیمات ناعادلانه یا نادرست منجر شود. مشکلات همخوانی نیز می‌تواند از چالش‌ها باشد، زیرا ادغام ابزارهای هوش مصنوعی با سیستم‌های موجود دشوار است و این امر ممکن است کار دستی را افزایش دهد. همچنین، کمبود دانش در زمینه هوش مصنوعی می‌تواند مشکل‌ساز باشد، به‌طوری‌که حسابرسان ممکن است از دانش لازم برای درک نحوه کار هوش مصنوعی و تفسیر نتایج آن بی‌بهره باشند (یانگ و همکاران[1]، ۲۰۲۴: ۴-۲). در نهایت،

1. Yang

نیاز به مهارت‌های جدید یکی از چالش‌های مهم است، زیرا استفاده از هوش مصنوعی نیاز به مهارت‌های جدیدی از جمله توانایی تحلیل داده‌ها و تفسیر نتایج دارد، و شرکت‌های حسابرسی ممکن است نیاز به سرمایه‌گذاری در آموزش کارکنان خود یا استخدام متخصصان هوش مصنوعی داشته باشند.

پذیرش هوش مصنوعی در شرکت‌های حسابرسی تحت تأثیر عوامل متعددی قرار دارد که شامل موارد زیر است: تکنولوژی مناسب و محدودیت‌های آن که باید قادر به بهبود کیفیت حسابرسی، کارایی و تجربه مشتری باشد، در عین حال محدودیت‌هایی مانند مشکل جعبه سیاه، تعصب در تصمیمات مبتنی بر داده و مشکلات همخوانی را نیز برطرف کند. مدیریت نوآوری نیز از اهمیت بالایی برخوردار است؛ شرکت‌ها باید استراتژی روشنی برای نوآوری و سیاستی برای آزمایش ایده‌های جدید داشته باشند. همچنین، عوامل سازمانی نقش مهمی ایفا می‌کنند، به‌طوری‌که شرکت‌ها باید نمایندگان ارتباطی، منابع سازمانی و دانش در مورد هوش مصنوعی در سطح مدیریت و مهارت‌های دیجیتال در کارکنان خود داشته باشند. در نهایت، آمادگی برای هوش مصنوعی از دیگر عوامل حیاتی است؛ شرکت‌ها باید برای پذیرش هوش مصنوعی آماده باشند و زیرساخت داده‌ای قوی ایجاد کنند (یانگ و همکاران، ۲۰۲۴: ۵-۴). جدول شماره ۱، عوامل مؤثر بر پذیرش هوش مصنوعی را نشان می‌دهد.

**جدول ۱**

*عوامل مؤثر بر پذیرش هوش مصنوعی*

| مفهوم اول | گزاره‌های مثالی | ابعاد |
|---|---|---|
| بهبود کیفیت حسابرسی | بهبودهایی در کیفیت حسابرسی و محصول حسابرسی ما. می‌دانیم که استانداردسازی و اتوماسیون، کیفیت را بهبود می‌بخشد. | عوامل فناوری |
| بهبود تجربه مشتری | اگر بتوانیم کارهای روتین و خسته کننده را از مشتریان خود بگیریم، این به این معنی است که حسابرسی تجربه بهتری برای هر دو حسابرسان و خود مشتریان خواهد بود. | عوامل فناوری |
| بهینه‌سازی کارایی | ما قصد داریم از کارایی بهره‌برداری کنیم، که بتوانیم زمان کامل را در مناطق قضاوتی و ریسک‌های بالا در حسابرسی کنیم. | عوامل فناوری |
| ایجاد تمایز | استفاده از هوش مصنوعی به عنوان ابزاری بازاریابی، خود را بازاریابی کنیم که ما متفاوت از سایر شرکت‌های سنتی بودیم. | عوامل فناوری |

| | | |
|---|---|---|
| مشکل جعبه سیاه | همه چیز باید قابل توضیح باشد. اما در واقعیت، اینطور نیست. اگر توضیح‌پذیر نباشد، کاربران به آن اعتماد نمی‌کنند و از آن استفاده نمی‌کنند. | محدودیت‌های فناوری |
| تعصب در تصمیمات مبتنی بر داده | از جمله ریسک‌هایی که باید به آن‌ها توجه کنیم، کامل بودن داده‌ها است، تا برای تصمیمات و قضاوت‌ها مناسب باشد. | محدودیت‌های فناوری |
| مشکلات همخوانی | اگر ابزارها نتوانند با MYOB صحبت کنند، پس برای ما بسیار دشوار است که اصلاً از آن‌ها استفاده کنیم؛ زمان زیادی صرف کار دستی برای تنظیم و اصلاح داده‌ها می‌شود. | محدودیت‌های فناوری |
| استراتژی نوآوری | فکر می‌کنم شرکت بیشتر به سمت دیجیتال متمرکز شده است، از طریق تمام خطوط خدمات. بنابراین، استراتژی، دیجیتال را به عنوان یک حوزه کلیدی قرار داده است. | مدیریت نوآوری |
| سیاست نوآوری | پس از اینکه ایده‌ها مطرح می‌شوند، سیاستی برای پیگیری آن‌ها از طریق نهادهای مختلف ملی و جهانی وجود ندارد، تا به مرحله آزمایش برسند. | مدیریت نوآوری |
| نمایندگان ارتباطی | تیم من در تضمین، به شدت با معادل در کسب‌وکار مشاوره مالی ما کار می‌کند. | عوامل سازمانی |
| منابع شرکت | ما توانایی‌های قوی‌ای ساخته‌ایم که در واقع حسادت شبکه ماست. شما توسعه نرم‌افزار کامل دارید. | عوامل سازمانی |
| آمادگی هوش مصنوعی مدیریت | یکی از موانع پذیرش احتمالاً در سطح من در میز مشارکت است، زیرا آن‌ها به طور کامل نرم‌افزار را درک نمی‌کنند یا اینکه شواهد از آن چگونه استخراج می‌شود و به آن اعتماد ندارند. | آمادگی هوش مصنوعی |
| مهارت‌های دیجیتال کارکنان | ما برنامه بزرگی برای ارتقاء مهارت‌های دیجیتال در سراسر BIG اجرا کرده‌ایم. ما متوجه شدیم که سرمایه‌گذاری‌های در فناوری به طور کامل استفاده نخواهد شد مگر اینکه در مهارت‌های دیجیتال سرمایه‌گذاری کنیم. | آمادگی هوش مصنوعی |
| زیرساخت داده | حسابرسی در حال حرکت به سمت زیرساخت داده‌ای آماده است و احتمالاً باعث خواهد شد که آن‌ها تجربه خوبی از ابزار داشته باشند ... شرکت‌های بیشتری که به سرعت فناوری ما را اتخاذ می‌کنند. | آمادگی هوش مصنوعی |

منبع: یانگ و همکاران (۲۰۲۴)

ملاحظات اضافی نشان می‌دهد که استانداردسازی وظایف حسابداری و مالی می‌تواند به تسهیل فرایند اتوماسیون کمک کند و امکان استفاده گسترده‌تر از هوش مصنوعی را فراهم کند (سولانکی و همکاران، ۲۰۲۴: ۳). همچنین، تعصبات در داده‌ها از اهمیت بالایی برخوردار است و باید اطمینان حاصل شود که داده‌های استفاده‌شده برای آموزش هوش مصنوعی عاری از تعصبات هستند، زیرا هوش مصنوعی می‌تواند تعصبات موجود در داده‌ها را تکرار کند. در این

راستا، نظارت انسانی بر هوش مصنوعی نیز ضروری است تا اطمینان حاصل شود که به درستی کار می‌کند و تصمیمات نادرستی اتخاذ نمی‌کند. علاوه بر این، باید توسعه مستمر توانایی‌های کارکنان برای هماهنگی با تغییرات فناوری وجود داشته باشد. به طور کلی، هوش مصنوعی می‌تواند تأثیر قابل توجهی بر فعالیت‌های حسابرسان و شرکت‌های حسابرسی داشته باشد و با درک مزایا و چالش‌های بالقوه، شرکت‌های حسابرسی می‌توانند تصمیمات آگاهانه‌ای درباره اجرای هوش مصنوعی اتخاذ کنند (یانگ و همکاران، ۲۰۲۴: ۵).

## فرضیه‌ها

فرضیه اول: فناوری‌های نوظهور (هوش مصنوعی و اتوماسیون فرآیند رباتیک) کارایی فعالیت‌های حسابرسی را با خودکارسازی وظایف تکراری و ساختاریافته افزایش می‌دهند.

فرضیه دوم: فناوری‌های نوظهور(هوش مصنوعی و اتوماسیون فرآیند رباتیک) اثربخشی فعالیت‌های حسابرسی را با پشتیبانی از تصمیم‌گیری و تحلیل داده‌های پیچیده بهبود می‌بخشند.

فرضیه سوم: استقرار فناوری‌های نوظهور منجر به کاهش تعداد کارکنان سطح پایین در مؤسسات حسابرسی به دلیل خودکارسازی وظایف آنان می‌شود.

فرضیه چهارم: با گسترش فناوری‌های نوظهور، تقاضا برای حسابرسان دارای مهارت‌های فناوری اطلاعات و تحلیل داده‌ها به طور قابل توجهی افزایش می‌یابد.

فرضیه پنجم: سطح دیجیتالی‌شدن مشتریان حسابرسی یک عامل تعیین‌کننده در میزان و اثربخشی پذیرش فناوری‌های نوظهور توسط مؤسسات حسابرسی است.

## روش‌شناسی

این پژوهش با به‌کارگیری رویکرد ترکیبی متوالی اکتشافی و با هدف تبیین دقیق سازوکارهای تأثیر فناوری‌های دیجیتال بر حسابرسی طراحی شد. در فاز کیفی، از طریق ۱۴ مصاحبه نیمه‌ساختاریافته با خبرگان و تحلیل محتوای کیفی، ابعاد، مؤلفه‌ها و روابط اولیه مدل استخراج گردید. در فاز کمی، داده‌های ۳۰۰ پرسشنامه معتبر از حسابرسان مؤسسات بزرگ، متوسط و کوچک با روش نمونه‌گیری طبقه‌ای متناسب گردآوری شد. ابزار پژوهش، پرسشنامه‌ای محقق‌ساخته مبتنی بر مقیاس لیکرت پنج‌درجه‌ای بود که روایی آن با نظرات

خبرگان و تحلیل عاملی تأییدی و پایایی آن با آلفای کرونباخ و پایایی ترکیبی (مقادیر بین ۰/۸۲ تا ۰/۹۱) تأیید شد. برای تحلیل داده‌ها و آزمون فرضیه‌ها، از مدل‌سازی معادلات ساختاری مبتنی بر کوواریانس (CB-SEM) با استفاده از نرم‌افزار Amos28 بهره گرفته شد. پیش از تحلیل، آزمون هارمن تک‌عاملی انجام و مشخص شد که واریانس تبیین‌شده توسط اولین عامل (۴۲/۲٪) کمتر از آستانه ۵۰٪ است؛ بنابراین تورش روش مشترک تهدید جدی برای نتایج محسوب نمی‌شود. شاخص‌های برازش مطلق ($\chi^2/df$ = ۲/۱۸)، تطبیقی (CFI = ۰/۹۴) و ریشه میانگین مربعات خطا (RMSEA=۰/۶۰) همگی حاکی از برازش مطلوب مدل نهایی با داده‌ها بودند. با توجه به ماهیت مقطعی داده‌ها، در تفسیر نتایج از ادعای رابطه علّی مستقیم پرهیز شده و بر روابط معنی‌دار ساختاری تأکید گردید.

## یافته‌های پژوهش

جدول شماره ۲، آزمون هارمن تک‌عاملی برای بررسی تورش روش مشترک را نشان می‌دهد.

**جدول ۲**

*آزمون هارمن تک‌عاملی برای بررسی تورش روش مشترک*

| مؤلفه | مقدار ویژه اولیه | مجموع بارهای استخراج‌شده مجذور | درصد واریانس تبیین‌شده | درصد تجمعی واریانس |
|---|---|---|---|---|
| ۱ | ۱۲/۶۷ | ۱۲/۶۷ | ٪۴۲/۲۳ | ٪۴۲/۲۳ |
| ۲ | ۲/۸۵ | ۱۵/۵۲ | ٪۹/۵۰ | ٪۵۱/۷۳ |
| ۳ | ۱/۹۱ | ۱۷/۴۳ | ٪۶/۳۷ | ٪۵۸/۱۰ |
| ۴ | ۱/۴۲ | ۱۸/۸۵ | ٪۴/۷۳ | ٪۶۲/۸۳ |
| ۵ | ۱/۱۸ | ۲۰/۰۳ | ٪۳/۹۳ | ٪۶۶/۷۶ |

برای بررسی احتمال وجود تورش روش مشترک ناشی از استفاده از پرسشنامه خوداظهاری، آزمون هارمن تک‌عاملی انجام شد. نتایج نشان داد که اولین عامل بدون چرخش تنها ۴۲/۲۳٪ از واریانس کل سازه‌ها را تبیین می‌کند. این مقدار زیر آستانه معیار ۵۰٪ است که نشان‌دهنده

عدم غلبه یک عامل واحد بر داده‌ها می‌باشد. بنابراین می‌توان نتیجه گرفت که تورش روش مشترک در این پژوهش تهدید جدی برای اعتبار درونی یافته‌ها محسوب نمی‌شود. این امر امکان تحلیل‌های بعدی مبتنی بر ساختار چندعاملی را فراهم می‌سازد و از قابلیت اعتماد نتایج حاصل از مدل‌سازی معادلات ساختاری پشتیبانی می‌کند. جدول شماره ۳، آمار توصیفی و ماتریس همبستگی پیرسون متغیرهای پژوهش را نشان می‌دهد.

**جدول ۳**

*آمار توصیفی و ماتریس همبستگی پیرسون متغیرهای پژوهش*

| متغیر | میانگین | انحراف معیار | ۱ | ۲ | ۳ | ٤ | ٥ |
|---|---|---|---|---|---|---|---|
| ۱. استفاده از RPA | ۳/۸۷ | ۰/۹۱ | ۱ | | | | |
| ۲. استفاده از هوش مصنوعی | ۳/۹۲ | ۰/۸۸ | ۰/۶۵ | ۱ | | | |
| ۳. کارایی حسابرسی | ۴/۱۸ | ۰/۷۹ | ۰/۶۳ | ۰/۷۱ | ۱ | | |
| ۴. اثربخشی حسابرسی | ۴/۰۵ | ۰/۸۳ | ۰/۵۸ | ۰/۷۸ | ۰/۷۴ | ۱ | |
| ۵. دیجیتالی‌شدن مشتری | ۴/۱۲ | ۰/۸۲ | ۰/۶۱ | ۰/۶۹ | ۰/۶۷ | ۰/۷۶ | ۱ |

تمامی ضرایب همبستگی در سطح ۰/۰۱ معنی‌دار هستند ($p < 0.01$)

آمار توصیفی و ماتریس همبستگی میان متغیرهای پژوهش نشان می‌دهد که تمامی سازه‌ها از میانگین بالاتر از میانگین نظری (۳) برخوردارند که نشان‌دهنده موضع مثبت پاسخ‌دهندگان نسبت به هریک از ابعاد مورد سنجش است. ضرایب همبستگی مثبت و معنی‌دار بین همه جفت متغیرها حاکی از وجود روابط خطی سازگار با مدل مفهومی پژوهش است. بالاترین همبستگی مشاهده‌شده بین هوش مصنوعی و اثربخشی (۰/۷۸) و پس از آن بین دیجیتالی‌شدن مشتری و اثربخشی (۰/۷۶) می‌باشد که مبین نقش کلیدی این دو متغیر در تحول فرایند حسابرسی است. این الگوی همبستگی از یکپارچگی درونی داده‌ها و تناسب آن‌ها برای تحلیل‌های چندمتغیره پیشرفته حمایت می‌کند. جدول شماره ۴، شاخص‌های برازش مدل معادلات ساختاری (CB-SEM) را نشان می‌دهد.

**جدول ٤**

*شاخص‌های برازش مدل معادلات ساختاری (CB-SEM)*

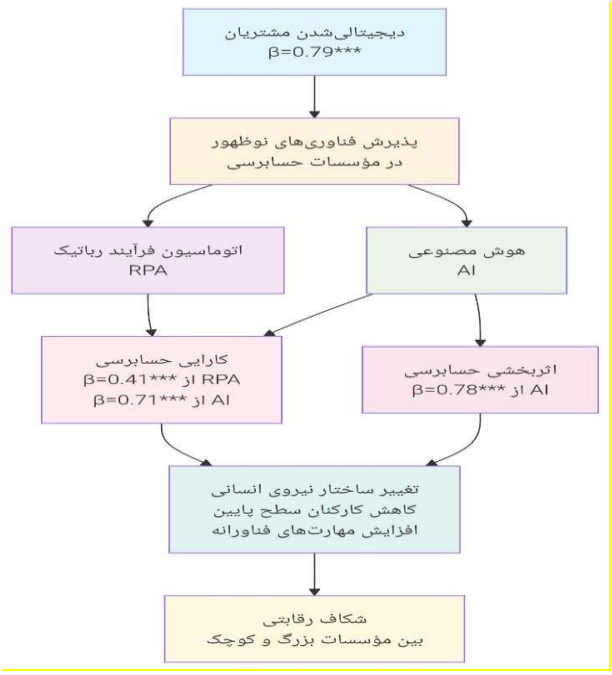
| شاخص برازش | مقدار بدست‌آمده | مقدار مطلوب | نتیجه |
|---|---|---|---|
| $\chi^2/df$ | ۲/۱۸ | ۳ > | مطلوب |
| CFI | ۰/۹۴ | ۰/۹۰ | مطلوب |
| TLI | ۰/۹۲ | ۰/۹۰ | مطلوب |
| RMSEA | ۰/۰۶ | ۰.۰۸ > | مطلوب |
| SRMR | ۰/۰۵ | ۰.۰۸ > | مطلوب |

برای ارزیابی برازش کلی مدل پژوهش، از شاخص‌های متعددی استفاده شد. نسبت کای‌دو به درجه آزادی (۲/۱۸) در دامنه قابل قبول قرار دارد. شاخص‌های CFI و TLI به ترتیب ۰/۹۴ و ۰/۹۲ هستند که هر دو فراتر از آستانه ۰/۹۰ می‌باشند. شاخص RMSEA نیز با مقدار ۰/۰۶ و SRMR با مقدار ۰/۰۵، هر دو نشان‌دهنده خطای برازش پایین هستند. مجموع این شواهد حاکی از برازش مطلوب و قابل قبول مدل ساختاری با داده‌های مشاهده‌شده است. این نتیجه، امکان تفسیر معنی‌دار پارامترهای مدل و آزمون فرضیه‌های پژوهش را فراهم می‌سازد و پایه‌ای مستحکم برای استنتاج‌های بعدی ایجاد می‌کند.

## مدل ساختاری پژوهش: تأثیر فناوری‌های نوظهور بر حسابرسی

مدل ساختاری پژوهش حاضر مبتنی بر تحلیل معادلات ساختاری (CB-SEM) طراحی شده و روابط بین شش سازه کلیدی را بررسی می‌کند. در این مدل، دیجیتالی‌شدن مشتریان به عنوان عامل محرک بیرونی با ضریب مسیر ۰/۷۹ بر پذیرش فناوری‌های نوظهور در مؤسسات حسابرسی تأثیر می‌گذارد. این پذیرش به نوبه خود موجب به‌کارگیری اتوماسیون فرآیند رباتیک و هوش مصنوعی می‌شود. هوش مصنوعی با ضریب ۰/۷۱ بر کارایی حسابرسی و با ضریب ۰/۷۸ بر اثربخشی حسابرسی تأثیر مستقیم و معناداری دارد، در حالی که اتوماسیون فرآیند رباتیک تنها بر کارایی (ضریب ۰/۴۱) اثرگذار است. بهبود کارایی و اثربخشی منجر به تغییر ساختار نیروی انسانی (کاهش نیروی سطح پایین و افزایش تقاضا برای مهارت‌های فناورانه)

و در نهایت تشدید شکاف رقابتی بین مؤسسات بزرگ و کوچک می‌شود. کلیه ضرایب مسیر در سطح ۰/۰۱ معنادار بوده و شاخص‌های برازش مدل (CFI=۰/۹۴، RMSEA=۰/۰۶) حاکی از برازش مطلوب آن با داده‌هاست. جدول شماره ۵، ضرایب مسیر استاندارد (β) و معنی‌داری را نشان می‌دهد.




**شکل ۱.** مدل ساختاری پژوهش

نتایج تحلیل مسیر در مدل نهایی نشان می‌دهد که کلیه مسیرهای فرضیه‌شده از نظر آماری معنی‌دار هستند ( P < ۰/۰۱). قوی‌ترین رابطه به تأثیر دیجیتالی‌شدن مشتری بر پذیرش فناوری ( β = ۰/۷۹) و سپس تأثیر هوش مصنوعی بر اثربخشی حسابرسی (β = ۰/۷۸) تعلق دارد. این یافته‌ها نه تنها بر نقش محوری محیط بیرونی (مشتریان) در تحول دیجیتالی مؤسسات حسابرسی تأکید می‌کنند، بلکه بر برتری نسبی هوش مصنوعی نسبت به اتوماسیون فرآیند رباتیک در ارتقای جنبه‌های قضاوتی و تحلیلی حرفه نیز صحه می‌گذارند. لازم به ذکر است

که با توجه به ماهیت مقطعی داده‌ها، این روابط همبستگی قوی را نشان می‌دهند و دلالت بر رابطه علّی قطعی نمی‌کنند.

**جدول ۵**

*ضرایب مسیر استاندارد (β) و معنی‌داری*

| مسیر | ضریب مسیر (β) | آماره T | سطح معنی‌داری (p) | نتیجه |
|---|---|---|---|---|
| RPA ← کارایی حسابرسی | ۰/۴۱ | ۶/۸۴ | ۰/۰۰۰ | تایید |
| هوش مصنوعی ←کارایی حسابرسی | ۰/۷۱ | ۱۱/۵۲ | ۰/۰۰۰ | تایید |
| هوش مصنوعی ←اثربخشی حسابرسی | ۰/۷۸ | ۱۲/۳۱ | ۰/۰۰۰ | تایید |
| دیجیتالی‌شدن مشتری ←پذیرش فناوری | ۰/۷۹ | ۱۲/۸۸ | ۰/۰۰۰ | تایید |
| پذیرش فناوری ←تغییر ساختار نیروی انسانی | ۰/۶۸ | ۱۰/۹۵ | ۰/۰۰۰ | تایید |

## نتیجه‌گیری

پژوهش حاضر با هدف تحلیل تأثیر فناوری‌های دیجیتال نوظهور ـ به‌ویژه هوش مصنوعی و اتوماسیون فرآیند رباتیک ـ بر کارایی، اثربخشی، ساختار نیروی انسانی و شکاف رقابتی مؤسسات حسابرسی ایران انجام شد. یافته‌های کمی و کیفی این مطالعه، که مبتنی بر یک چارچوب نظری ترکیبی و با به‌کارگیری روش مدل‌سازی معادلات ساختاری (CB-SEM) تحلیل شدند، نشان‌دهنده تحولی عمیق و چندبعدی در حرفه حسابرسی تحت تأثیر این فناوری‌هاست. مدل نهایی پژوهش که برازش مطلوبی با داده‌ها داشت، روابط ساختاری معناداری بین متغیرهای کلیدی را تأیید کرد. نتایج نشان داد که فناوری‌های نوظهور به‌طور معناداری کارایی فرآیند حسابرسی را افزایش می‌دهند. این یافته به‌ویژه با توجه به ضریب مسیر قوی هوش مصنوعی (β = ۰/۷۱) و اتوماسیون فرآیند رباتیک (β = ۰/۴۱) بر کارایی، قابل تبیین است. این نتیجه با پژوهش‌های پیشین همچون موفیت و همکاران (۲۰۱۸) و

لاکویورزانو (۲۰۲۰) همسو است که بر نقش خودکارسازی در تسریع وظایف تکراری و کاهش خطاهای دستی تأکید داشتند. در بعد اثربخشی، هوش مصنوعی با ضریب مسیر ۰/۷۸ قوی‌ترین نقش را در بهبود کیفیت قضاوت حرفه‌ای و تحلیل داده‌های پیچیده ایفا کرد. این امر حاکی از آن است که هوش مصنوعی فراتر از یک ابزار کمکی، به یک «همکار تحلیلی» تبدیل شده که عمق و دقت ارزیابی‌های حسابرس را ارتقاء می‌دهد. چنین نقشی با چارچوب نظری «حسابرسی شناختی» و مطالعاتی مانند ژانگ و همکاران (۲۰۲۲) سازگار است که بر قابلیت‌های پیشرفته تحلیلی هوش مصنوعی تأکید می‌کنند.

یکی از یافته‌های ساختاری مهم، تأثیر فناوری بر ترکیب نیروی انسانی بود. مطابق با فرضیه سوم، استقرار این فناوری‌ها با کاهش معنادار تعداد کارکنان سطح پایین همراه بود ($\beta$ = ۰/۵۲) برای اتوماسیون وظایف. این تحول، بازتابی از جایگزینی وظایف روتین و ساختاریافته توسط ربات‌های نرم‌افزاری است، پدیده‌ای که در ادبیات جهانی تحت عنوان «جابجایی شغلی ناشی از اتوماسیون» مورد بحث قرار گرفته است. در مقابل، همان‌طور که فرضیه چهارم تأیید کرد، تقاضا برای حسابرسان دارای مهارت‌های فناوری اطلاعات و تحلیل داده به‌طور چشمگیری افزایش یافته است (میانگین ۴/۳۰). این دوگانگی، گذار حرفه از مدل سنتی مبتنی بر نیروی کار انبوه به مدل نوین مبتنی بر تخصص‌گرایی فناورانه را نشان می‌دهد. این یافته با دیدگاه یانگ و همکاران (۲۰۲۴) همخوانی کامل دارد که آینده حسابرسی را در گرو ادغام مهارت‌های حرفه‌ای با سواد دیجیتال می‌دانند. از منظر محیطی، یافته‌ها به وضوح نقش محوری دیجیتالی‌شدن مشتریان را به عنوان عامل تعیین‌کننده در پذیرش فناوری توسط مؤسسات حسابرسی آشکار ساخت ($\beta$ = ۰/۷۹). این نتیجه، از نظریه وابستگی به محیط پشتیبانی می‌کند و نشان می‌دهد که فشار نهادهای بیرونی (به‌ویژه مشتریان پیشرو) می‌تواند محرک قوی‌تری برای نوآوری دیجیتالی نسبت به انگیزه‌های درونی باشد. در واقع، مؤسسات حسابرسی برای حفظ ارتباط مؤثر با مشتریانی که از سیستم‌های یکپارچه‌ای مانند برنامه‌ریزی منابع سازمانی و پلتفرم‌های داده‌محور استفاده می‌کنند، ناگزیر به هم‌تکاملی فناورانه هستند. این تحولات، اگرچه فرصت‌های بی‌سابقه‌ای برای افزایش شفافیت، دقت و ارزش‌آفرینی در حسابرسی ایجاد می‌کنند، اما با چالش‌ها و پیامدهای مهمی همراه هستند. اولاً، یافته‌ها حاکی

از تعمیق شکاف رقابتی بین مؤسسات بزرگ و کوچک حسابرسی است. مؤسسات بزرگ با برخورداری از منابع مالی بیشتر، دسترسی بهتری به فناوری‌های پیشرفته داشته و می‌توانند نیروهای متخصص جذب کنند، در حالی که مؤسسات کوچک و متوسط ممکن است در تأمین سرمایه اولیه و توسعه مهارت‌ها با مانع مواجه شوند. این امر می‌تواند به تدریج به تمرکز بازار و کاهش تنوع در ارائه خدمات حسابرسی بینجامد. راه‌حل‌هایی مانند تشکیل کنسرسیوم‌های فناوری، برون‌سپاری سکوهای تحلیلی، یا تدوین استانداردهای حمایتی توسط نهادهای حرفه‌ای می‌تواند به تعدیل این شکاف کمک کند. ثانیاً، چالش‌های اخلاقی و حرفه‌ای جدیدی مطرح می‌شود. مسئله «جعبه سیاه» در الگوریتم‌های هوش مصنوعی، امکان وجود تعصب در داده‌های آموزشی، و کاهش قابلیت ردیابی تصمیم‌ها، می‌تواند استقلال و اعتبار حرفه‌ای حسابرسی را تحت تأثیر قرار دهد. بنابراین، توسعه چارچوب‌های نظارتی و اخلاقی مختص فناوری‌های نوظهور در حساب، تدوین استانداردهای حسابرسی دیجیتال، و تقویت سواد فناورانه حسابرسان برای ارزیابی نقدی سیستم‌های هوشمند، به یک ضرورت تبدیل می‌شود.

این پژوهش با محدودیت‌هایی روبرو بوده است که مسیرهایی برای پژوهش‌های آینده می‌گشاید. نخست، با توجه به مقطعی بودن داده‌ها، روابط کشف‌شده علی نیستند و تنها همبستگی قوی را نشان می‌دهند. انجام مطالعات طولی می‌تواند تأثیرات بلندمدت فناوری بر تحول شغل حسابرسی و پویایی شکاف رقابتی را روشن‌تر کند. دوم، نمونه‌گیری در ایران انجام شده و تعمیم نتایج به سایر بافت‌های فرهنگی-اقتصادی نیازمند احتیاط است. مطالعات تطبیقی بین کشورهای در حال توسعه و توسعه‌یافته می‌تواند نقش عوامل نهادی و زیرساختی را شفاف‌تر سازد. سوم، این پژوهش فناوری را یک کل یکپارچه در نظر گرفت. پژوهش‌های آتی می‌توانند به بررسی تفصیلی تأثیرات گونه‌های مختلف هوش مصنوعی (مانند پردازش زبان طبیعی، بینایی ماشین) یا الگوهای مختلف استقرار (خرید سکو، توسعه درون‌سازمانی) بپردازند. در نهایت، می‌توان نتیجه گرفت که فناوری‌های دیجیتال نوظهور در حال تبدیل حسابرسی از یک حرفه مبتنی بر نمونه‌گیری و قضاوت تجربی به یک رشته مبتنی بر تحلیل تمام‌نگر داده‌ها و همکاری انسان-ماشین هستند. این گذار، تنها منحصر به اتوماسیون فرآیندها

نیست، بلکه بازتعریف ماهیت مهارت‌ها، ساختار سازمانی، مدل‌های کسب‌وکار و انتظارات ذی‌نفعان را در بر دارد. موفقیت در این مسیر مستلزم عزم سه‌جانبه است: از سوی نهادهای حرفه‌ای و سیاست‌گذار برای به‌روزرسانی استانداردها و ایجاد زیرساخت‌های اشتراکی؛ از سوی مؤسسات حسابرسی برای سرمایه‌گذاری راهبردی در فناوری و بازآموزی نیروی انسانی؛ و از سوی مراکز آموزشی برای بازطراحی اساسی برنامه‌های درسی و تربیت نسل جدید حسابرسان دیجیتال. تنها با چنین نگرش پیش‌دستانه و جامعی می‌توان چالش‌های این تحول اجتناب‌ناپذیر را به فرصت‌هایی برای ارتقای اعتبار، کارایی و ارزش اجتماعی حرفه حسابرسی تبدیل کرد.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## References

Abdolmohammadi, M. J. (1999). A comprehensive taxonomy of audit task structure, professional rank, and decision aids for behavioral research. *Behavioral Research in Accounting*, *11*, 51–92.

Afsay, A., Tahriri, A., & Rezaee, Z. (2023). A meta-analysis of factors affecting acceptance of information technology in auditing. *International Journal of Accounting Information Systems*, *49*, 100608. https://doi.org/10.1016/j.accinf.2022.100608

Alassuli, A. (2025). Impact of artificial intelligence using the robotic process automation system on the efficiency of internal audit operations at Jordanian commercial banks. *Banks and Bank Systems*, *20*(1), 122–135. https://doi.org/10.21511/bbs.20(1).2025.11

Ashraf, M. (2024). Does automation improve financial reporting? Evidence from internal controls. *Review of Accounting Studies*, *30*(1), 436–479. https://doi.org/10.1007/s11142-024-09822-y

Bztaş, A., Gujrati, R., Kapr, D., Tambuskar, S., Ganguly, I., Singh, K., Shaw, M., Beg, M. S., Nair, A., Uygun, H., Wadhawa, S., Kaushik, M., Srivastava, Y. Y., Singh, A., & Narang, T. (2025). Emerging technology & innovation: Digital transformation with sustainable development. *In AI for Human-Centered Transformation.* Editorial Alumni. https://doi.org/10.37497/alimni.inbks

Dahabiyeh, L., & Mwafi, A. (2023). Challenges of using RPA in auditing: A sci-technical systems approach. *Intelligent Systems in Accounting, Finance and Management*, *30*(2), 76–86. https://doi.org/10.1002/isaf.1537

Dahiyat, A. (2022). Robotic process automation and audit quality. *Corporate Governance and Organizational Behavior Review*, *6*(1), 160–167. https://doi.org/10.22495/cgobrv6i1p12

Damerji, H., & Salimi, A. (2021). Mediating effect of use perceptions on technology readiness and adoption of artificial intelligence in accounting. *Accounting Education*, *30*(2), 107–130. https://doi.org/10.1080/09639284.2021.1872035

Dyball, M. C., & Seethamraju, R. (2021). Client use of blockchain technology: Exploring its (potential) impact on financial statement audits of Australian accounting firms. *Accounting, Auditing & Accountability Journal*, *35*(7).

Eulerich, M., Pawlowski, J., Waddups, N. J., & Wood, D. A. (2022). A framework for using robotic process automation for audit tasks. *Contemporary Accounting Research*, *39*(1), 691–720.

Eulerich, M., Waddups, N., Wagener, M., & Wood, D. A. (2024). The dark side of robotic process automation (RPA): Understanding risks and challenges with RPA. *Accounting Horizons*, *38*(2), 143–152. https://doi.org/10.2308/horizons-2022-019

Florea, A. (2024). The emerging technologies: The drivers for digital transformation in business and education. *International Journal of Advanced Statistics and IT&C for Economics and Life Sciences*, 14(1), 213–221. https://doi.org/10.2478/ijasitels-2024-0019

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerization? *Technological Forecasting and Social Change*, *114*, 254–280.

Gajjar, N., Rathod, K., & Jani, K. (2022). A systematic literature review on robotic process automation security (Version 1). *arXiv*. https://doi.org/10.48550/arXiv.2212.05544

Hazar, H., & Toplu, C. (2023). The use of robotic process automation in accounting. *Prizren Social Science Journal*, *7*(3), 45–50. https://doi.org/10.32936/pssj.v7i3.481

Horvat, D., Ivanišević, R., & Gluščević, L. (2024). Risks associated with robotic process automation. *Journal of Project Management in New Technologies*. https://doi.org/10.5937/jpmnt12-50617.

Huang, F., & Vasarhelyi, M. A. (2019). Applying robotic process automation (RPA) in auditing: A framework. *International Journal of Accounting Information Systems*, *35*, 100433. https://doi.org/10.1016/j.accinf.2019.100433

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting*, *13*(2), 1–20.

Kokina, J., Gilleran, R., Blanchette, S., & Stoddard, D. (2021). Accountant as digital innovator: Roles and competencies in the age of automation. *Accounting Horizons*, *35*(1), 153–184.

Lacurezeanu, R., Tiron-Tudor, A., & Bresfelean, V. P. (2020). Robotic process automation in audit and accounting. *Audit Financiar*, *18*(160), 752–770. https://doi.org/10.20869/auditf/2020/160/024

Liu, S. L. (2022). Robotic process automation (RPA) in auditing: A commentary. *International Journal of Computer Auditing*, *4*(1), 22–27. https://doi.org/10.53106/256299802022120401003

Mffitt, K. C., Rozari, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. *Journal of Emerging Technologies in Accounting*, *15*(1), 1–10. https://doi.org/10.2308/jeta-10589

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics*, *167*(2), 209–234. https://doi.org/10.1007/s10551-019-04407-1

Muqattash, R., Qasim, A., & Kharbat, F. (2024). Exploring the impact of robotic process automation and artificial intelligence technologies on the auditing profession. In *Global Congress on Emerging Technologies (GCET-2024)* (pp. 132–137). https://doi.org/10.1109/gcet64327.2024.10934349

Patjshi, P. K., Majaz Ahmad Khan, B., S. M., Inumula, K. M., Sharma, K., & Mittal, P. (2025). Digital transformation in management: Leveraging emerging technologies for enhanced business financial operations. In *2025 6th International Conference for Emerging Technology (INCET)* (pp. 1–6). https://doi.org/10.1109/incet64471.2025.11140452

Perdana, A., Lee, W. E., & Mui Kim, C. (2023). Prototyping and implementing robotic process automation in accounting firms: Benefits, challenges, and opportunities for audit automation. *International Journal of Accounting Information Systems*, *51*, 100641. https://doi.org/10.1016/j.accinf.2023.100641

Richins, G., Stapleton, A., Stratpuls, T. C., & Wang, C. (2017). Big data analytics: Opportunity or threat for the accounting profession? *Journal of Information Systems*, *31*(3), 63–79.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Solanki, U., Mehta, K., & Shukla, V. K. (2024). Robotic process automation and audit quality: A comprehensive analysis. In *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (pp. 1–4). https://doi.org/10.1109/icrito61523.2024.10522375

Tetteh, S. G., Agyeman, A. Y., & Mhammed-Nurudeen, S. (2025). Engineering Ghana's future: The impact of emerging technologies and digital transformation. *Journal of Engineering Research and Reports*, *27*(5), 54–71. https://doi.org/10.9734/jerr/2025/v27i51492

Vincent, N. E., Igu, A., & Burns, M. B. (2020). Preparing for the robots: A proposed course in robotic process automation. *Journal of Emerging Technologies in Accounting*, *17*(2), 75–91. https://doi.org/10.2308/jeta-2020-020

Vitali, S., & Giuliani, M. (2024). Emerging digital technologies and auditing firms: Opportunities and challenges. *International Journal of Accounting Information Systems*, *53*, 100676. https://doi.org/10.1016/j.accinf.2024.100676

Vitharanage, I., & Thibbotuwawa, A. (2021). Enterprise robotic process automation. *Bolgoda Plains*, *1*(1), 10–12. https://doi.org/10.31705/bprm.2021.2

Wang, R., Liu, J., Zhao, W., Li, S., & Zhang, D. (2025). Automating financial statement audits with large language models (Version 1). *arXiv*. https://doi.org/10.48550/arXiv.2506.17282

Warner, K. S., & Wager, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3), 326–349.

Yang, J., Blount, Y., & Amrollahi, A. (2024). Artificial intelligence adoption in a professional service industry: A multiple case study. *Technological Forecasting and Social Change*, 201, 123251. https://doi.org/10.1016/j.techfore.2024.123251.

Zhang, C., Cho, S., & Vasarhelyi, M. (2022). Explainable Artificial Intelligence (XAI) in auditing. *International Journal of Accounting Information Systems*, *46*, Article 100572. https://doi.org/10.1016/j.accinf.2022.100572.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Review Paper**

# Opportunities and Challenges of Artificial Intelligence in Enhancing Financial Reporting Quality: A Systematic Review of Existing Studies [1]

**Gholamhossein Mikaeilou [*2] and Mahmood Nasiri[3]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 333-370

Received: 2026.08.14
Revised: 2026.09.27
Accepted: 2026.10.27

## Abstract

The aim of this study is to examine the opportunities and challenges associated with artificial intelligence in enhancing the quality of financial reporting. The research was conducted using a systematic review methodology. The study population comprises all articles published in reputable domestic journals regarding artificial intelligence and financial reporting Published between 2018 and 2025. The sample consisted of 30 articles, which were selected and analyzed using a purposive approach following a multi-stage screening process.The results of the systematic review and qualitative content analysis of the articles were were organized into two overarching categories: opportunities and challenges regarding the role of artificial intelligence in enhancing the quality of financial reporting. In the opportunities section, 8 global themes, 22 organizing themes, and 90 basic themes were identified; in the challenges section, 4 global themes, 9 organizing themes, and 30 basic themes were identified. The global themes within the opportunities section include the smartening of accounting and financial reporting processes, enhancing the quality and reliability of financial information, intelligent data analysis and financial forecasting, risk management and financial fraud and security, improving decision-making and financial performance, professional transformation and innovation in accounting, increasing transparency and accountability, and accelerating data analysis and financial reporting. The challenges identified include security, privacy and data governance, ethical and legal issues, human resource Provision and retraining, as well as economic and implementation hurdles. To effectively leverage artificial intelligence opportunities in financial reporting, it is essential to train and develop the workforce and invest in technological infrastructure.

**Keywords**: Opportunities and Challenges, Artificial Intelligence, Financial Reporting Quality.

**JEL classification:** *M4.*

---

[1] https://doi.org/10.22034/JISTA.2026.596973.1096
[1] Selected paper of the 2nd National Conference on Corporate Governance and Information Technology Risk Management
[2] M.Sc. Student in Accounting, University of Zanjan, Zanjan, Iran. (Corresponding Author). Email: ghh.m@znu.ac.ir
[3] Assistant Professor, Ph.D. in Accounting, University of Zanjan, Zanjan, Iran. Email: Ac.mahmood@znu.ac.ir

## 1. INTRODUCTION

The primary objective of financial reporting is to provide relevant information to facilitate effective decision-making (Hosseini, Jabbarzadeh Kangarlouei, & Bahri Sales, 2021). One tool that can be effective in this regard is the use of Artificial intelligence(AI) in financial reporting. Information technology systems offer greater accuracy and efficiency in data management and internal controls, thereby influencing the quality of financial reporting (Choudhary, Sigler, & Ramdas, 2022).

Numerous studies have been conducted on the opportunities and challenges associated with AI and financial reporting quality, each highlighting various advantages and disadvantages. However, this research aims to synthesize and analyze these findings through a systematic review, identifying the overarching or core themes regarding the opportunities and challenges of AI in the context of financial reporting quality.

## 2. MATERIALS AND METHODS

This research is descriptive in nature and, based on its execution method, is classified as a systematic study. The statistical population comprises all valid research articles published in the fields of artificial intelligence and financial reporting Published between 2018 and 2025 (Solar Hijri calendar). The study sample was selected from all articles published within this timeframe following a screening process that involved reviewing titles and abstracts. Once the final articles were selected, the data gathered from them were coded in three stages: first, initial codes were identified; next, organizing themes were extracted; and finally, global themes were derived.

## 3. RESULTS AND DISCUSSION

After reviewing the results of the selected articles, the research findings regarding the opportunities and challenges of artificial intelligence in enhancing the quality of financial reporting were categorized as shown in the chart below.

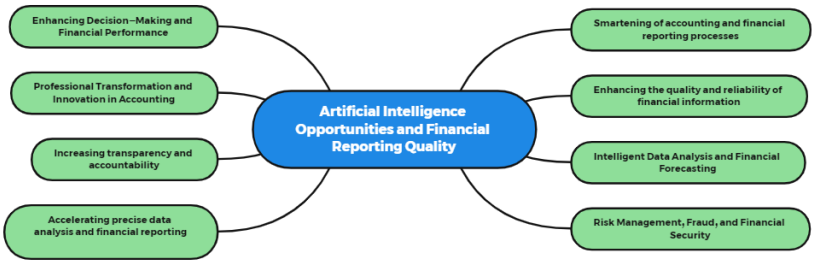



**Figure 1.** Artificial Intelligence Opportunities and Financial Reporting Quality




**Figure 2.** Artificial Intelligence Challenges and Financial Reporting Quality

## 4. CONCLUSION

The results of this systematic review indicate that artificial intelligence, as one of the most significant transformative technologies, holds substantial potential to enhance financial reporting in accounting and auditing; however, its effective utilization requires the simultaneous management of the associated opportunities and challenges. The research findings revealed that the opportunities presented by AI in financial reporting can be categorized into eight overarching themes: the intelligentization of accounting and financial reporting processes; the enhancement of financial information quality and reliability; intelligent data analysis and financial forecasting; risk management, fraud detection, and financial security; the improvement of decision-making and financial performance; professional transformation and innovation in accounting; increased transparency and accountability; and the acceleration of accurate data analysis and financial reporting. These findings indicate that AI is not merely a tool for automating repetitive tasks; rather, by accelerating information processing, enhancing the accuracy and quality of financial reports,

strengthening predictive capabilities, and improving risk management and fraud detection, it paves the way for more informed decision-making by managers, investors, and other stakeholders. Furthermore, by shifting the accountant's role from operational tasks to analytical, advisory, and strategic functions, this technology can transform the accounting profession and enhance value creation for organizations.

Conversely, the findings indicate that the deployment and development of AI in financial reporting entail significant challenges, which can be categorized into four overarching themes: security, privacy, and data governance; ethical and legal issues; human resource acquisition and retraining; and economic and implementation challenges. These challenges demonstrate that successful AI adoption depends not merely on developing technological infrastructure but also requires establishing appropriate legal and ethical frameworks, ensuring data security and confidentiality, investing in the training and empowerment of human capital, and securing the financial resources necessary for the technology's implementation and maintenance.Otherwise, risks such as privacy breaches, cybersecurity threats, bias in AI outputs, a shortage of skilled personnel, and high implementation costs could diminish the effectiveness of this technology.

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

**مقالهٔ ترویجی**

# فرصت‌ها و چالش‌های هوش مصنوعی در ارتقاء کیفیت گزارشگری مالی: مرور نظام‌مند مطالعات موجود[1]

**غلامحسین میکائیلو*[2] و محمود نصیری[3]**

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۳۳۳ - ۳۷۰

تاریخ دریافت: ۱۴۰۵/۰۵/۲۳
تاریخ بازنگری: ۱۴۰۵/۰۷/۰۵
تاریخ پذیرش: ۱۴۰۵/۰۸/۰۵

## چکیده

*هدف پژوهش، بررسی فرصت‌ها و چالش‌های هوش مصنوعی در ارتقای کیفیت گزارشگری مالی است. این پژوهش با روش مرور نظام‌مند انجام شده است. جامعه پژوهش شامل تمامی مقالات منتشرشده در مجلات معتبر داخلی در زمینه هوش مصنوعی و گزارشگری مالی طی سال‌های ۱۳۹۸ تا ۱۴۰۴ است. نمونه پژوهش شامل ۳۰ مقاله بود که به‌صورت هدفمند و پس از غربالگری در مراحل مختلف انتخاب و تحلیل شدند. نتایج مرور نظام‌مند و تحلیل کیفی محتوای مقالات در دو بخش فرصت‌ها و چالش‌های هوش مصنوعی در ارتقای کیفیت گزارشگری مالی دسته‌بندی شد. در بخش فرصت‌ها، ۸ مضمون فراگیر، ۲۲ مضمون سازمان‌دهنده و ۹۰ مضمون پایه و در بخش چالش‌ها، ۴ مضمون فراگیر، ۹ مضمون سازمان‌دهنده و ۳۰ مضمون پایه شناسایی شد. مضامین فراگیر بخش فرصت‌ها شامل هوشمندسازی فرایندهای حسابداری و گزارشگری مالی؛ ارتقای کیفیت و قابلیت اتکای اطلاعات مالی؛ تحلیل هوشمند داده‌ها و پیش‌بینی مالی؛ مدیریت ریسک ، تقلب و امنیت مالی؛ ارتقای تصمیم‌گیری و عملکرد مالی؛ تحول حرفه‌ای و نوآوری در حسابداری؛ افزایش شفافیت و پاسخگویی؛ و تسریع در تحلیل داده‌ها و گزارشگری مالی است. در بخش چالش‌ها نیز امنیت، حریم خصوصی و حاکمیت داد ه ها؛ مسائل اخلاقی و حقوقی؛ تأمین منابع انسانی و بازآموزی آنها؛ و چالش‌های اقتصادی و پیاده‌سازی شناسایی شد. به منظور بهره گیری اثر بخش از فرصت های هوش مصنوعی در گزارشگری مالی، آموزش و توسعه مهارت‌های نیروی انسانی و سرمایه‌گذاری در زیرساخت‌های فناورانه ضروری است.*

**واژه‌های کلیدی:** *فرصت‌ها و چالش‌ها، هوش مصنوعی، کیفیت گزارشگری مالی.*

**طبقه‌بندی موضوعی:** *M4*

---

[1] https://doi.org/10.22034/JISTA.2026.596973.1096

[1] مقاله منتخب دومین همایش ملی حاکمیت شرکتی و مدیریت ریسک‌های فناوری اطلاعات

[2] دانشجوی کارشناسی ارشد حسابداری، دانشگاه زنجان، زنجان، ایران. (نویسنده مسئول). (ghh.m@znu.ac.ir)

[3] استادیار، دکتری حسابداری، دانشگاه زنجان، زنجان، ایران. (Ac.mahmood@znu.ac.ir)

**مقدمه**

گزارشگری مالی یکی از مهم‌ترین سازوکارهای ارتباطی میان واحدهای اقتصادی و استفاده‌کنندگان اطلاعات مالی است و نقش اساسی در فراهم‌کردن اطلاعات مربوط، قابل اتکا و به‌موقع برای تصمیم‌گیری‌های اقتصادی ایفا می‌کند. سرمایه‌گذاران، اعتباردهندگان، مدیران و سایر ذی‌نفعان برای ارزیابی عملکرد واحد تجاری، پیش‌بینی جریان‌های نقدی، سنجش ریسک و اتخاذ تصمیم‌های اقتصادی به اطلاعات مندرج در گزارش‌های مالی اتکا دارند. از این‌رو، کیفیت گزارشگری مالی، به‌عنوان یکی از مؤلفه‌های اساسی شفافیت و کارایی بازارهای مالی، همواره مورد توجه پژوهشگران و حرفه حسابداری بوده است (آذرسعید و رستمی،۱۴۰۲: ۸۷ ؛ حسینی و همکاران، ۱۴۰۰: ۱۲۹-۱۳۰). با این حال، افزایش حجم، سرعت و پیچیدگی داده‌های مالی در محیط کسب‌وکار امروز، روش‌های سنتی پردازش و گزارشگری اطلاعات را با محدودیت‌هایی مواجه کرده است.

توسعه فناوری‌های دیجیتال، سامانه‌های اطلاعاتی، داده‌کاوی، بلاک‌چین و به‌ویژه هوش مصنوعی؛ شیوه گردآوری، پردازش، تحلیل و ارائه اطلاعات مالی را دستخوش تحول کرده است (الحاتمی[1]، ۲۰۲۲). در این میان، هوش مصنوعی به دلیل توانایی پردازش حجم عظیمی از داده‌ها، شناسایی الگوها، یادگیری از داده‌های گذشته و انجام برخی فعالیت‌های تحلیلی و کمک کننده به امر تصمیم گیری، به یکی از مهم‌ترین فناوری‌های اثرگذار بر آینده حسابداری و گزارشگری مالی تبدیل شده است.

اهمیت استفاده از هوش مصنوعی در گزارشگری مالی از آن جهت است که این فناوری می‌تواند بخشی از محدودیت‌های روش‌های سنتی را کاهش دهد. پردازش سریع داده‌ها، افزایش دقت محاسبات، شناسایی ناهنجاری‌ها، کاهش خطاهای انسانی، بهبود کنترل‌های داخلی و فراهم‌کردن اطلاعات به‌موقع، از جمله فرصت‌هایی است که در ادبیات پژوهش برای استفاده از هوش مصنوعی در حوزه مالی و حسابداری مطرح شده است. مواچیکوکا[2] (۲۰۲۴: ۱۷۵۱)، در بررسی آثار هوش مصنوعی بر دقت گزارشگری مالی، بر ظرفیت این فناوری برای بهبود دقت و کارایی فرایند گزارشگری تأکید کرده است. همچنین سرسلی وکاداگیشویلی[3](۲۰۲۳: ۷۲)،

---

1. Al-Hattami
2. Mwachikoka
3. Sreseli & Kadagishvili

در یک مطالعه مروری، کاربردهای هوش مصنوعی در حسابداری و گزارشگری مالی را بررسی کرده و در کنار مزایای آن، به مسائل و چالش‌های مرتبط با استفاده از این فناوری اشاره کرده‌اند.آپویین[1](۲۰۲۴: ۴۵) نیز با تمرکز بر گزارشگری مالی و رعایت الزامات، هوش مصنوعی را دارای ظرفیت قابل توجهی برای ارتقای کارایی و کیفیت فرایندهای مالی دانسته، اما هم‌زمان موضوعاتی مانند ملاحظات اخلاقی، چالش‌های اجرایی و الزامات نظارتی را مورد توجه قرار داده است.

در پژوهش‌های داخلی نیز بر نقش فناوری‌های نوین در افزایش کارایی، کاهش خطا و هزینه و ارتقای شفافیت اطلاعات مالی تأکید شده است (احمدی و باغیشنی،۱۴۰۳: ۱).علاوه بر این، پژوهش‌های اخیر نشان می‌دهند که رابطه میان هوش مصنوعی و کیفیت گزارشگری مالی را نمی‌توان صرفاً از منظر افزایش سرعت یا کاهش خطا بررسی کرد. کیفیت گزارشگری مالی مفهومی چندبعدی است که ویژگی‌هایی مانند دقت، قابلیت اتکا، به‌موقع‌بودن، شفافیت و مربوط‌بودن اطلاعات را دربرمی‌گیرد. بنابراین، آثار هوش مصنوعی بر کیفیت گزارشگری مالی می‌تواند به شرایط استفاده از فناوری، کیفیت داده‌های ورودی، میزان نظارت انسانی، سطح مهارت کارکنان و الزامات محیط قانونی و حرفه‌ای وابسته باشد. به همین دلیل، یافته‌های مطالعات مختلف ممکن است بر ابعاد متفاوتی از فرصت‌ها و چالش‌های این فناوری تمرکز کرده باشند و تصویری پراکنده از وضعیت موجود ارائه دهند.

مرور مطالعات پیشین نشان می‌دهد که اگرچه پژوهش‌های متعددی به کاربرد هوش مصنوعی در حسابداری، حسابرسی، دقت گزارشگری مالی، رعایت الزامات و مسائل اخلاقی پرداخته‌اند، اما در میان مطالعات داخلی بررسی‌شده، پژوهش معتبر و مستقیمی که به‌صورت منسجم فرصت‌ها و چالش‌های هوش مصنوعی را در ارتباط با کیفیت گزارشگری مالی شناسایی و دسته‌بندی کرده باشد، مشاهده نشد.

بر این اساس، پژوهش حاضر با استفاده از روش مرور نظام‌مند مطالعات موجود، درصدد است پژوهش‌های انجام‌شده درباره هوش مصنوعی و کیفیت گزارشگری مالی را شناسایی، بررسی و دسته‌بندی کند و مهم‌ترین فرصت‌ها و چالش‌های مطرح‌شده در این مطالعات را استخراج نماید. نتایج این پژوهش می‌تواند ضمن کمک به توسعه ادبیات علمی موضوع، برای

---

[1]. Apooyin

پژوهشگران، مدیران، حسابداران، حسابرسان و سیاست‌گذاران در درک بهتر ظرفیت‌ها و محدودیت‌های استفاده از هوش مصنوعی برای ارتقای کیفیت گزارشگری مالی مفید باشد.

## مبانی نظری و پیشینه پژوهش

گزارشگری مالی یکی از مهم‌ترین ابزارهای ارتباطی واحد تجاری با استفاده‌کنندگان اطلاعات مالی است و فرایندی است که از طریق آن اطلاعات مربوط به وضعیت مالی، عملکرد مالی و جریان‌های نقدی واحد تجاری شناسایی، اندازه‌گیری، پردازش و در قالب صورت‌های مالی و سایر گزارش‌های مالی به استفاده‌کنندگان ارائه می‌شود. هدف اساسی گزارشگری مالی، فراهم کردن اطلاعات مالی مفید برای سرمایه‌گذاران، اعتباردهندگان و سایر استفاده‌کنندگان در تصمیم‌گیری‌های اقتصادی است(هیئت استانداردهای بین‌المللی حسابداری،۲۰۱۸)

کیفیت گزارشگری مالی را می‌توان میزان توانایی گزارش‌های مالی در ارائه اطلاعات مربوط، قابل اتکا، به موقع و صادقانه واقعیت‌های اقتصادی واحد تجاری دانست(هیئت استانداردهای بین‌المللی حسابداری،۲۰۱۸)؛ به‌گونه‌ای که استفاده‌کنندگان بتوانند بر اساس آن تصمیم‌های اقتصادی آگاهانه اتخاذ کنند. بنابراین،گزارشگری مالی باکیفیت باید علاوه بر انعکاس مناسب رویدادهای اقتصادی، اطلاعاتی شفاف، قابل فهم، به‌موقع و قابل مقایسه در اختیار استفاده‌کنندگان قرار دهد.

اهمیت کیفیت گزارشگری مالی را می‌توان از منظر نظریه نمایندگی و عدم تقارن اطلاعاتی تبیین کرد. هیلی و پالپود[1](۲۰۰۱) یکی از مهم‌ترین دلایل تقاضا برای گزارشگری و افشای شرکتی را عدم تقارن اطلاعاتی و وجود تضاد منافع میان مدیران و سرمایه‌گذاران می دانند. بنابراین، هر عاملی که بتواند فرآیند تولید، پردازش، کنترل و افشای اطلاعات مالی را دقیق‌تر، سریع‌تر و شفاف‌تر کند، بالقوه می‌تواند بر کیفیت گزارشگری مالی اثرگذار باشد.

تحولات فناوری اطلاعات در سال‌های اخیر، به‌ویژه ظهور هوش مصنوعی، فرایند تولید، پردازش و ارائه اطلاعات مالی را با تغییرات اساسی مواجه کرده است. هوش مصنوعی به مجموعه‌ای از فناوری‌ها و روش‌های محاسباتی اطلاق می‌شود که قابلیت انجام فعالیت‌هایی مانند

[1]. Healy & Palepu

یادگیری، تشخیص الگو، پردازش اطلاعات، پیش‌بینی و تصمیم‌گیری را با استفاده از داده‌ها فراهم می‌کنند.

به لحاظ نظری، می‌توان انتظار داشت که هوش مصنوعی از چند مسیر بر کیفیت گزارشگری مالی اثر بگذارد. نخست، خودکارسازی فرآیندها می‌تواند میزان دخالت دستی و در نتیجه احتمال برخی خطاهای انسانی را کاهش دهد. دوم، پردازش سریع و هم‌زمان داده‌ها می‌تواند به‌موقع‌بودن اطلاعات مالی را افزایش دهد. سوم، تحلیل پیشرفته داده‌ها می‌تواند شناسایی ناهنجاری‌ها، معاملات غیرعادی و الگوهای مشکوک را تسهیل کند. چهارم، استفاده از الگوریتم‌ها در کنترل و پردازش اطلاعات می‌تواند قابلیت استانداردسازی برخی فعالیت‌های گزارشگری را افزایش دهد. این آثار با ویژگی‌های کیفی اطلاعات مالی، به‌ویژه مربوط‌بودن، به‌موقع‌بودن، قابلیت تأیید و ارائه صادقانه، ارتباط مستقیم دارند (گادفری[1] و همکاران،۱۴۰۲: ۳۰۳-۳۱۹).

با وجود این فرصت‌ها، استفاده از هوش مصنوعی در گزارشگری مالی با چالش‌هایی نیز همراه است. در صورت نبود سازوکارهای کنترلی و نظارتی مناسب، همین فناوری می‌تواند منبعی برای ایجاد خطا، ابهام و تهدیدهای جدید در فرایند گزارشگری باشد. بر همین اساس، بررسی فرصت‌ها و چالش‌های هوش مصنوعی در کیفیت گزارشگری مالی، مستلزم توجه همزمان به ظرفیت‌های فناوری و محدودیت‌ها و الزامات استفاده از آن است.

بر مبنای مطالب نظری بیان شده، بررسی یافته‌های پژوهش‌های انجام‌شده می‌تواند شواهد تجربی لازم درباره فرصت‌ها و چالش‌های به‌کارگیری هوش مصنوعی در کیفیت گزارشگری مالی را فراهم سازد. ادونکور و همکاران[2](۲۰۲۴: ۱۷۲) در پژوهشی با عنوان »تأثیر هوش مصنوعی بر رویه های حسابداری و بررسی چگونگی تغییر روش های سنتی حسابداری و گزارشگری مالی« ، به این نتیجه دست یافتند که هوش مصنوعی، دقت و کارایی گزارشگری مالی را به طور چشمگیری بهبود می بخشد، وظایف تکراری را خودکار و تحلیل های پیش بینی را برای تصمیم گیری های استراتژیک تسهیل می کند.

---

1. Godfrey
2. Odonkor & et al

طبق نتایج پژوهش علی خانی و عطایی(۱۴۰۴: ۲۲۶) استفاده از فناوری بلاکچین در حسابداری می تواند به افزایش شفافیت و اطمینان در اطلاعات مالی منجر شود و به عنوان یک ابزار موثر در جلوگیری از تقلب و افزایش اعتماد سرمایه گذاران عمل کند.

عدنان حمود و همکاران (۱۴۰۴: ۵۳۵) در پژوهشی با عنوان « امکان سنجی بهره گیری از فناوری های نوین هوش مصنوعی در بهبود فرایندهای حسابرسی در کشور»، ابزارهای مبتنی بر هوش مصنوعی با پیش بینی مالی در زمان واقعی، تشخیص ناهنجاریها و کاهش خطاها، فرایند حسابرسی را بهبود می بخشند.

سرسلی و کاداگیشویلی(۲۰۲۳: ۷۲) توانایی تحلیل حجم عظیمی از داده‌های مالی و فراهم‌کردن اطلاعات در زمان مناسب را به عنوان مزایای استفاده از هوش مصنوعی در حسابداری و گزارشگری مالی مطرح کرده‌اند.

آذرسعید و رستمی (۱۴۰۲: ۸۷) در پژوهشی با عنوان «هوش مصنوعی و تصمیم‌گیری اخلاقی در حسابداری و حسابرسی»، نشان دادند که بی‌طرفی، حریم خصوصی، شفافیت، پاسخگویی و اعتمادپذیری مهم‌ترین چالش‌های اخلاقی مرتبط با استفاده از هوش مصنوعی در این حوزه هستند.

با وجود گسترش مطالعات داخلی و خارجی درباره کاربرد هوش مصنوعی در حسابداری، حسابرسی و گزارشگری مالی، بخش عمده این مطالعات بر یک یا چند کاربرد یا پیامد خاص تمرکز داشته و کمتر به بررسی همزمان فرصت‌ها و چالش‌های هوش مصنوعی در کیفیت گزارشگری مالی پرداخته‌اند. همچنین، جمع‌بندی و طبقه‌بندی نظام‌مند یافته‌های مطالعات موجود، به‌ویژه با تمرکز بر مطالعات انجام‌شده در ایران، محدود است؛ ازاین‌رو، پژوهش حاضر با رویکرد مرور نظام‌مند درصدد پر کردن این خلأ و ارائه تصویری جامع از فرصت‌ها و چالش‌های هوش مصنوعی در کیفیت گزارشگری مالی است.

## روش پژوهش

پژوهش حاضر از نوع توصیفی و از نظر روش اجرا، یک مطالعه مرور نظام‌مند (سیستماتیک) است. در این روش، مطالعات مرتبط متناسب با اهداف پژوهش شناسایی، غربالگری و ارزیابی شده و پس از بررسی، یافته‌های آنها استخراج و ترکیب می‌شوند (دی لو، ملنیچاک، ماری و

پلامر[1]، ۲۰۱۶). جامعه پژوهش شامل مقالات پژوهشی معتبر منتشرشده در مجلات داخلی در زمینه هوش مصنوعی و گزارشگری مالی طی سال‌های ۱۳۹۸ تا ۱۴۰۴ بوده است.

راهبرد جستجو بر اساس ترکیب واژه محوری «هوش مصنوعی» با مفاهیم مرتبط با فرصت‌ها، مزایا، ظرفیت‌ها، کاربردها، چالش‌ها و محدودیت‌های آن، و همچنین واژه‌ها و عبارات مرتبط با حوزه گزارشگری مالی، شامل «گزارشگری مالی»، «گزارشگری حسابداری»، «کیفیت اطلاعات مالی» و «کیفیت گزارشگری مالی»، طراحی و اجرا شد. بر این اساس، جستجودر پایگاه‌های اطلاعاتی داخلی، شامل مرکز اطلاعات علمی جهاد دانشگاهی، مگیران، نورمگز و سیویلیکا انجام گرفت.

در مرحله نخست جستجو، حدود ۲۱۲ مقاله شناسایی شد. پس از بررسی نتایج و حذف مطالعات تکراری، حدود ۶۳ مقاله کنار گذاشته شد. سپس در مرحله غربالگری عنوان و چکیده، حدود ۱۱۹ مقاله به دلیل نداشتن ارتباط مستقیم با عنوان پژوهش حذف و در نهایت ۳۰ مقاله که بیشترین ارتباط مستقیم و غنای محتوایی را با موضوع پژوهش داشتند، برای تحلیل نهایی انتخاب شدند.

ارزیابی نهایی مطالعات منتخب با مطالعه چکیده، یافته‌ها و نتایج آنها انجام گرفت و یافته‌های مرتبط مستقیم با فرصت‌ها و چالش‌های استفاده از هوش مصنوعی در کیفیت گزارشگری مالی برای تحلیل کیفی استخراج شد. فرایند کدگذاری و استخراج مضامین مطابق روش آنسلم و کوربین[2](۱۳۹۰) و آترید-استرلینگ[3] (۲۰۰۱) در سه مرحله انجام شد. ابتدا، گزاره‌ها، مفاهیم و یافته‌های مرتبط با سؤال پژوهش شناسایی و به‌عنوان «مضامین پایه»کدگذاری شدند. سپس، مضامین پایه بر اساس شباهت مفهومی، ارتباط معنایی و هم‌راستایی موضوعی مقایسه و در قالب«مضامین سازمان‌دهنده» دسته‌بندی شدند. در مرحله سوم، مضامین سازمان‌دهنده بر اساس ارتباط مفهومی و ماهیت مشترک در سطوح بالاتر ترکیب و به «مضامین فراگیر» تبدیل شدند که تصویری جامع از فرصت‌ها و چالش‌های هوش مصنوعی در کیفیت گزارشگری مالی ارائه می‌کردند.

---

1. de Loë, Melnychuk, Murray & Plummer
2. Anselm & Corbin
3. Attride-Stirling

برای ارزیابی کیفیت و اعتمادپذیری یافته‌ها، با توجه به ماهیت کیفی پژوهش، معیارهای اعتبارپذیری، قابلیت اتکا و تأییدپذیری مورد توجه قرار گرفت. برای افزایش اعتبارپذیری؛ انتخاب مطالعات، استخراج داده‌ها و کدگذاری به‌صورت نظام‌مند و مرحله‌ای و بر اساس معیارهای از پیش تعیین‌شده انجام شد و متن مطالعات منتخب و کدهای استخراج‌شده چندین بار بازبینی و با یکدیگر تطبیق داده شدند. برای افزایش قابلیت اتکا؛ مراحل جست‌وجو، انتخاب مطالعات، استخراج اطلاعات، ایجاد کدهای اولیه، ادغام کدهای مشابه و تشکیل مضامین سازمان‌دهنده و فراگیر مستندسازی شد تا مسیر دستیابی از داده‌های اولیه به نتایج نهایی قابل پیگیری باشد. همچنین، برای تأییدپذیری؛ مضامین نهایی بر اساس شواهد موجود در مطالعات منتخب شکل گرفت و تلاش شد از تحمیل دیدگاه شخصی پژوهشگر جلوگیری شود. در مجموع، این اقدامات موجب افزایش انسجام، شفافیت و قابلیت پیگیری فرایند استخراج و تحلیل مضامین شد.

## یافته‌های پژوهش

### فرصت‌های هوش مصنوعی و کیفیت گزارشگری مالی

با توجه به بررسی و تحلیل نتایج مقالات منتخب، ابتدا تمامی یافته‌های اولیه (مضامین پایه) مرتبط با فرصت‌های هوش مصنوعی در ارتقای کیفیت گزارشگری مالی استخراج و در جدول شماره ۱ ارائه شدند.

**جدول ۱**

*مضامین پایه استخراج شده در زمینه فرصت های هوش مصنوعی و کیفیت گزارشگری مالی*

| سال پژوهش | محقق/محققین | مضامین پایه استخراج شده از نتایج مقالات |
|---|---|---|
| ۱۳۹۸ | فاطمه قشقایی،شهناز مشایخ | - امکان استفاده از سیستم اطلاعاتی یکپارچه در کل سازمان |
| ۱۳۹۸ | مجتبی تاراسی ، بهاره بنی طالبی دهکردی ، بهزاد زمانی | -پیش بینی وکشف احتمال گزارشگری مالی متقلبانه شرکت ها<br>-مدیریت ریسک، اعتبارسنجی و کشف تقلب |
| ۱۳۹۹ | علیرضا علی اکبرلو ، غلامرضا منصورفر ، فرزاد غیور | -معیارهای تشخیص شرکت های درمانده مالی با استفاده از هوش مصنوعی |
| ۱۳۹۹ | الهام اثنی عشری | کمک به حل مشکلات حسابداری و عملیاتی |

| | | |
|---|---|---|
| ۱۴۰۰ | ماریام یوخنه القیانی، جمال بحری ثالث، سعید جبارزاده کنگرلوئی، اکبر زواری رضایی | - افزایش قدرت پیش بینی گزارشگری مالی-مالیاتی متقلبانه |
| ۱۴۰۱ | ریحانه عنایتی طائبی ، علیرضا مهرآذین ، مهدی جباری نوقابی | پیش بینی بازده غیرعادی سهام |
| ۱۴۰۱ | حسین کامرانی ، بیژن عابدینی | افزایش قدرت پیش بینی کشف تقلب در صورتهای مالی |
| ۱۴۰۱ | آزاده مهرانی ، حمید علیزاده ، عبدالرسول رسولی | - توانایی پردازش و تحلیل داده های عظیم<br>- تصمیم گیری دقیق تر در خدمات مالی |
| ۱۴۰۲ | نیما رضایی | - خودکارسازی فرآیندهای مالی<br>- کاهش خطاهای انسانی<br>-کاهش وظایف تکراری<br>-تحلیل های پیشرفته و مشاوره های استراتژیک مالی<br>بهبود فرآیندهای مالی و ارتقاء نقش حسابداران |
| ۱۴۰۲ | مانا میرزاپور | -نقش مشاور با تخصص خاص تر در امور مالی و تجاری |
| ۱۴۰۲ | احسان جوادی | - افزایش بهره وری، دقت و نوآوری در حسابداری<br>- کاهش خطاهای انسانی<br>-ارائه تحلیل های پیشرفته<br>- بهبود تصمیم گیری |
| ۱۴۰۲ | ایوب رستمی ایوب، نصراله خلیلی تیرتاشی | - بهینه سازی تصمیم گیری های مالی<br>- کاهش ریسک سرمایه گذاری |
| ۱۴۰۲ | فاطمه کریم پور | - ارتقاء دقت پیش بینی های مالی |
| ۱۴۰۳ | حمید زارع، زهره حاجیها ، امیررضا کیقبادی | تاثیر مثبت بر کیفیت فرایند حسابرسی صورت های مالی |
| ۱۴۰۳ | غلامرضا سلیمانی امیری ، سارا محمدی سه دران | - ارتقا کیفیت حسابرسی<br>-افزایش پاسخگویی گزارشگری مالی<br>- ایجاد مزیت رقابتی<br>- بهبود تشخیص تقلب<br>- افزایش دقت در تشخیص ناهنجاریها |
| ۱۴۰۳ | احمد احمدی، وحید باغیشنی | - امکان دسترسی به اطلاعات مالی به روز و دقیق<br>- بهبود تصمیم گیری های مالی<br>- افزایش شفافیت و کاهش خطاها<br>- کاهش هزینه ها<br>- افزایش کارایی در فرآیندهای حسابداری |
| ۱۴۰۳ | محمد رضایی، علی احمدی | - بهبود تصمیم گیری های مالی |
| ۱۴۰۳ | راحله نظریان، فهیمه مظفری | -افزایش دقت و صحت<br>- افزایش جامعیت و دقت گزارش دهی<br>- کاهش دوباره کاری<br>- تجزیه وتحلیل صحیح داده ها<br>- کاهش زمان تجزیه وتحلیل داده ها |

| | | |
|---|---|---|
| | | – افزایش کارایی و بهبود کیفیت فرایندهای حسابداری<br>– فراهم کردن داده های تغییرناپذیر، امن و مطمئن<br>– کاهش تقلب، حساب سازی<br>– بهبود کیفیت گزارشگری مالی |
| ۱٤۰٤ | فاطمه قربانی ، منصور گرکز ، عبدالخالق خنکا ، علی خوزین ، علیرضا معطوفی | – مدیریت مالی،<br>– امنیت،<br>– انعطاف پذیری |
| ۱٤۰٤ | زهرا حاجی حسینی | –تسریع در ثبت و تجزیه و تحلیل داده های مالی<br>– کاهش خطاهای انسانی<br>–صرفه جویی در زمان<br>– افزایش دقت در تجزیه و تحلیل اطلاعات مالی<br>–پیشگیری و کشف به موقع تقلبات مالی |
| ۱٤۰٤ | یاسر جفائیان ، رضا صیدخانی ، مجتبی مرادپور ، رحمت اله محمدی پور | –بهینه سازی تصمیم گیری های مالی<br>– افزایش عدالت و پایداری مالی |
| ۱٤۰٤ | زینب آرمون منش، حسن پور خورشید | –بهبودکیفیت گزارشگری مالی<br>تاثیر مثبت تجربه بالا در حضور هوش مصنوعی |
| ۱٤۰٤ | امیدعلی کهریزی ، سیدامیرحسین سیدمیرزائی ، سیدابوالفضل علوی | –افزایش دقت گزارشدهی<br>– کشف تقلب،<br>– ارتقای شفافیت و اعتماد |
| ۱٤۰٤ | محمدمعید جمالی مهر | تحلیل کلان داده با هوش مصنوعی |
| ۱٤۰٤ | هاشم حیدر یوسف، پرویز پیری، پری چالاکی | –خودکارسازی فرایندهای گزارشگری مالی<br>– افزایش دقت فرایندهای گزارشگری مالی<br>–بهبود شناسایی روندها و قابلیت های تصمیم گیری<br>–گزارشگری کارآمدتر، دقیق تر و روشن<br>–کمک به کسب وکارها جهت تصمیم های مالی بهتر<br>–کاهش ریسک احتمالی<br>–تسریع در ارائه گزارشگری مالی<br>–کمک به توسعهٔ دانش و نوآوری در زمینه مالی |
| ۱٤۰٤ | علی دلیلی،کیهان آزادی هیر، محسن ارچین لیسار | –تشخیص زودهنگام ریسک بازده منفی<br>–ارتقاء کیفیت اطلاعات مالی<br>– زمینه ساز کاهش عدم قطعیت<br>– افزایش شفافیت در تصمیمات سرمایه گذاری<br>–تعمیق فهم علمی از روابط بین گزارشگری محافظه کارانه و ریسک بازده سهام<br>–کاربرد عملی برای تحلیلگران مالی، مدیران و سیاست گذاران بازار سرمایه |

| | | |
|---|---|---|
| ۱۴۰۴ | پرویز پیری، محمد عدنان حمود، علی آشتاب | -پردازش کارآمد حجم عظیمی از داده های مالی<br>-شناسایی الگوها و تشخیص ناهنجاری ها<br>- بهبود کیفیت حسابرسی<br>-خودکارسازی فعالیت های روزمرهٔ حسابرسی<br>- ارتقای دقت و کیفیت حسابرسی<br>-فراهم سازی فرصت برای تحلیل های پیچیده<br>-پیش بینی مالی در زمان واقعی<br>- تشخیص ناهنجاری ها و کاهش خطاها<br>-بهبود فرایند حسابرسی<br>- فراهم ساختن بودجه بندی و شناسایی حساب های مشکوک با تحلیل داده های تاریخی<br>-کمک به تصمیم گیری استراتژیک حسابرسان و مدیران<br>- کاهش ریسک |
| ۱۴۰۴ | محمداورسجی، رضا مهاجر منقوش ، فاطمه بالاخیلی ، علیرضا مشکور ،سجاد قاسمی | -انجام فعالیت های تکراری<br>- تحلیل داده های مالی در مقیاس وسیع<br>- شناسایی الگوهای غیرعادی<br>-ارتقای شفافیت و پاسخگویی مالی |
| ۱۴۰۴ | الهه رنجبر | -اتوماسیون(استفاده از نرم افزار) ورود داده ها<br>- تطبیق حساب ها و فعالیت های روتین حسابداری<br>-کاهش ریسک خطاهای انسانی<br>-فراهم نمودن تمرکز حسابداران به سمت فعالیت های استراتژیک<br>- امکان استخراج بینش های ارزشمند از داده های ساختار نیافته<br>-تسهیل تولید گزارش های مالی جامع و شفاف<br>- افزایش سرعت گزارشگری<br>-امکان ارتباط بهتر ذی نفعان با اطلاعات مالی<br>- امکان ثبت سوابق غیر قابل تغییر و ردیابی دقیق تراکنش ها<br>- کاهش تقلب<br>- افزایش اعتماد مشتری |

مضامین پایه بر اساس ارتباط مفهومی و معنایی در قالب« مضامین سازمان‌دهنده» دسته‌بندی و مضامین مرتبط نیز در سطح بالاتر در قالب مضامین فراگیر تجمیع شدند. نتایج این فرایند در جدول ۲ ارائه شده است.

**جدول۲**

*مضامین سازمان دهنده و مضامین فراگیر استخراج شده از مضامین پایه در زمینه فرصت های هوش مصنوعی و کیفیت گزارشگری مالی*

| مضامین پایه مستخرج از نتایج مقالات | مضامین سازمان دهنده | مضامین فراگیر |
|---|---|---|
| امکان استفاده از سیستم اطلاعاتی یکپارچه در کل سازمان | یکپارچه‌سازی سیستم‌های اطلاعات مالی | هوشمند سازی فرآیندهای حسابداری و گزارشگری مالی |
| –خودکارسازی فرآیندهای مالی<br>–اتوماسیون ورود داده‌ها<br>– تطبیق حساب‌ها<br>–فعالیت‌های روتین حسابداری<br>– کاهش وظایف تکراری<br>– انجام فعالیت‌های تکراری<br>–خودکارسازی فرآیندهای گزارشگری مالی<br>–خودکارسازی فعالیت‌های روزمره حسابرسی | خودکارسازی فرآیندهای حسابرسی و گزارشگری | |
| –افزایش دقت و صحت<br>–افزایش دقت فرآیندهای گزارشگری مالی<br>– افزایش بهره‌وری، دقت و نوآوری در حسابداری | افزایش دقت و صحت اطلاعات | |
| –کاهش خطاهای انسانی<br>کاهش ریسک خطاهای انسانی<br>کاهش هزینه‌ها، کاهش دوباره‌کاری | کاهش هزینه و خطاهای انسانی | |
| –بهبود کیفیت گزارشگری مالی<br>– گزارشگری کارآمدتر، دقیق‌تر و روشن‌تر<br>– افزایش جامعیت و دقت گزارش‌دهی<br>– افزایش دقت گزارش‌دهی<br>– افزایش پاسخگویی گزارشگری مالی<br>– تسهیل تولید گزارش‌های مالی جامع و شفاف | ارتقای کیفیت گزارشگری | ارتقای کیفیت و قابلیت اتکای اطلاعات مالی |
| –تأثیر مثبت بر کیفیت فرآیند حسابرسی،<br>–ارتقای کیفیت حسابرسی،<br>– بهبود کیفیت حسابرسی،<br>– ارتقای دقت و کیفیت حسابرسی،<br>– بهبود فرآیند حسابرسی،<br>–بودجه‌بندی با تحلیل داده‌های تاریخی | ارتقای کیفیت حسابرسی | |

| مضامین پایه مستخرج از نتایج مقالات | مضامین سازمان دهنده | مضامین فراگیر |
|---|---|---|
| -ارتقای کیفیت اطلاعات مالی،<br>- امکان دسترسی به اطلاعات مالی به‌روز و دقیق | ارتقای کیفیت اطلاعات مالی | |
| -توانایی پردازش و تحلیل داده‌های عظیم<br>-تحلیل کلان‌داده<br>- پردازش کارآمد حجم عظیمی از داده‌های مالی<br>-تحلیل داده‌های مالی در مقیاس وسیع | پردازش کلان‌داده‌های مالی | تحلیل هوشمند داده ها و پیش بینی مالی |
| -امکان استخراج بینش‌های ارزشمند از داده‌های ساختارنیافته<br>- شناسایی الگوها<br>-شناسایی الگوهای غیرعادی<br>-بهبود شناسایی روندها | استخراج بینش از داده‌های مالی | |
| -پیش‌بینی بازده غیرعادی سهام<br>- تشخیص زودهنگام ریسک بازده منفی | پیش بینی بازده و ریسک سهام | |
| -مدیریت ریسک<br>- کاهش ریسک<br>- کاهش ریسک احتمالی<br>-کاهش ریسک سرمایه‌گذاری<br>- اعتبارسنجی<br>-معیارهای تشخیص شرکت‌های درمانده مالی | مدیریت ریسک مالی | مدیریت ریسک، تقلب و امنیت مالی |
| - یش‌بینی و کشف احتمال گزارشگری مالی متقلبانه<br>- افزایش قدرت پیش‌بینی کشف تقلب<br>- افزایش قدرت پیش‌بینی گزارشگری مالیاتی متقلبانه<br>-پیشگیری و کشف به‌موقع تقلبات مالی<br>- کشف تقلب، بهبود تشخیص تقلب<br>-کاهش تقلب<br>-کاهش حساب‌سازی | کشف و پیشگیری از تقلب | |
| -افزایش دقت در تشخیص ناهنجاری‌ها<br>-تشخیص ناهنجاری‌ها<br>- شناسایی حساب‌های مشکوک | تشخیص ناهنجاری‌های مالی | |
| --فراهم کردن داده‌های امن، مطمئن و تغییرناپذیر<br>- ثبت سوابق غیرقابل تغییر و ردیابی تراکنش‌ها<br>- امنیت، افزایش اعتماد مشتری<br>- امکان ارتباط بهتر ذی‌نفعان با اطلاعات مالی | تقویت امنیت، قابلیت ردیابی و اعتماد | |
| -بهبود تصمیم‌گیری<br>بهبود تصمیم‌گیری‌های مالی | بهبود تصمیم‌گیری مالی و مدیریتی | ارتقای تصمیم گیری و عملکرد مالی |

| مضامین پایه مستخرج از نتایج مقالات | مضامین سازمان دهنده | مضامین فراگیر |
|---|---|---|
| - بهینه‌سازی تصمیم‌گیری‌های مالی<br>- تصمیم‌گیری دقیق‌تر در خدمات مالی<br>- کمک به کسب‌وکارها برای تصمیم‌های مالی بهتر<br>- کمک به تصمیم‌گیری استراتژیک مدیران و حسابرسان | | |
| - فراهم‌سازی تحلیل‌های پیشرفته<br>- مشاوره‌های استراتژیک مالی<br>- تعمیق فهم علمی از روابط بین گزارشگری محافظه کارانه و ریسک بازده سهام<br>- کاربرد عملی برای تحلیلگران، مدیران و سیاست‌گذاران بازار سرمایه | کاربردهای راهبردی هوش مصنوعی در مدیریت مالی | |
| -بهبود فرآیندهای مالی و ارتقای نقش حسابداران<br>-نقش مشاور تخصصی‌تر<br>- تمرکز حسابداران بر فعالیت‌های استراتژیک<br>- کمک به حل مشکلات حسابداری و عملیاتی | توسعه نقش راهبردی حسابداران | تحول حرفه ای و نوآوری در حسابداری |
| -ایجاد مزیت رقابتی<br>-کمک به توسعه دانش و نوآوری در زمینه مالی،<br>-انعطاف‌پذیری<br>- تأثیر مثبت تجربه بالا در حضور هوش مصنوعی | ایجاد مزیت رقابتی و نوآوری | |
| -افزایش شفافیت<br>- ارتقای شفافیت و اعتماد<br>- ارتقای شفافیت و پاسخگویی مالی<br>- افزایش عدالت و پایداری مالی | افزایش شفافیت و پاسخگویی | افزایش شفافیت و پاسخگویی |
| --صرفه‌جویی در زمان<br>-افزایش سرعت گزارشگری<br>- تسریع در ارائه گزارشگری مالی | افزایش سرعت پردازش و گزارشگری | |
| -ارتقای دقت پیش‌بینی‌های مالی<br>پیش‌بینی مالی در زمان واقعی | پیش بینی دقیق و به موقع مالی | تسریع در تحلیل دقیق داده ها و گزارشگری مالی |
| -تجزیه و تحلیل صحیح داده‌ها<br>-کاهش زمان تجزیه و تحلیل داده‌ها<br>- افزایش دقت در تجزیه و تحلیل اطلاعات مالی<br>- تسریع در ثبت و تجزیه و تحلیل داده‌های مالی | تجزیه تحلیل صحیح و سریع داده‌های مالی | |

**تبیین و مقایسه یافته‌ها در زمینه فرصت های هوش مصنوعی و کیفیت گزارشگری مالی**

**هوشمندسازی فرآیندهای حسابداری و گزارشگری مالی:** از زیرمضمون‌های مرتبط با این مضمون می‌توان به یکپارچه‌سازی سیستم‌های اطلاعات مالی و خودکارسازی فرایندهای حسابداری، حسابرسی و گزارشگری اشاره کرد. هوش مصنوعی با یکپارچه‌سازی داده‌ها و خودکارسازی فعالیت‌ها، ضمن حذف فعالیت‌های تکراری، افزایش سرعت و هماهنگی فرایندها و کاهش خطاهای انسانی، می‌تواند کارایی و کیفیت گزارشگری مالی را ارتقا دهد. همچنین، کاهش فعالیت‌های روتین، فرصت بیشتری برای حسابداران و حسابرسان جهت تمرکز بر تحلیل‌های تخصصی، قضاوت حرفه‌ای و ارزیابی ریسک فراهم می‌کند.

این یافته با نتایج مواچیکوکا (۲۰۲۴: ۱۷۵۱)همسو است که نشان داد هوش مصنوعی با افزایش کارایی و کاهش خطا می‌تواند دقت گزارشگری مالی را بهبود بخشد. همچنین مورفی و همکاران[1](۲۰۲۴: ۹) در مرور ادبیات هوش مصنوعی و حسابداری، بر ظرفیت این فناوری برای خودکارسازی فعالیت‌ها و ایجاد ارزش در فرایندهای حسابداری تأکید کرده‌اند.

**ارتقای کیفیت و قابلیت اتکای اطلاعات مالی:** از زیرمضمون‌های مرتبط با این مضمون می‌توان به افزایش دقت و صحت اطلاعات، کاهش هزینه‌ها و خطاهای انسانی، ارتقای کیفیت گزارشگری و اطلاعات مالی و بهبود کیفیت حسابرسی اشاره کرد که به‌کارگیری هوش مصنوعی با کاهش خطاهای انسانی و افزایش دقت تحلیل اطلاعات، می‌تواند کیفیت و قابلیت اتکای گزارشگری مالی را ارتقا دهد. در نتیجه، اطلاعات مالی از نظر دقت، قابلیت اتکا، به‌موقع‌بودن و شفافیت، ویژگی‌های مطلوب‌تری پیدا کرده و مبنای مناسب‌تری برای تصمیم‌گیری مدیران، سرمایه‌گذاران و سایر ذی‌نفعان فراهم می‌شود. این یافته با نتایج پژوهش جوهری(۲۰۲۵: ۱۰۹۶) که نشان داد هوش مصنوعی، همراه با نظام کنترل داخلی و کیفیت سیستم‌های اطلاعات حسابداری، می‌تواند به‌طور مثبت بر دقت گزارش داده‌های مالی اثرگذار باشد، همسو است.

**تحلیل هوشمند داده‌ها و پیش‌بینی مالی:** هوش مصنوعی با پردازش کلان‌داده‌های مالی و استخراج بینش‌های ارزشمند از داده‌ها، امکان شناسایی الگوهای پنهان، روندهای مالی و روابط پیچیده میان متغیرها را فراهم می‌سازد. این قابلیت‌ها می‌تواند دقت پیش‌بینی بازده و

[1] . Murphy et al

ریسک سهام را افزایش داده و از تصمیم‌گیری آگاهانه مدیران، سرمایه‌گذاران و سایر ذی‌نفعان حمایت کند.

این یافته با نتایج کورلجوسیچ و کارگر[1] (۲۰۲۳: ۸۱) همسو است؛ آنان در یک مرور نظام‌مند، کاربرد هوش مصنوعی در پیش‌بینی‌های حسابداری مالی را بررسی و نشان دادند که استفاده از مدل‌های مبتنی بر هوش مصنوعی می‌تواند ظرفیت تحلیل و پیش‌بینی مسائل مالی و حسابداری را افزایش دهد.

**مدیریت ریسک، تقلب و امنیت مالی:** یکی از مضامین فراگیر شناسایی‌شده، نقش هوش مصنوعی در مدیریت ریسک، کشف و پیشگیری از تقلب، شناسایی ناهنجاری‌های مالی و افزایش قابلیت ردیابی اطلاعات است. الگوریتم‌های هوش مصنوعی با پردازش حجم زیادی از داده‌های مالی و شناسایی الگوهای غیرعادی، می‌توانند در تشخیص به‌موقع مخاطرات، معاملات مشکوک و رفتارهای متقلبانه مؤثر باشند. این قابلیت‌ها با کمک به شناسایی زودهنگام تقلب و ناهنجاری‌ها، می‌توانند احتمال دستکاری اطلاعات را کاهش داده و در نتیجه به افزایش قابلیت اتکای گزارش‌های مالی کمک کنند.

این یافته با نتایج پژوهش شهانا و همکاران[2] (۲۰۲۳: ) و هرناندز آروس و همکاران[3] (۲۰۲۴: ۱) همسو است؛ آنان در پژوهش خود نشان دادند که روش‌های داده‌کاوی و یادگیری ماشین به‌طور فزاینده‌ای برای شناسایی الگوهای تقلب و ناهنجاری‌های مالی به کار گرفته می‌شوند.

**ارتقای تصمیم‌گیری و عملکرد مالی:** یکی دیگر از مضامین فراگیر شناسایی‌شده، نقش هوش مصنوعی در بهبود تصمیم‌گیری و ارتقای عملکرد مالی سازمان‌هاست. بهره‌گیری از قابلیت‌های تحلیلی و پیش‌بینی هوش مصنوعی، امکان پردازش سریع‌تر و دقیق‌تر اطلاعات و ارائه بینش‌های مبتنی بر داده را فراهم می‌کند و می‌تواند به بهبود کیفیت تصمیم‌های مالی و مدیریتی و کاهش عدم‌اطمینان در تصمیم‌گیری منجر شود. همچنین، استفاده از این فناوری می‌تواند مدیران را در زمینه‌هایی مانند تخصیص منابع، ارزیابی گزینه‌های سرمایه‌گذاری، مدیریت ریسک و تدوین راهبردهای مالی یاری کند. این یافته با نتایج یه و چن[4] (۲۰۲۴: ۳۰)

---

1. Kureljusic & Karger
2. Shahana et al
3. Hernandez Aros et al
4. Ye & Chen

که بر نقش هوش مصنوعی در پشتیبانی از تصمیم‌گیری حسابداری و مدیریت عملکرد تأکید کرده‌اند، همسو است.

**تحول حرفه‌ای و نوآوری در حسابداری:** هوش مصنوعی زمینه‌ساز تحول حرفه‌ای و نوآوری در حسابداری است. به‌کارگیری این فناوری، با توسعه نقش راهبردی حسابداران، موجب انتقال تمرکز آنان از انجام وظایف تکراری و عملیاتی به فعالیت‌های تحلیلی، مشاوره‌ای و ارزش‌آفرین می‌شود. همچنین، بهره‌گیری از قابلیت‌های هوش مصنوعی با ایجاد مزیت رقابتی و تقویت نوآوری، سازمان‌ها را در بهبود فرایندهای کسب‌وکار، ارائه خدمات مالی هوشمند و افزایش توان رقابتی یاری می‌دهد. این یافته با نتایج گرین‌من و همکاران[1] (۲۰۲۴: ۱۸۸) همسو است؛ آنان نشان دادند که هوش مصنوعی با خودکارسازی وظایف روتین و تقویت تحلیل داده‌ها، نقش حسابداران و حسابرسان را به سمت فعالیت‌های باارزش‌تری مانند مشاوره راهبردی و مدیریت ریسک سوق می‌دهد. همچنین عصیدی و همکاران[2] (۲۰۲۵: ۹۱۵) نشان دادند که پذیرش هوش مصنوعی می‌تواند به تغییر و توسعه نقش‌ها و مسئولیت‌های حرفه‌ای حسابداران و افزایش بهره‌وری محیط کار منجر شود.

**افزایش شفافیت و پاسخگویی:** هوش مصنوعی می‌تواند از طریق افزایش شفافیت و پاسخگویی، نقش مؤثری در بهبود نظام گزارشگری مالی ایفا کند. استفاده از قابلیت‌های هوش مصنوعی در ثبت، پردازش و تحلیل اطلاعات مالی، دسترسی به داده‌های دقیق‌تر، به‌موقع و قابل ردیابی را برای ذی‌نفعان فراهم می‌سازد. این امر با کاهش ابهام اطلاعاتی و تقویت سازوکارهای نظارتی، زمینه افزایش پاسخگویی مدیران و اعتماد استفاده‌کنندگان از گزارش‌های مالی را فراهم می‌کند.

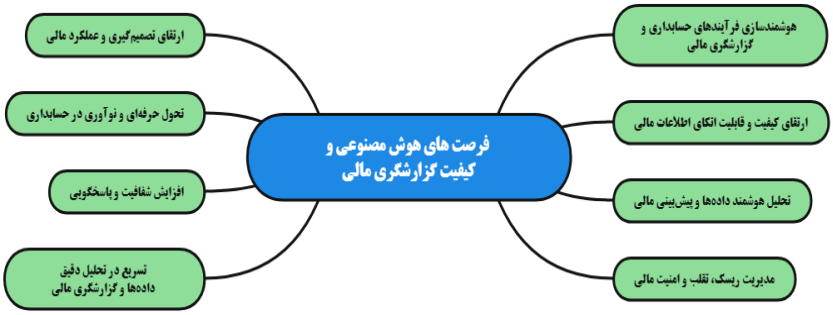
این یافته با نتایج یانگ و زو(۲۰۲۵: ۱۰۷۷) همسو است؛ آنان دریافتند که پذیرش هوش مصنوعی به‌طور معناداری کیفیت افشای اطلاعات حسابداری را بهبود می‌بخشد و از جمله سازوکارهای این اثر را کاهش عدم تقارن اطلاعاتی و افزایش اعتبار و به‌موقع‌بودن افشا عنوان کردند.

---

1. Greenman et al
2. Assidi et al

**تسریع در تحلیل دقیق داده‌ها و گزارشگری مالی:** هوش مصنوعی با افزایش سرعت پردازش و تحلیل داده‌های مالی، امکان دسترسی سریع‌تر مدیران و سایر ذی‌نفعان به اطلاعات موردنیاز را فراهم می‌کند. پردازش سریع حجم زیادی از داده‌ها و ارائه تحلیل‌ها و پیش‌بینی‌های بهنگام می‌تواند زمان انجام فرایندهای گزارشگری را کاهش داده و بهبود تصمیم‌گیری‌های مالی و مدیریتی را به دنبال داشته باشد. همچنین، دسترسی سریع‌تر به اطلاعات، سازمان‌ها را قادر می‌سازد واکنش مناسب‌تری نسبت به تغییرات محیطی و مالی نشان دهند.

این یافته با نتایج لیائو و همکاران[1] (۲۰۲۴) که نشان دادند که هوش مصنوعی در کاهش تأخیر انتشار گزارش حسابرسی و به‌موقع‌بودن گزارش‌ها ارتباط دارد، همسو است.




**نمودار ۱.** فرصت های هوش مصنوعی و کیفیت گزارشگری مالی

## چالش‌های هوش مصنوعی و کیفیت گزارشگری مالی

با توجه به بررسی و تحلیل نتایج مقالات منتخب، ابتدا تمامی یافته‌های اولیه (مضامین پایه)مرتبط با چالش‌های هوش مصنوعی در ارتقای کیفیت گزارشگری مالی استخراج و در جدول شماره ۳ ارائه شدند.

[1]. Liao et al

## جدول شماره۳

*مضامین پایه استخراج شده در زمینه چالش های هوش مصنوعی و کیفیت گزارشگری مالی*

| سال پژوهش | محقق/محققین | مضامین پایه استخراج شده از نتایج مقالات |
|---|---|---|
| ۱۴۰۱ | آزاده مهرانی ، حمید علیزاده ، عبدالرسول رسولی | – هزینه پیاده سازی<br>– مسائل مربوط به حریم خصوصی |
| ۱۴۰۲ | نیما رضایی | –مسائل اخلاقی و قانونی در استفاده از هوش مصنوعی |
| ۱۴۰۲ | مانا میرزاپور | – کسب مهارت های لازم از طریق آموزش |
| ۱۴۰۲ | احسان جوادی | – امنیت داده ها<br>–نیاز به بازآموزی حسابداران<br>–مسائل اخلاقی |
| ۱۴۰۲ | فاطمه کریم پور | رعایت مسائل اخلاقی<br>– حفاظت از داده ها |
| ۱۴۰۳ | غلامرضا سلیمانی امیری ، سارا محمدی سه دران | –هزینه بالا برنامه های هوش مصنوعی<br>– افزایش بیکاری،<br>–فقدان آیین نامه اخلاقی برای استفاده از هوش مصنوعی<br>– نیاز به نیروی کار متخصص<br>– محدودشدن توانایی هوش مصنوعی به توانایی طراح آن |
| ۱۴۰۳ | بهنام گلشاهی ، علیرضا مرتضی زاده | – کاهش بهره وری افراد<br>–عدم امنیت داده<br>– نقض حریم خصوصی در سازمان،<br>–نارضایتی و ترک خدمت سرمایه های انسانی سازمان |
| ۱۴۰۳ | احمد احمدی، وحید باغیشنی | – مسائل امنیتی<br>– نیاز به آموزش کارکنان برای استفاده از فناوری های جدید |
| ۱۴۰۴ | هاشم حیدر یوسف، پرویز پیری، پری چالاکی | –سوءاستفاده ها و تهدیدهای امنیتی |
| ۱۴۰۴ | محمداورسجی، رضا مهاجر منقوش ، فاطمه بالاخیلی ، علیرضا مشکور ،سجاد قاسمی | – کمبود مهارت های تخصصی<br>– ریسک های امنیت سایبری<br>– مسائل اخلاقی |
| ۱۴۰۴ | الهه رنجبر | – امنیت داده ها<br>– ملاحظات اخلاقی<br>– لزوم بازآموزی حسابداران |

| سال پژوهش | محقق/محققین | مضامین پایه استخراج شده از نتایج مقالات |
|---|---|---|
| | | - نیازمند سرمایه گذاری |
| ۱۴۰۴ | امیدعلی کهریزی ، سیدامیرحسین سیدمیرزائی ، سیدابوالفضل علوی | - خطر گزارش دهی تزئینی یا سوگیری شده<br>-انتشار اطلاعات رفتاری و شخصی مشتریان |
| ۱۴۰۴ | زهرا حاجی حسینی | -امنیت داده ها<br>- حفظ حریم خصوصی<br>-نیازمند آموزش حسابداران |

مضامین پایه بر اساس ارتباط مفهومی و معنایی در قالب« مضامین سازمان‌دهنده» دسته‌بندی و مضامین مرتبط نیز در سطح بالاتر در قالب «مضامین فراگیر» تجمیع شدند. نتایج این فرایند در جدول شماره ۴ ارائه شده است.

**جدول٤**

*مضامین سازمان دهنده و مضامین فراگیر استخراج شده از مضامین پایه در زمینه چالش های هوش مصنوعی و کیفیت گزارشگری مالی*

| مضامین پایه مستخرج از نتایج مقالات | مضامین سازمان دهنده | مضامین فراگیر |
|---|---|---|
| -امنیت داده‌ها<br>- عدم امنیت داده<br>- مسائل امنیتی<br>-ریسک‌های امنیت سایبری<br>-سوءاستفاده‌ها و تهدیدهای امنیتی<br>-حفاظت از داده | امنیت داده‌ها و اطلاعات | چالش‌های امنیت، حریم خصوصی و حاکمیت داده |
| -مسائل مربوط به حریم خصوصی<br>- حفظ حریم خصوصی<br>- نقض حریم خصوصی در سازمان<br>-انتشار اطلاعات رفتاری و شخصی مشتریان | حفظ حریم خصوصی | |
| -مسائل اخلاقی<br>- رعایت مسائل اخلاقی<br>- ملاحظات اخلاقی<br>-مسائل اخلاقی و قانونی در استفاده از هوش مصنوعی | ملاحظات اخلاقی در به کار گیری هوش مصنوعی | مسائل اخلاقی و حقوقی |

| مضامین پایه مستخرج از نتایج مقالات | مضامین سازمان دهنده | مضامین فراگیر |
|---|---|---|
| -فقدان آیین‌نامه اخلاقی برای استفاده از هوش مصنوعی | الزمات قانونی و مقرراتی | |
| -خطر گزارش‌دهی تزیینی یا سوگیری‌شده<br>-محدود شدن توانایی هوش مصنوعی به توانایی طراح آن | مخاطرات سوگیری و قابلیت اتکای خروجی ها | |
| -کسب مهارت‌های لازم از طریق آموزش<br>- نیاز به آموزش کارکنان برای استفاده از فناوری‌های جدید<br>- نیازمند آموزش حسابداران<br>-نیاز به بازآموزی حسابداران<br>-لزوم بازآموزی حسابداران | آموزش وبازآموزی نیروی انسانی | تامین منابع انسانی و بازآموزی آنها |
| -نیاز به نیروی کار متخصص<br>- کمبود مهارت‌های تخصصی | کمبود نیروی انسانی متخصص | |
| -افزایش بیکاری،<br>- کاهش بهره‌وری افراد،<br>-نارضایتی و ترک خدمت سرمایه‌های انسانی سازمان | پیامدهای شغلی و سازمانی | |
| -هزینه پیاده‌سازی<br>- هزینه بالای برنامه‌های هوش مصنوعی<br>-نیازمند سرمایه‌گذاری | هزینه پیاده سازی و سرمایه گذاری | چالش های اقتصادی و پیاده سازی |

**تبیین و مقایسه یافته‌ها در زمینه چالش های هوش مصنوعی و کیفیت گزارشگری مالی**

**چالش‌های امنیت، حریم خصوصی و حاکمیت داده ها:** چالش‌های امنیت، حریم خصوصی و حاکمیت داده‌ها از مهم‌ترین موانع بهره‌گیری اثربخش از هوش مصنوعی در گزارشگری مالی محسوب می‌شوند. وابستگی سامانه‌های هوش مصنوعی به حجم گسترده‌ای از داده‌های مالی، ضرورت توجه ویژه به امنیت داده‌ها و اطلاعات و ایجاد سازوکارهای مناسب برای جلوگیری از دسترسی غیرمجاز، افشای اطلاعات و تهدیدهای سایبری را افزایش داده است. همچنین، حفظ حریم خصوصی ذی‌نفعان و استفاده مسئولانه از داده‌های مالی، از الزامات اساسی پذیرش این فناوری به شمار می‌رود. این یافته با نتایج کوکینا و همکاران[1] (۲۰۲۵: ۱)

[1]. Kokina et al

همسو است؛ آنان بر اساس مصاحبه با متخصصان حسابرسی، حریم خصوصی داده‌ها را در کنار سوگیری و قابلیت اتکا، از مهم‌ترین چالش‌های پذیرش هوش مصنوعی در حسابرسی شناسایی کردند.

**مسائل اخلاقی و حقوقی:** مسائل اخلاقی و حقوقی از جمله چالش‌های اساسی در به‌کارگیری هوش مصنوعی در گزارشگری مالی است. استفاده از این فناوری مستلزم توجه به ملاحظات اخلاقی، تدوین الزامات قانونی و مقرراتی مناسب و اطمینان از قابلیت اتکای خروجی‌های الگوریتمی است. سوگیری در داده‌ها یا فرآیندهای تصمیم‌گیری هوشمند می‌تواند به کاهش اعتماد به اطلاعات مالی و اتخاذ تصمیمات نادرست منجر شود. ازاین‌رو، طراحی چارچوب‌های اخلاقی و نظارتی شفاف، همراه با سازوکارهای کنترل، پاسخگویی و ارزیابی مستمر، برای تضمین استفاده مسئولانه و قابل اعتماد از هوش مصنوعی در گزارشگری مالی ضروری است.

این یافته با نتایج پرداناو همکاران[1] (۲۰۲۴: ۳۲۱) و کوکینا و همکاران(۲۰۲۵: ۱) که بر اهمیت سوگیری، شفافیت، پاسخگویی، قابلیت اتکا و ضرورت وجود سازوکارهای کنترلی و راهنمایی برای استفاده مسئولانه از هوش مصنوعی تأکید کرده‌اند، همسو است.

**تأمین منابع انسانی و بازآموزی آنها:** استفاده اثربخش از فناوری هوش مصنوعی نیازمند آموزش و بازآموزی مستمر نیروی انسانی، توسعه مهارت‌های تخصصی و تربیت کارکنانی با توانایی ترکیب دانش حسابداری و فناوری‌های نوین است. همچنین، کمبود نیروی انسانی متخصص و نگرانی‌های مرتبط با تغییر ماهیت مشاغل، کاهش برخی وظایف سنتی و پیامدهای سازمانی ناشی از اتوماسیون، می‌تواند فرآیند پذیرش هوش مصنوعی را با چالش مواجه سازد. ازاین‌رو، سرمایه‌گذاری در توسعه سرمایه انسانی و بازطراحی نقش‌های شغلی، شرطی اساسی برای بهره‌برداری پایدار و موفق از ظرفیت‌های هوش مصنوعی در حرفه حسابداری و گزارشگری مالی محسوب می‌شود.

این یافته با نتایج پژوهش کوکینا و همکاران(۲۰۲۵: ۱) که بر نیاز به راهنمایی و آمادگی حرفه‌ای در مواجهه با چالش‌های پذیرش هوش مصنوعی در حسابرسی تأکید کرده‌اند، همسو است.

---

[1]. Perdana

**چالش‌های اقتصادی و پیاده‌سازی:** یافته‌های این پژوهش نشان می‌دهد که چالش‌های اقتصادی و پیاده‌سازی از عوامل مهم تأثیرگذار بر پذیرش و توسعه هوش مصنوعی در گزارشگری مالی است. هزینه‌های بالای پیاده‌سازی، توسعه زیرساخت‌های فناورانه، نگهداری سامانه‌ها و نیاز به سرمایه‌گذاری اولیه قابل‌توجه، می‌تواند مانعی برای استفاده گسترده سازمان‌ها از این فناوری باشد.

این یافته با نتایج سرسلی و کاداگیشویلی (۲۰۲۳: ۷۲) همسو است؛ آنان در بررسی کاربرد هوش مصنوعی در حسابداری و گزارشگری مالی، هزینه‌های پیاده‌سازی، نیاز به زیرساخت‌های فناورانه و ضرورت سرمایه‌گذاری و آمادگی سازمانی را از جمله ملاحظات مهم پذیرش این فناوری مطرح کرده‌اند. بنابراین، اتخاذ رویکردی مرحله‌ای و سرمایه‌گذاری هدفمند می‌تواند زمینه استفاده اثربخش و پایدار از هوش مصنوعی در فرآیندهای گزارشگری مالی را فراهم سازد.




**نمودار۲.** چالش های هوش مصنوعی و کیفیت گزارشگری مالی

## بحث و نتیجه‌گیری

نتایج این مرور نظام‌مند نشان می‌دهد که هوش مصنوعی به‌عنوان یکی از مهم‌ترین فناوری‌های تحول‌آفرین، ظرفیت قابل‌توجهی برای بهبود گزارشگری مالی در حسابداری و حسابرسی دارد، اما بهره‌گیری اثربخش از آن مستلزم مدیریت هم‌زمان فرصت‌ها و چالش‌های پیش‌رو است. یافته‌های پژوهش نشان داد که فرصت‌های هوش مصنوعی در گزارشگری مالی را می‌توان در هشت مضمون فراگیر شامل هوشمندسازی فرآیندهای حسابداری و گزارشگری مالی؛ ارتقای کیفیت و قابلیت اتکای اطلاعات مالی؛ تحلیل هوشمند داده‌ها و پیش‌بینی مالی؛ مدیریت ریسک، تقلب و امنیت مالی؛ ارتقای تصمیم‌گیری و عملکرد مالی؛ تحول حرفه‌ای و

نوآوری در حسابداری؛ افزایش شفافیت و پاسخگویی؛ و تسریع در تحلیل دقیق داده‌ها و گزارشگری مالی طبقه‌بندی کرد. این یافته‌ها بیانگرآن است که هوش مصنوعی صرفاً ابزاری برای خودکارسازی فعالیت‌های تکراری نیست، بلکه با افزایش سرعت پردازش اطلاعات، ارتقای دقت و کیفیت گزارش‌های مالی، تقویت توان پیش‌بینی، بهبود مدیریت ریسک و کشف تقلب، زمینه را برای تصمیم‌گیری آگاهانه‌تر مدیران، سرمایه‌گذاران و سایر ذی‌نفعان فراهم می‌سازد. همچنین، این فناوری با تغییر نقش حسابداران از انجام فعالیت‌های عملیاتی به ایفای نقش‌های تحلیلی، مشاوره‌ای و راهبردی، می‌تواند موجب تحول در حرفه حسابداری و افزایش ارزش‌آفرینی برای سازمان‌ها شود.

در مقابل، یافته‌ها نشان داد که استقرار و توسعه هوش مصنوعی در گزارشگری مالی با چالش‌های مهمی نیز همراه است که در چهار مضمون فراگیر شامل چالش‌های امنیت، حریم خصوصی و حاکمیت داده ها؛ مسائل اخلاقی و حقوقی؛ تأمین منابع انسانی و بازآموزی آن‌ها؛ و چالش‌های اقتصادی و پیاده‌سازی قابل طبقه‌بندی هستند. این چالش‌ها بیانگر آن است که موفقیت در به‌کارگیری هوش مصنوعی تنها به توسعه زیرساخت‌های فناورانه وابسته نیست، بلکه مستلزم ایجاد چارچوب‌های حقوقی و اخلاقی مناسب، تضمین امنیت و محرمانگی داده‌ها، سرمایه‌گذاری در آموزش و توانمندسازی سرمایه انسانی و تأمین منابع مالی موردنیاز برای استقرار و نگهداری این فناوری است. در غیر این صورت، مخاطراتی نظیر نقض حریم خصوصی، تهدیدهای امنیت سایبری، سوگیری در خروجی‌های هوش مصنوعی، کمبود نیروی انسانی متخصص و هزینه‌های بالای پیاده‌سازی می‌تواند اثربخشی این فناوری را کاهش دهد.

## پیشنهادها

### پیشنهادهای کاربردی

با توجه به یافته‌های پژوهش و شناسایی فرصت‌ها و چالش‌های به‌کارگیری هوش مصنوعی در گزارشگری مالی، پیشنهادهای زیر ارائه می‌شود:

۱. سیاست‌گذاران و نهادهای ناظر چارچوب‌های قانونی و نظارتی متناسب با هوش مصنوعی در گزارشگری مالی، شامل مسئولیت‌پذیری، شفافیت الگوریتم‌ها، قابلیت اتکا، حفاظت از داده‌های مالی و نظارت بر تصمیمات هوشمند، تدوین کنند.

۲. شرکت‌ها و واحدهای تجاری پیش از پیاده‌سازی هوش مصنوعی، ارزیابی هزینه ـ منفعت انجام داده و آن را به‌صورت مرحله‌ای و متناسب با ظرفیت‌های مالی، فنی و سازمانی اجرا کنند و هم‌زمان زیرساخت‌های فناوری اطلاعات، امنیت سایبری و حاکمیت داده‌ها را تقویت کنند.
۳. سازمان‌های حرفه‌ای حسابداری آموزش و بازآموزی مستمر حسابداران، حسابرسان و مدیران مالی را با تأکید بر تحلیل داده، ابزارهای هوش مصنوعی، ارزیابی خروجی الگوریتم‌ها و ملاحظات اخلاقی و امنیتی توسعه دهند.
۴. دانشگاه‌ها و مراکز آموزشی با بازنگری سرفصل‌های حسابداری و حسابرسی، آموزش هوش مصنوعی، تحلیل داده، یادگیری ماشین، حاکمیت داده و اخلاق فناوری را تقویت کنند تا نیروی انسانی متناسب با تحولات حرفه تربیت شود.
۵. مدیران مالی و حسابرسان هوش مصنوعی را جایگزین قضاوت حرفه‌ای انسان ندانند و نظارت و کنترل انسانی را حفظ کنند؛ به‌ویژه در تصمیمات بااهمیت، خروجی‌های هوش مصنوعی از نظر صحت، سوگیری، قابلیت اتکا و انطباق با استانداردهای حرفه‌ای ارزیابی شوند.

## پیشنهاد برای تحقیقات آتی

با توجه به خلأهای شناسایی‌شده در ادبیات پژوهش، پیشنهاد می‌شود تحقیقات آتی در محورهای زیر انجام شوند:

۱. مطالعه تجربی و طولی رابطه استفاده از هوش مصنوعی با کیفیت گزارش‌های مالی بر اساس داده‌های واقعی شرکت‌ها و مقایسه وضعیت شرکت‌ها پیش و پس از پذیرش این فناوری
۲. بررسی تأثیر هوش مصنوعی بر اعتماد استفاده‌کنندگان اطلاعات مالی، به‌ویژه سرمایه‌گذاران، اعتباردهندگان و تحلیلگران، و نقش ابهام و سوگیری الگوریتمی در افزایش یا کاهش این اعتماد

۳. تبیین نقش حاکمیت شرکتی، کنترل‌های داخلی و تخصص فناوری اطلاعات در تقویت یا تعدیل آثار هوش مصنوعی بر کیفیت گزارشگری مالی و مقایسه آثار و چالش‌های این فناوری بر اساس اندازه شرکت، صنعت و سطح بلوغ دیجیتال

۴. انجام مطالعات اقتصادی و هزینه ـ منفعت درباره پیاده‌سازی و نگهداری هوش مصنوعی، به‌ویژه در شرکت‌های کوچک و متوسط، و تعیین شرایط توجیه‌پذیری هزینه‌های استقرار و نگهداری بر اساس منافع حاصل از این فناوری

## محدودیت‌های پژوهش

پژوهش حاضر، همانند هر پژوهش دیگری، با محدودیت‌هایی مواجه است که در تفسیر یافته‌های آن باید مورد توجه قرار گیرد.

– نتایج این پژوهش به مطالعاتی محدود است که در پایگاه‌های اطلاعاتی مورد بررسی و در بازه زمانی تعیین‌شده شناسایی و در دسترس پژوهشگر قرار گرفته‌اند.

– شناسایی، کدگذاری و دسته‌بندی مضامین، با وجود تلاش برای رعایت اصول نظام‌مند و بازبینی مراحل تحلیل، می‌تواند تا حدی تحت تأثیر تفسیر پژوهشگر قرار گیرد.

– با توجه به سرعت بالای تحول فناوری‌های هوش مصنوعی، یافته‌های پژوهش ممکن است با ظهور فناوری‌ها، مقررات و کاربردهای جدید در آینده نیازمند بازنگری و به‌روزرسانی باشد.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع

آذرسعید، یاشار؛ رستمی، شعیب(۱۴۰۲). هوش مصنوعی و تصمیم گیری اخلاقی در حسابداری و حسابرسی: تحلیل چالش های مرتبط .*قضاوت و تصمیم گیری در حسابداری و حسابرسی*،۲ (۷)،۱۱۴-۸۷.

آزمون‌منش، زینب؛ پورخورشید، حسن(۱۴۰۴). تأثیر استفاده از هوش مصنوعی در حسابرسی بر کیفیت گزارشگری مالی با نقش تعدیل‌گر تجربه حسابرس. *حسابداری، امور مالی و هوش محاسباتی*، ۳(۳)، ۱–۱۵.

آنسلم، استراوس؛ کوربین ، جولیت(۱۳۹۰). *اصول روش تحقیق کیفی: نظریه مبنایی، رویه‌ها و شیوه‌ها*.(مترجم: بیوک محمدی). انتشارات: پژوهشگاه علوم انسانی و مطالعات فرهنگی

اثنی‌عشری، الهام. (۱۳۹۹). تأثیر فناوری اطلاعات بر گزارشگری مالی. *پژوهشنامه اورمزد،۱۲ (۵۳)*، ۹۴–۱۰۴.

احمدی، احمد، ؛ باغیشنی، وحید(۱۴۰۳). دیجیتالی شدن و گزارشگری مالی: چگونگی تغییر نوآوری در فناوری به سمت حسابداری مداوم در ایران. *کنفرانس بین‌المللی مدیریت، حسابداری و توسعه اقتصادی، ۱۳* .

یوخنه القیانی، ماریام ؛ بحری ثالث، جمال؛ جبارزاده کنگرلوئی، سعید؛ زواری رضایی، اکبر(۱۴۰۰). تبیین گزارشگری مالی–مالیاتی متقلبانه شرکت‌ها: رویکرد ترکیبی داده‌کاوی کلاسیک، ANFISو الگوریتم‌های فراابتکاری. *مطالعات تجربی حسابداری مالی، ۱۸* (۷۱)، ۸۹–۱۱۱

اورسجی، محمد؛ مهاجر منقوش، رضا؛ بالاخیلی، فاطمه؛ مشکور، علیرضا؛و قاسمی، سجاد. (۱۴۰۴). بررسی نقش هوش مصنوعی در حسابداری بخش عمومی. *پژوهش‌های نوین بین‌رشته‌ای علوم پایه و فنی و مهندسی*، ۵(۳)، ۱–۱۰.

تاراسی، مجتبی؛ بنی‌طالبی دهکردی، بهاره، و زمانی، بهزاد. (۱۳۹۸). پیش‌بینی گزارشگری مالی متقلبانه از طریق شبکه عصبی مصنوعی .(ANN) *حسابداری مدیریت، ۱۲* (۴۰)، ۶۳–۷۹.

جفائیان، یاسر؛ صیدخانی، رضا؛ مرادپور، مجتبی؛ محمدی‌پور، رحمت‌اله (۱۴۰۴). طراحی مدل استراتژی‌های مالی سازمان تأمین اجتماعی با استفاده از هوش مصنوعی. *مدیریت استراتژیک هوشمند*، ۴(۴)، ۲۲۱–۲۵۲.

جمالی‌مهر، محمدمعید (۱۴۰۴). به سوی زیست‌بوم‌های هوش مصنوعی؛ پیوند تحلیل کلان‌داده با هوش مصنوعی. *کنفرانس بین‌المللی مدیریت، علوم کامپیوتر و هوش مصنوعی، ۱* .

جوادی، احسان (۱۴۰۲). تأثیر فناوری هوش مصنوعی بر حرفه حسابداری. *کنفرانس بین‌المللی مدیریت، حسابداری و توسعه اقتصادی، ۱۲* .

حاجی حسینی، زهرا (۱۴۰۴). مروری بر تأثیرات هوش مصنوعی بر حرفه حسابداری. *کنفرانس ملی یافته‌های نوین در مدیریت، روانشناسی و حسابداری، ۱۱* .

حسینی، احد؛ جبارزاده کنگرلویی، سعید؛ بحری ثالث، جمال؛ سعدی، رسول(۱۴۰۰). تبیین موانع پیاده سازی استانداردهای بین المللی گزارشگری مالی، رویکرد نظریه داده بنیاد .*تحقیقات مالی*، ۲۳ (۱)، ۱۳۳-۱۰۸

دلیلی، علی، آزادی‌هیر، کیهان؛ ارچین‌لیسار، محسن (۱۴۰۴). پیش‌بینی وقوع بازده منفی سهام با الگوریتم‌های هوش مصنوعی و ارتباط آن با گزارشگری محافظه‌کارانه در شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران. *حسابداری، امور مالی و هوش محاسباتی*، ۳(۱)، ۱–۱۹.

رستمی، ایوب؛ خلیلی تیرتاشی، نصراله (۱۴۰۲). کاربرد هوش مصنوعی در سیستم‌های مالی از دیدگاه اقتصاد اسلامی. *مطالعات فقه اقتصادی*، ۵(۲)، ۲۱–۳۴.

رضایی، محمد؛ احمدی، علی (۱۴۰۳). شناسایی عوامل تأثیرگذار بر رفتار مالی سرمایه‌گذاران در بازارهای نوظهور. *حسابداری، امور مالی و هوش محاسباتی*، ۲ (۱)، ۴۵–۵۶.

رضایی، نیما (۱۴۰۲). آینده حسابداری: چگونگی تحول نقش حسابداران در گزارشگری مالی توسط هوش مصنوعی. *حسابداری، امور مالی و هوش محاسباتی*، ۱ (۲)، ۵۳–۶۵.

رنجبر، الهه (۱۴۰۴). فرصت‌ها و تهدیدها؛ حسابداری در گذار به هوش مصنوعی. *کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق*، ۱۵ .

زارع، حمید؛ حاجی‌ها، زهره؛ کیقبادی، امیررضا(۱۴۰۳). بررسی تأثیر استفاده از هوش مصنوعی در حسابرسی بر فرایند کیفیت حسابرسی صورت‌های مالی. *پژوهش‌های حسابرسی حرفه‌ای*، ۴ (۱۶)، ۳۸–۶۵.

سلیمانی امیری، غلامرضا؛ محمدی سه‌دران، سارا (۱۴۰۳). حسابرسی در عصر هوش مصنوعی. *حسابداری و منافع اجتماعی*، ۱۴ (۳)، ۱–۳۶.

صاحبی، مریم؛ ممیز، آیت‌اله؛ یدالهی فارسی، جهانگیر (۱۴۰۴). مدیریت هوشمند خدمات مالی: چارچوبی استراتژیک برای پذیرش هوش مصنوعی. *مدیریت استراتژیک هوشمند*، ۴ (۴)، ۹۵–۱۱۴.

عدنان حمود، محمد؛ پیری، پرویز؛ آشتاب، علی(۱۴۰۴). امکان سنجی بهره گیری از فناوری های نوین هوش مصنوعی در بهبود فرایندهای حسابرسی در کشور. بررسی های *حسابداری و حسابرسی*، ۳۲ (۳). ۵۳۵-۵۵۹.

علی خانی، رضیه؛ عطایی، جواد(۱۴۰۴). نقش فناوری بالکچین در حسابداری و حسابرسی .*نشریه علمی حسابرسی سیستم ها و فناوری اطلاعات*،۱ (۱). ۲۲۶-۲۵۶

علی‌اکبرلو، علیرضا؛ منصورفر؛ غلامرضا؛ غیور، فرزاد (۱۳۹۹). مقایسه معیارهای تشخیص شرکت‌های درمانده مالی با استفاده از رگرسیون لجستیک و روش‌های هوش مصنوعی. *چشم‌انداز مدیریت مالی*، ۱۰ (۱)، ۱۴۷–۱۶۶.

عنایتی طائبی، ریحانه؛ مهرآذین، علیرضا؛ جباری نوقابی، مهدی (۱۴۰۱). مقایسه توان مدل‌های آشوبی و شبکه عصبی مصنوعی در تبیین بازده غیرعادی سهام پیرامون تاریخ انتشار صورت‌های مالی سالانه. *تحقیقات حسابداری و حسابرسی*، ۱۴ (۵۳)، ۱۳۵–۱۵۴.

قربانی، فاطمه؛گرکز، منصور؛ خنکا، عبدالخالق؛ خوزین، علی؛ معطوفی، علیرضا (۱۴۰۴). الگوی پذیرش سیستم‌های حسابداری مالی مبتنی بر هوش مصنوعی. *حسابداری، امور مالی و هوش محاسباتی*، ۳ (۲)، ۲–۲۴.

کامرانی، حسین؛ عابدینی، بیژن (۱۴۰۱). تدوین مدل کشف تقلب صورت‌های مالی با استفاده از روش‌های شبکه عصبی مصنوعی و ماشین بردار پشتیبان در شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران. *دانش حسابداری و حسابرسی مدیریت*، ۱۱ (۴۱)، ۲۸۵–۳۱۴.

کریم‌پور، فاطمه(۱۴۰۲). به‌کارگیری هوش مصنوعی برای ارتقای دقت پیش‌بینی‌های مالی. *تکنولوژی در کارآفرینی و مدیریت استراتژیک*، ۲ (۳)، ۱–۵.

کهریزی، امیدعلی؛ سیدمیرزائی، سیدامیرحسین؛ علوی، سیدابوالفضل (۱۴۰۴). هوش مصنوعی در چارچوب ESGمؤسسات مالی: مرور صنعتی، پیامدهای مدیریتی و الزامات حکمرانی داده. *کنفرانس ملی مدیریت، اقتصاد و علوم اسلامی، ۱۱*.

گادفری، جین؛ گادسن، آلن؛ تراکا، آن؛همیلتون،جین؛هلمز،اسکات(۱۴۰۲). *تئوری حسابداری جلد اول*. (مترجم؛ حمید حقیقت، محمحسین صفرزاده،افسانه رفیعی) . تهران: انتشارات مرکز آموزش حسابداران خبره نشریه شماره۹.

گلشاهی، بهنام؛ مرتضی‌زاده، علیرضا (۱۴۰۳). سناریوپردازی مخاطرات گسترش هوش مصنوعی در فرایندهای مدیریت سرمایه انسانی. *مدیریت هوشمند سرمایه انسانی، ۱*(۱)، ۲۹–۶۰.

منصوری، محمد جواد؛ کرمی، غلامرضا؛ یزدانی، حمیدرضا(۱۴۰۳). شناسایی پیشران های مؤثر بر آینده حسابرسی: رویکردفراترکیب .*بررسی های حسابداری و حسابرسی، ۳۱*(۲)۴۲۷-۳۹۰.

مهرانی،آزاده؛ علیزاده، حمید؛ رسولی، عبدالرسول (۱۴۰۱). ارزیابی نقش ابزارهای هوش مصنوعی در توسعه خدمات مالی و بازاریابی. *تکنولوژی در کارآفرینی و مدیریت استراتژیک، ۱*(۱)، ۷۱–۸۲.

میرزاپور، مانا (۱۴۰۲). مروری بر اثرات هوش مصنوعی بر اهداف حسابرسی صورت‌های مالی. *همایش ملی پژوهش‌های مدیریت و علوم انسانی در ایران، ۱۶*.

نظریان، راحله؛ مظفری، فهیمه(۱۴۰۳). واکاوی ابعاد مؤثر فناوری‌های نوین بر حرفه حسابداری: کاربست فراترکیب. *بررسی‌های حسابداری و حسابرسی، ۳۱*(۴)، ۷۶۳–۷۹۳.

## References

Adnan Hammood, M., Piri, P., & Ashtab, A. (2025). Feasibility of Utilizing Advanced Artificial Intelligence Technologies to Improve Auditing Processes in the Country. *Accounting and Auditing Review*, *32*(3), 535-559. https://doi.org/10.22059/acctgrev.2025.391837.1009085. (in persian)

Ahmadi, A., & Baghishani, V. (2024). Digitalization and financial reporting: How technological innovation is shifting toward continuous accounting. *Seventh National Conference on Management Studies and Humanities in Iran*. https://civilica.com/doc/1022751. (in persian).

Al-Hattami, H. M. (2022). Impact of AIS success on decision-making effectiveness among SMEs in less developed countries. *Information Technology for Development*, *12*(2), 1-21. DOI: 10.1080/02681102.2022.2073325

Aliakbarlou, A., Mansourfar, G., & Ghayour, F. (2020). Comparing the Identifying Criteria for Financially Distressed Companies using Logistic Regression and Artificial Intelligence Methods. *Financial Management Perspective*, *10*(29), 147-166. https://doi.org/10.52547/jfmp.10.29.147. (in persian)

Alikhani,R.,& Ataei, J.(2025). The Role of Blockchain Technology in Accounting and Auditing. *Journal of Information System and Technology Auditing,1*(1).74-84. https://doi.org/10.22034/JISTA. 2025. 541245.1059. (in persian)

Al-Okaily, M. (2024). Artificial intelligence and its applications in the context of accounting and disclosure. *Journal of Financial Reporting and Accounting*, *23*(4), 1387–1401. https://doi.org/10.1108/JFRA-04-2024-0209.

Apooyin, A. (2024). The impact of artificial intelligence on financial reporting and compliance: Opportunities, challenges, and ethical considerations. *Journal of Financial Compliance*, *8*(3), 45-62.

Armoonmanesh, Z., & Pourkhorshid , H. (1404). The Effect of Artificial Intelligence Utilization in Auditing on Financial Reporting Quality: The Moderating Role of Auditor Experience. *Accounting, Finance and Computational Intelligence*, *3*(3), 1-15. https://jafci.com/index.php/jafci/article/view/172. (in persian)

Ashraf, M. (2025). Does automation improve financial reporting? Evidence from internal controls. R*eview of Accounting Studies, 30*(1), 436–479. https://doi.org/10.1007/s11142-024-09822-y

Asna-Ashari, E. (2020). The Impact of Information Technology on Financial Reporting. Ourmazd Research Journal, 12(53), 94–104.https://civilica.com/doc/1546830. (in persian)

Assidi, S., Omran, M., Rana, T., & Borgi, H. (2025). The role of AI adoption in transforming the accounting profession: A diffusion of innovations theory approach. *Journal of Accounting & Organizational Change, 21*(5), 915–936. https://doi.org/10.1108/JAOC-04-2024-0124

Athna'ashari, E. (2020). The impact of information technology on financial reporting. *Ourmazd Journal*، *(12)*53, 94–104.https://civilica.com/doc/1546830 (in persian)

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative research, 1*(3),

Azarsa'id, Y., & Rostami, S. (2023). Artificial intelligence and ethical decision-making

Azarsaeed, Y, Rostami, S.(2023). "Artificial Intelligence and Ethical Decision-Making in Accounting and Auditing: Analysis of Related Challenges." *Judgment and Decision Making in Accounting and Auditing, 2*(7). 87-114.. https://doi.org/10.30495/jdaa.2023.705528. (in persian)

Choudhary, P., Sigler, J. & Ramadas, V. (2022). The Implications of IT Environment on the Audit and Financial Reporting Quality. *PCAOB, 29* (5), 1021-1053.

Dalili, A. ., Azadi hir, K., & Archin lisar, M. . (1404). Predicting the Occurrence of Negative Stock Returns Using Artificial Intelligence Algorithms and Its Relationship with Conservative Reporting in Companies Listed on the Tehran Stock Exchange. *Accounting, Finance and Computational Intelligence*, *3*(1), 1-19. https://jafci.com/index.php/jafci/article/view/92.(in persian)

De Loë, R. C., Melnychuk, N., Murray, D., & Plummer, R. (2016). Advancing the state of policy Delphi practice: A systematic review evaluating methodological evolution, innovation, and opportunities. *Technological Forecasting and Social Change, 104*, 78-88. DOI: 10.1016/j.techfore.2015.12.009.

Enayati Tayebi, R., Mehrazeen, A., & Jabbari Noqabi, M. (2022). Comparison of the potential of chaotic models and artificial neural networks in explaining abnormal stock returns around the release date of annual financial statements. *Accounting and Auditing Research, 14*(53), 135-154. https://doi.org/10.22034/iaar.2022.151103. (in persian)

Enholm, I. M., Papagiannidis, E., Mikalef, P. & Krogstie, J. (2022). Artificial intelligence and business value: A literature review. *Information Systems Frontiers, 24*(5), 1709-1734. DOI: 10.1007/s10796-021-10186-w

Fadlalla, A. M., & Amani, F. A. (2017). Data mining applications inaccounting: A review of the literature and rganizing framework.International *Journal of Accounting Information Systems, Elsevier, 24*(C),32-58. DOI: 10.1016/j.accinf.2016.12.004.

Ghorbani, F. ., Garkaz, M., Khonaka, A., Khozein , A. ., & Matoufi, A. (1404). Artificial Intelligence-Based Financial Accounting Systems Adoption Model. *Accounting,*

*Finance and Computational Intelligence*, *3*(2). . https://jafci.com/index.php/jafci/article/view/127. (in persian)

Godfrey, J., Godson, A., Trakha, A., Hamilton, J., & Holmes, S. (2023). *Accounting theory* (Vol. 1; H. Haghighat, M. H. Safarzadeh, & A. Rafiei, Trans.). Tehran: Center for Professional Accountants' Training, Publication No. 9. (in persian)

Golshahi, B., & Mortezazadeh, A. (2024). Scenario Planning for the Risks of Expanding Artificial Intelligence in Human Capital Management Processes. *Intelligent Management of Human Capital*, *1*(1), 60-29.) . https://doi.org/10.22034/imhr.2024.480339.1011. (in Persian)

Greenman, C., Esplin, D., Johnston, R., & Richards, J. (2024). An analysis of the impact of artificial intelligence on the accounting profession. *Journal of Accounting, Ethics & Public Policy*, *25*(2), 188–?. https://doi.org/10.60154/jaepp.2024.v25n2p188

Hajihosseini, Z. (2025). A review of the impacts of artificial intelligence on the accounting profession. National .*Conference on New Findings in Management, Psychology, and Accounting, 11*. (in persian)

Hayder Yousif, H., Piri, P., & Chalaki, P. (2025). A Foresight Model for Adopting Artificial Intelligence in Financial Reporting: Emphasizing Perceived Usefulness and Ease of Use. *Financial Research Journal*, *27*(3), 660-684. https://doi.org/10.22059/frj.2024.383400.1007651. (in persian)

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, *31*(1–3), 405–440. https://doi.org/10.1016/S0165-4101(01)00018-0

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, *11*, (1).1-22. DOI: 10.1057/s41599-024-03606-0.

Hosseini, A., Jabbarzade Kangaarloye, S., Bahri Sales, J., & Sadi, R. (2021). Explaining the Obstacles to Implementing International Financial Reporting Standards; Grounded Theory Approach. *Financial Research Journal*, *23*(1), 108-133.https://doi.org/10.22059/frj.2020.292297.1006948. (in persian)

International Accounting Standards Board (IASB). (2018). *Conceptual Framework for Financial Reporting*. London: IFRS Foundation.

Jafaiean, Y. , Seyedkhani, R. , Moradpour, M. and Mohammadipour, R. (2025). Designing a Financial Strategy Model for the Social Security Organization Using Artificial Intelligence. Journal of Intelligent Strategic Management .4(4), 221-252. doi: 10.87453/bumara.2026.372301.48151. . (in persian)

Jamalimehr, M. M. (2025). Toward artificial intelligence ecosystems: Linking big data analytics with artificial intelligence. 1st International Conference on Management, Computer Science, and Artificial. https://civilica.com/doc/2600095. (in persian)

Javadi, E. (2023). The impact of artificial intelligence technology on the accounting profession. International. *Conference on Management, Accounting, and Economic Development, 12*. (in persian)

Johri, A. (2025). Impact of artificial intelligence on the performance and quality of accounting information systems and accuracy of financial data reporting. *Accounting Forum*, *49*(5), 1096–1120. https://doi.org/10.1080/01559982.2025.2451004

Kahrizi, O. A., Seyedmirzaei, S. A. H., & Alavi, S. A. (2025). Artificial intelligence within the ESG framework of financial institutions: An industry review, managerial implications, and data governance requirements. National. *11th National Conference*

*on Management, Economy & Islamic Science*..https://civilica.com/doc/2590123. (in persian)

Kamrani, H., & Abedini, B. (2022). Formulation of Financial Statement Fraud Detection Model Using Artificial Neural Network and Support Vector Machine Approaches in Companies Listed in Tehran Bahador Stock Exchange. *Journal of Management Accounting and Auditing Knowledge*, *11*(41), 285-314. (in persian)

Karimpour, F. (2023). Employing Artificial Intelligence to Enhance the Accuracy of Financial Forecasts. *Journal of Technology in Entrepreneurship and Strategic Management (JTESM)*, *2*(3), 1-5.https://doi.org/10.61838/kman.jtesm.2.3.1. (in persian).

Kokina, J., Blanchette, S., Davenport, T. H., & Pachamanova, D. (2025). Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. *International Journal of Accounting Information Systems*, *56*, 100734. https://doi.org/10.1016/j.accinf.2025.100734

Kureljusic, M., & Karger, E. (2023). Forecasting in financial accounting with artificial intelligence – A systematic literature review and future research agenda. *Journal of Applied Accounting Research*, *25*(1), 81–104. https://doi.org/10.1108/JAAR-06-2022-0146

Liao, F.-N., Zhang, C., Zhang, J.-J., Yan, X., & Chen, T.-X. (2024). Hyperbole or reality? The effect of auditors' AI education on audit report timeliness. *International Review of Financial Analysis*, *91*, 103050. https://doi.org/10.1016/j.irfa.2023.103050

Manihuruk, L. C. G., & Dewayanto, T. (2025). Peran dan tantangan Artificial Intelligence dalam kualitas pelaporan keuangan – A systematic literature review. Diponegoro *Journal of Accounting*, *14*(3).

Mansouri, M. J., Karami, G., & Yazdani, H. R. (2024). Identifying Key Drivers Influencing the Future of Auditing: A Meta-Synthesis Approach. *Accounting and Auditing Review*, *31*(2), 390-427. https://doi.org/10.22059/acctgrev.2024.380683.1008994. (in persian)

Mehrani, A. ., Alizadeh, H., & Rasouli, A. (2022). Evaluation of the Role of Artificial Intelligence Tools in the Development of Financial Services and Marketing. *Journal of Technology in Entrepreneurship and Strategic Management (JTESM)*, *1*(1), 71-82. https://journaltesm.com/index.php/journaltesm/article/view/278.(in persian)

Mirzapour, M. (2023). A review of the effects of artificial intelligence on the objectives of financial statement auditing. National *Conference on Management and Humanities Research in Iran*, *16*. (in persian)

Murphy, B., Feeney, O., Rosati, P., & Lynn, T. (2024). Exploring accounting and AI using topic modelling. *International Journal of Accounting Information Systems*, *55*, 100709. https://doi.org/10.1016/j.accinf.2024.100709

Mwachikoka, C. F. (2024). Effects of artificial intelligence on financial reporting accuracy. *World Journal of Advanced Research and Reviews*, *23*(3), 1751-1767.

Nazarian, R., & Mozafari, F. (2024). Analyzing the Effective Dimensions of Emerging Technologies on the Accounting Profession: A Meta-synthesis. *Accounting and Auditing Review*, *31*(4), 763-793.https://doi.org/10.22059/acctgrev.2024.369192.1008891. (in persian)

Odonkor, B., Kaggwa, S., Uwaoma, P. U., Hassan, A. O. & Farayola, O. A. (2024). The impactof AI on accounting practices: A review: Exploring how artificial intelligence is transforming traditional accounting methods and financial reporting. **World Journal of Advanced Research and Reviews**, 21(1), 172-188.

Oorsaji, M., Mohajer Mangoush, R., Balakhili, F., Mashkour, A., & Ghasemi, S. (2025). Investigating the role of artificial intelligence in public sector accounting. *New*

*Interdisciplinary Research in Basic Sciences and Technical and Engineering Sciences, 5*(3), 1–10. https://civilica.com/doc/2402187. (in persian)

Perdana, A., Wang, T. D., & Arifin, S. (2024). Artificial Intelligence in Accounting: Ethical Challenges and Legal Perspectives. *In Digital Transformation in Accounting and Auditing* (pp. 321–345). Springer. DOI: 10.1007/978-3-031-46209-2_11.

Polak, P. (2021). Welcome to the digital era—the impact of AI on business and society. *Society*,*58*(3), 177-178

Ranjbar, E. (2025). Opportunities and threats: Accounting in the transition to artificial intelligence. International and National *Conference on Management, Accounting, and Law Studies, 15*. https://civilica.com/doc/2438917. (in persian)

Rezaei, M., & Ahmadi, A. (2024). Identifying the Influential Factors on Financial Behavior of Investors in Emerging Markets. *Accounting, Finance and Computational Intelligence*, *2*(1), 45-56. https://jafci.com/index.php/jafci/article/view/24. (in persian)

Rezaei, N. (2024). The Future of Accounting: How AI is Reshaping the Role of Accountants in Financial Reporting. *Accounting, Finance and Computational Intelligence*, *1*(2), 53-65. https://jafci.com/index.php/jafci/article/view/12.(in persian)

Rostami, A., & Khalili Tirtashi, N. (2023). Application of artificial intelligence in financial systems from the perspective of Islamic *economics. Islamic Economic Jurisprudence Studies, 5*(2), 21–34. https://doi.org/10.22034/ejs.2023.385433.1379. (in persian)

Sahebi, M., Momayez, A., & Yadollahi Farsi, J. (2025). Intelligent Financial Services Management: A Strategic Framework for Artificial Intelligence Adoption. *Journal of Intelligent Strategic Management*, *4*(4), 95-114. https://doi.org/10.87453/bumara.2026.373601.4841. (in persian)

Shahana, T., Lavanya, V., & Bhat, A. R. (2023). State of the art in financial statement fraud detection: A systematic review. *Technological Forecasting and Social Change*, *192*, 122527. https://doi.org/10.1016/j.techfore.2023.122527.

Soleimani Amiri, G. and mohammadi sedaran, S. (2024). Auditing in the Age of Artificial Intelligence. *Journal of Accounting and Social Interests*, *14*(3), 1-36. doi: 10.22051/jaasci.2024.47350.1862. (in persian)

Sreseli, N., & Kadagishvili, N. (2023). Use of artificial intelligence for accounting and financial reporting purposes: A review of the key issues. *American International Journal of Business Management (AIJBM)*, *6*(8), 72-83.

Strauss, A., & Corbin, J. (2011). *Principles of qualitative research methods: Grounded theory, procedures, and techniques* (B. Mohammadi, Trans.). Institute for Humanities and Cultural Studies. (in persian)

Tarasi, M., Bani-Talebi Dehkordi, B., & Zamani, B. (2019). Forecasting Fraudulent Financial Reporting Through Artificial Neural Network. *Management Accounting, 12*(40), 63–79. (in persian)

Thottoli, M. M., Ahmed, E. R. & Thomas, K. V. (2022). Emerging technology and auditing practice: analysis for future directions. *European Journal of Management Studies, 27*(1), 99-119. DOI: 10.1108/EJMS-06-2021-0058

Yang, T., & Zhou, N. (2025). Artificial intelligence and the quality of corporate accounting information disclosure. *Finance Research Letters, (85)*,1077-1092. 108136. https://doi.org/10.1016/j.frl.2025.108136

Ye, A., & Chen, W. (2024). Artificial intelligence in performance management: Enhancing accounting decision support. Probe - *Accounting, Auditing and Taxation, 6*(4). https://doi.org/10.59429/paat.v6i4.8395

Yokhanehalghyani, M., bahrisales, J., Jabbarzadeh Kangarluei, S., & Zavari Rezaei, A. (2021). Combination of CDM, ANFIS & MH Algorithms in a model to determine

Fraudulent Financial-Tax Report. *Empirical Studies in Financial Accounting*, *18*(71), 87-112.https://doi.org/10.22054/qjma.2021.59092.2234. (in persian)

zare, H., hajiha, Z., & Keyghobadi, A. (2024). Investigating the impact of using artificial intelligence on the quality of the financial statement audit process. *Professional Auditing Research*, *4*(16), 38-65. https://doi.org/10.22034/jpar.2024.2011220.1224. . (in persian)

COPYRIGHT

This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

Journal of
Information System and Technology Auditing

**Review Paper**

# Platform Corporate Governance in the Digital Age: An Integrative Conceptual Framework for Smart Organizations [1]

**Masoome Kazemi [2*], Ghodratallah Barzegar [3] and Danial Hassanzadeh [4]**

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 371-398

Received: 2026.08.22
Revised: 2026.10.09
Accepted: 2026.10.30

## Abstract

Digital transformation and the expansion of platform-based business models have reshaped value creation, organizational boundaries, stakeholder relationships, and the requirements for oversight and accountability, challenging the adequacy of traditional corporate governance mechanisms in networked and ecosystem-based environments. This study aims to review and conceptually synthesize the literature on corporate governance, platform governance, ecosystem governance, data governance, and artificial intelligence governance, drawing on stakeholder theory and network theory, to conceptualize *platform corporate governance* and explain its relationship with the smart organization. The study adopts a review-conceptual approach based on the comparison, classification, and reinterpretation of previous studies. The findings suggest that platform corporate governance is neither a substitute for corporate governance nor synonymous with platform governance. Rather, it represents a coordinating architecture that interactively integrates corporate governance, platform and ecosystem governance, data and technology governance, artificial intelligence governance, and control and accountability mechanisms. From the perspectives of stakeholder theory and network theory, this architecture explains the need to redesign governance mechanisms in response to expanding organizational relationships and interdependencies. The smart organization is conceptualized as an organizational state characterized by knowledge, learning, connectivity, and intelligent decision-making, rather than as an inevitable outcome of platformization. The proposed conceptual framework elucidates the interactive relationships among different governance layers and the smart organization and may provide a basis for reconsidering governance, accountability, and risk management mechanisms in digital and platform-based companies in Iran. However, empirical validation and the development of assessment indicators are necessary for its practical application.

**Keywords**: Platform Corporate Governance; Digital Transformation; Smart Organization.
**JEL classification:** *M15, M40, O33, L86.*

---

[1] https://doi.org/10.22034/JISTA.2026.598611.1098
[1] Selected paper of the 2nd National Conference on Corporate Governance and Information Technology Risk Management
[2] Ph.D., Department of Accounting, Mazandaran Institute of Technology, Babol, Iran. (Corresponding Author). (masoomekazemi@mit.ac.ir).
[3] Associate Professor of Accounting, Faculty of Economics & Administrative Science, University of Mazandaran, Babolsar, Iran. (Gh_barzegar@umz.ac.ir).
[4] M.Sc. in Accounting, Department of Accounting, University of Mazandaran, Babolsar, Iran. (acc.danial@gmail.com).

## 1. INTRODUCTION

Digital transformation extends beyond the adoption of digital technologies in organizational activities, as it can reshape value creation, organizational structures, decision-making, control, and accountability (Vial, 2019: 118–120; Jiang & Li, 2024; Möslein, 2025: 629–632). This transformation becomes more complex in platform-based firms, where value creation depends on interactions among firms, users, complementors, developers, suppliers, and other ecosystem actors. Consequently, conventional governance mechanisms may no longer be sufficient to address the increasingly networked, data-driven, and technology-dependent nature of organizational activities (Fenwick et al., 2019: 171–174; Costabile, 2024). The central issue is therefore not whether corporate governance should be replaced by platform governance, but how corporate governance can be reconfigured to respond to platform, ecosystem, data, technology, and artificial intelligence requirements.

Recent literature emphasizes that platform governance does not eliminate the relevance of corporate governance; rather, corporate governance mechanisms can complement platform governance by strengthening oversight, accountability, and stakeholder-related decision-making (Cai & Hou, 2022; Cai, 2024). Nevertheless, the literature remains fragmented across corporate governance, platform and ecosystem governance, stakeholder and network governance, data and technology governance, and AI governance. Recent reviews also indicate that platform ecosystem governance is multidimensional and characterized by tensions such as openness versus control and data sharing versus privacy (Costabile, 2024; Pan et al., 2025; Zou et al., 2026). However, an integrated conceptual framework connecting these governance layers at the corporate level remains insufficiently developed.

Accordingly, this study conceptualizes platform corporate governance as a proposed framework for reconfiguring corporate governance architecture in platform-based and digitally enabled environments. The framework integrates conventional corporate governance mechanisms—including oversight, accountability,

transparency, control, and risk management—with platform and ecosystem governance, stakeholder and network governance, data and technology governance, and AI governance. Drawing on stakeholder and network perspectives, the study develops a conceptual framework through a review and integration of the relevant literature. The proposed framework is not an empirically tested causal model; rather, it conceptualizes platform corporate governance as a multilayered and interactive architecture and positions the smart organization as an organizational horizon whose realization depends on the alignment of governance, digital capabilities, data, organizational learning, and intelligent decision-making. The study contributes by providing an integrated conceptual language for connecting fragmented governance perspectives and by offering a basis for future empirical research and the development of indicators for assessing platform corporate governance maturity.

## 2. THEORETICAL FOUNDATIONS AND LITERATURE REVIEW

Digital transformation extends beyond the adoption of digital technologies and can reshape value creation, organizational structures, decision-making, and firms' responses to environmental changes (Vial, 2019). Platformization represents an important manifestation of this transformation, whereby digital infrastructures facilitate interactions among users, partners, developers, and other ecosystem actors, thereby extending value creation beyond traditional organizational boundaries (Fenwick et al., 2019; Costabile, 2024). Costabile (2024), based on a systematic review of 103 studies, conceptualizes digital platform ecosystem governance through five interrelated building blocks: governance structure, governance mechanisms, governance scope, contingency factors, and outcomes. Nevertheless, platformization should not be equated with digital transformation, since not all digitally transformed organizations operate as platforms and platform-based transformation is not necessarily linear or unidirectional (Vial, 2019; Zou et al., 2026).

Corporate governance concerns the relationships and mechanisms through which strategic direction, managerial oversight, accountability, control, and risk management are exercised, whereas platform governance primarily addresses the rules, interactions, access, participation, and coordination of actors within a platform ecosystem (OECD, 2023; Halckenhaeusser et al., 2020; Pan et al., 2025). Platform governance therefore does not replace corporate governance; rather, platform-based firms continue to face conventional corporate governance responsibilities while simultaneously confronting new requirements arising from platform ecosystems (Cai & Hou, 2022; Cai, 2024). Accordingly, this study conceptualizes platform corporate governance as the redesign and extension of corporate governance architecture to digital and platform environments, integrating conventional governance mechanisms with ecosystem, stakeholder, network, data, technology, and artificial intelligence governance. From a stakeholder and network perspective, this architecture recognizes the broader interdependencies among firms, users, complementors, and other ecosystem actors while distinguishing participation in value creation from formal governance rights.

Furthermore, increasing dependence on data, digital technologies, algorithms, and artificial intelligence introduces new governance requirements concerning data quality, privacy, security, transparency, explainability, bias, accountability, human oversight, and technological risk (Jiang & Li, 2024). These dimensions are mutually interdependent with corporate governance rather than subordinate to it. Finally, the smart organization is conceptualized not as an inevitable stage following platformization, but as an organizational state or horizon that depends on the alignment of governance, digital capabilities, data and technology, organizational learning, and intelligent decision-making. Thus, the proposed framework adopts an interactive and multidimensional perspective in which platform corporate governance serves as a connecting architecture among corporate governance, platform ecosystem governance, data and technology governance, and AI governance,

while sustainability is considered an independent organizational outcome or orientation rather than a defining component of the smart organization.

## 3. DISCUSSION AND CONCLUSION

This study aimed to explain how corporate governance evolves in response to digital transformation and platformization and to propose a conceptual framework for supporting the transition toward a smart organization. The findings indicate that platform-based organizations do not require a choice between corporate governance and platform governance; rather, they require a reconfiguration of the corporate governance architecture to accommodate an environment in which value creation, information, decision-making, and risk are increasingly shaped by networks of stakeholders, data, and technology. From a stakeholder and network perspective, the governance domain therefore extends beyond the boundaries of the firm to encompass its relationships with users, partners, service providers, and other ecosystem actors. However, participation in value creation does not, by itself, imply voting rights or board representation; the nature and extent of stakeholder participation in governance should be determined according to legal rights, affectedness, decision significance, and associated risks.

The conceptual contribution of this study is the introduction of the term platform corporate governance as an integrated conceptual construct rather than as an established independent theory. It links core corporate governance responsibilities—including strategic oversight, accountability, risk management, and control—with the governance requirements of platforms and ecosystems, data and technology, and artificial intelligence. Accordingly, platform corporate governance is neither a substitute for corporate governance nor a synonym for platform governance; rather, it represents an approach to adapting and redesigning corporate governance for digital and platform-based environments. The proposed framework consequently adopts an interactive and multilayer architecture rather than a linear sequence from digital transformation to platformization

and then to a smart organization. From a practical perspective, the framework can inform the reassessment of board responsibilities, internal controls, risk management, reporting, and oversight of data, technology, and AI. Nevertheless, the framework is conceptual and has not been empirically validated. Future research should therefore develop and validate measures of platform corporate governance and examine their relationships with reporting quality, internal control effectiveness, risk management, transparency, stakeholder trust, innovation, and organizational performance across different industries and institutional contexts.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

مقالهٔ ترویجی

# حاکمیت شرکتی پلتفرمی در عصر دیجیتال: چارچوب مفهومی یکپارچه برای سازمان‌های هوشمند[1]

معصومه کاظمی[2]*، قدرت اله برزگر[3] و دانیال حسن‌زاده[4]

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۳۷۱ – ۳۹۸

تاریخ دریافت: ۱۴۰۵/۰۵/۳۱
تاریخ بازنگری: ۱۴۰۵/۰۷/۱۷
تاریخ پذیرش: ۱۴۰۵/۰۸/۰۸

## چکیده

*تحول دیجیتال و گسترش مدل‌های کسب‌وکار پلتفرمی، منطق خلق ارزش، مرزهای سازمان، روابط ذینفعان و الزامات نظارت و پاسخگویی را دگرگون کرده و کفایت سازوکارهای سنتی حاکمیت شرکتی را در محیط‌های شبکه‌ای و اکوسیستمی با چالش مواجه ساخته است. هدف پژوهش حاضر، مرور و ترکیب مفهومی ادبیات حاکمیت شرکتی، حاکمیت پلتفرمی، حاکمیت اکوسیستم، حاکمیت داده و هوش مصنوعی، با تکیه بر نظریه ذینفعان و نظریه شبکه، و ارائه چارچوبی برای مفهوم‌پردازی «حاکمیت شرکتی پلتفرمی» و تبیین ارتباط آن با سازمان هوشمند است. پژوهش از نوع مروری ـ مفهومی بوده و با مقایسه، دسته‌بندی و بازتفسیر مطالعات پیشین انجام شده است. یافته‌ها نشان می‌دهد حاکمیت شرکتی پلتفرمی، جایگزین حاکمیت شرکتی یا حاکمیت پلتفرمی نیست، بلکه معماری هماهنگ‌کننده‌ای است که حاکمیت شرکتی، پلتفرم و اکوسیستم، داده، فناوری و هوش مصنوعی و سازوکارهای کنترل و پاسخگویی را به‌صورت تعاملی پیوند می‌دهد. بر مبنای نظریه ذینفعان و شبکه، این معماری با گسترش روابط و وابستگی‌های سازمانی، ضرورت بازطراحی سازوکارهای حاکمیت را تبیین می‌کند. سازمان هوشمند نیز یک وضعیت سازمانی مبتنی بر دانش، یادگیری، اتصال و تصمیم‌گیری هوشمند است و پیامد قطعی پلتفرمی‌شدن تلقی نمی‌شود. چارچوب مفهومی پیشنهادی، با تبیین پیوندهای تعاملی میان لایه‌های مختلف حاکمیت و سازمان هوشمند، می‌تواند مبنایی برای بازنگری سازوکارهای حاکمیت، پاسخ‌گویی و مدیریت ریسک در شرکت‌های دیجیتال و پلتفرمی ایران فراهم کند؛ بااین‌حال، اعتبارسنجی تجربی و توسعه شاخص‌های ارزیابی آن برای کاربرد عملی ضروری است.*

**واژه‌های کلیدی:** *حاکمیت شرکتی پلتفرمی، تحول دیجیتال، سازمان هوشمند.*

**طبقه‌بندی موضوعی:** *M15, M40, O33, L86.* .

---

[1] https://doi.org/10.22034/JISTA.2026.598611.1098

[1] مقاله منتخب دومین همایش ملی حاکمیت شرکتی و مدیریت ریسک‌های فناوری اطلاعات

[2] گروه حسابداری، موسسه آموزش عالی صنعتی مازندران، بابل، ایران. (نویسنده مسئول). (masoomekazemi@mit.ac.ir)

[3] دانشیار گروه حسابداری، دانشکده علوم اقتصادی و اداری، دانشگاه مازندران، بابلسر، ایران. (Gh_barzegar@umz.ac.i)

[4] دانشجوی کارشناسی ارشد حسابداری، دانشکده علوم اقتصادی و اداری، دانشگاه مازندران، بابلسر، ایران. (acc.danial@gmail.com)

**مقدمه**

تحول دیجیتال فرایندی فراتر از به‌کارگیری فناوری‌های دیجیتال در فعالیت‌های سازمانی است؛ این فرایند می‌تواند مسیرهای خلق ارزش و ساختارهای سازمانی را تحت تأثیر قرار داده و سازمان‌ها را به بازنگری در شیوه‌های فعالیت و سازمان‌دهی خود وادار کند(ویال[1]، ۲۰۱۹: ۱۱۸).گسترش داده، هوش مصنوعی، زیرساخت‌های دیجیتال و پلتفرم‌ها موجب شده است که فناوری و داده از ابزارهای پشتیبان فعالیت‌های سازمانی به مؤلفه‌هایی اثرگذار بر تصمیم‌گیری، کنترل، نظارت و پاسخگویی تبدیل شوند( جیانگ و لی[2] ۲۰۲۴: ۶۳ ؛ موسلاین[3]، ۲۰۲۵: ۶۲۹). در شرکت‌های پلتفرمی، این تحول پیچیده‌تر است؛ زیرا خلق ارزش به تعامل و هماهنگی میان شرکت و مجموعه‌ای از کاربران، مکمل‌ها، توسعه‌دهندگان، تأمین‌کنندگان و سایر بازیگران اکوسیستم وابسته است و در نتیجه، مرزهای سازمانی و سازوکارهای سنتی کنترل و هماهنگی با شبکه‌ای گسترده‌تر از روابط درهم‌تنیده می‌شوند(فنویک، مک‌کهری و ورمولن[4] ۲۰۱۹: ۱۷۲ ؛ کوستابیله[5]، ۲۰۲۴: ۱). .بنابراین، مسئله حاکمیت در چنین شرکت‌هایی صرفاً به هدایت و کنترل فعالیت‌های درون شرکت محدود نمی‌شود، بلکه تنظیم روابط اکوسیستمی، مدیریت داده و فناوری و پاسخگویی در برابر پیامدهای تصمیم‌های دیجیتال را نیز دربرمی‌گیرد.

این شرایط، پرسش اساسی درباره کفایت معماری متعارف حاکمیت شرکتی در محیط‌های پلتفرمی و دیجیتال را مطرح می‌کند. ادبیات اولیه حاکمیت پلتفرم بر تفاوت منطق پلتفرم‌ها با سازمان‌های سلسله‌مراتبی و ضرورت توجه به سازوکارهای حاکمیتی متناسب با روابط شبکه‌ای تأکید کرده است(فنویک و همکاران، ۲۰۱۹: ۱۷۲). بااین‌حال، پژوهش‌های بعدی نشان داده‌اند که حاکمیت پلتفرمی به معنای حذف حاکمیت شرکتی نیست و سازوکارهای حاکمیت شرکتی می‌توانند از حاکمیت پلتفرم پشتیبانی کنند؛ برای مثال، هیئت‌مدیره، مدیران مستقل و سازوکارهای مرتبط با ذینفعان می‌توانند در هدایت و پاسخگویی شرکت پلتفرمی نقش داشته باشند(کای و هو[6]،۲۰۲۲). هم‌زمان، فناوری‌های داده‌محور و هوش مصنوعی نیز ساختارهای

[1] Vial
[2] Jiang, Li
[3] Möslein
[4] Fenwick , McCahery and Vermeulen
[5] Costabile
[6] Cai and Hou

سنتی اطلاعات، نظارت و تصمیم‌گیری شرکتی را تغییر داده و در کنار فرصت‌های جدید، مسائل مربوط به شفافیت، مسئولیت‌پذیری، کنترل و ریسک را ایجاد کرده‌اند(کای و هو،۲۰۲۲؛ موسلاین،۲۰۲۵: ۶۲۹). از این منظر، مسئله اصلی نه انتخاب میان «حاکمیت شرکتی» و «حاکمیت پلتفرمی»، بلکه چگونگی بازآرایی و هماهنگ‌سازی معماری حاکمیت شرکت در مواجهه با منطق پلتفرمی، شبکه‌ای و داده‌محور است.

با وجود گسترش این ادبیات، مطالعات موجود عمدتاً در جریان‌های نسبتاً مجزا توسعه یافته‌اند. مرور کوستابیله(۲۰۲۴: ۱) بر ۱۰۳ مقاله مجله‌ای و مقاله کنفرانسی، پراکندگی ادبیات حاکمیت اکوسیستم پلتفرمی را نشان می‌دهد و این ادبیات را در قالب پنج بُعد ساختار حاکمیت، سازوکارهای حاکمیت، دامنه حاکمیت، عوامل اقتضایی و پیامدها صورت‌بندی می‌کند. همچنین مرور (پن، لوئو، لیو و ژانگ [1]، ۲۰۲۵) بر چندبعدی بودن حاکمیت پلتفرمی تأکید دارد و مرور زو، وو و وانگ [2](۲۰۲۶) بر پایه ۱۵۲ مطالعه، نشان می‌دهد که تحول دیجیتال مبتنی بر اکوسیستم‌های پلتفرمی فرایندی خطی نیست و با تنش‌هایی مانند گشودگی در برابر کنترل [3] و اشتراک‌گذاری داده در برابر حریم خصوصی [4] همراه است. با وجود این پیشرفت‌ها، هنوز نیاز به چارچوبی وجود دارد که اصول و سازوکارهای حاکمیت شرکتی را با حاکمیت پلتفرم و اکوسیستم، ذینفعان و شبکه، داده و فناوری و حاکمیت هوش مصنوعی در سطح معماری حاکمیت شرکت به یکدیگر مرتبط کند. این خلأ، مبنای شکل‌گیری مفهوم پیشنهادی«حاکمیت شرکتی پلتفرمی»در پژوهش حاضر است.

در این پژوهش، «حاکمیت شرکتی پلتفرمی» به‌عنوان یک سازه مفهومی پیشنهادی برای بازآرایی معماری حاکمیت شرکت‌های پلتفرمی در نظر گرفته می‌شود؛ معماری‌ای که در آن سازوکارهای بنیادین حاکمیت شرکتی، شامل نظارت، پاسخگویی، شفافیت، کنترل و مدیریت ریسک، با الزامات حاکمیت پلتفرم و اکوسیستم، حاکمیت ذینفعان و شبکه و حاکمیت داده، فناوری و هوش مصنوعی هماهنگ می‌شوند. مبنای نظری این صورت‌بندی، ترکیب دیدگاه ذینفعان و نظریه شبکه [5] است؛ در این ترکیب نظری، دیدگاه ذینفعان عمدتاً مبنای تحلیل حقوق،

[1] Pan, Luo , Liu & Zhang
[2] Zou , Wu , and Wang
[3] openness versus control
[4] data sharing versus privacy
[5] Visconti. Corporate Governance, Digital Platforms and Network Theory

منافع و پاسخگویی در برابر گروه‌های متأثر از سازمان را فراهم می‌کند، در حالی که نظریه شبکه برای تبیین وابستگی متقابل، روابط و جریان‌های تعامل میان بازیگران اکوسیستم به کار گرفته می‌شود. بنابراین، روابط میان لایه‌های مختلف حاکمیت، خطی و یک‌سویه فرض نمی‌شود؛ بلکه به‌صورت تعاملی در نظر گرفته می‌شود، به‌گونه‌ای که طراحی پلتفرم، الزامات داده و فناوری و ریسک‌های دیجیتال می‌توانند بر نظارت و کنترل شرکت اثر بگذارند و تصمیم‌های حاکمیتی نیز می‌توانند بر طراحی و استفاده از فناوری و روابط اکوسیستمی اثرگذار باشند.

هدف پژوهش حاضر، تبیین مفهوم حاکمیت شرکتی پلتفرمی و ارائه یک چارچوب مفهومی برای سازمان‌دهی لایه‌ها و سازوکارهای آن و تشریح پیوند مفهومی این معماری با افق سازمان هوشمند است. پژوهش از نظر روش‌شناختی یک مطالعه مروری ـ مفهومی است که با بررسی و یکپارچه‌سازی ادبیات مرتبط، استخراج مفاهیم کلیدی، مقایسه جریان‌های نظری و بازتفسیر روابط میان آن‌ها، به تدوین چارچوب پیشنهادی می‌پردازد؛ ازاین‌رو، چارچوب ارائه‌شده یک مدل تجربی آزمون‌شده یا رابطه علّی اثبات‌شده نیست. این رویکرد با مطالعات مروری و چارچوب‌سازی مفهومی اخیر در حوزه حاکمیت اکوسیستم‌های پلتفرمی و تحول دیجیتال هم‌راستا است(کوستابیله، ۲۰۲۴: ۱؛ زو و همکاران، ۲۰۲۶). یافته حاصل از یکپارچه‌سازی ادبیات نشان می‌دهد که حاکمیت شرکتی پلتفرمی را می‌توان به‌عنوان یک معماری چندلایه و تعاملی در نظر گرفت که در هسته آن حاکمیت شرکتی قرار دارد و در تعامل با حاکمیت پلتفرم و اکوسیستم، ذینفعان و شبکه، داده و فناوری و هوش مصنوعی شکل می‌گیرد. در این معماری، سازمان هوشمند نه به‌عنوان مرحله‌ای قطعی یا اجتناب‌ناپذیر پس از پلتفرمی‌شدن، بلکه به‌عنوان یک افق سازمانی در نظر گرفته می‌شود که تحقق آن به هم‌راستایی حاکمیت، قابلیت‌های دیجیتال، داده، یادگیری سازمانی و سازوکارهای تصمیم‌گیری هوشمند وابسته است. بر این اساس، دستاورد نظری پژوهش، ارائه یک صورت‌بندی مفهومی مشترک برای پیوند و یکپارچه‌سازی جریان‌های پراکنده ادبیات و صورت‌بندی مفهوم حاکمیت شرکتی پلتفرمی است؛ و از نظر کاربردی، چارچوب پیشنهادی می‌تواند مبنایی برای هیئت‌مدیره، مدیران، کمیته‌های تخصصی و نهادهای سیاست‌گذار در شناسایی مسئولیت‌های مرتبط با پلتفرم، داده، فناوری، هوش مصنوعی، روابط اکوسیستمی و مبنایی مفهومی برای توسعه شاخص‌های ارزیابی آمادگی و بلوغ حاکمیت شرکتی پلتفرمی در پژوهش‌های آتی فراهم کند.

## مبانی نظری و پیشینه پژوهش

### تحول دیجیتال، پلتفرمی‌شدن و تغییر منطق سازمان

تحول دیجیتال فرایندی است که در آن فناوری‌های دیجیتال با ایجاد تغییر در مسیرهای خلق ارزش، ساختارهای سازمانی و شیوه‌های پاسخ‌گویی به تغییرات محیطی، منطق فعالیت و سازمان‌دهی شرکت‌ها را دگرگون می‌کنند(ویال، ۲۰۱۹: ۱۱۸). پلتفرمی‌شدن نیز یکی از نمودهای مهم این تحول است که در آن سازمان به‌جای اتکای صرف بر فرایندهای درون‌سازمانی، از زیرساخت‌ها و سازوکارهای دیجیتال برای تسهیل تعامل میان گروه‌های مختلف کاربران، شرکا، توسعه‌دهندگان و سایر بازیگران اکوسیستم استفاده می‌کند(فنویک و همکاران، ۲۰۱۹: ۱۷۱). در سازمان‌های پلتفرمی، خلق ارزش بیش از پیش به تعامل میان مجموعه‌ای از بازیگران وابسته می‌شود و ازاین‌رو، مرزهای سازمانی سنتی با شبکه‌ای از روابط و وابستگی‌های متقابل میان شرکت، کاربران و مکمل‌ها پیوند می‌خورد(فنویک و همکاران، ۲۰۱۹: ۱۷۲ ؛ کوستابیله، ۲۰۲۴: ۱–۳). مرور نظام‌مند کوستابیله(۲۰۲۴: ۱) بر مبنای ۱۰۳ مقاله و مقاله کنفرانسی نشان می‌دهد که ادبیات حاکمیت اکوسیستم پلتفرمی از مفاهیم متنوعی تشکیل شده و برای یکپارچه‌سازی آن می‌توان پنج مؤلفه اصلی شامل ساختار حاکمیت، سازوکارهای حاکمیت، دامنه حاکمیت، عوامل اقتضایی و پیامدها را در نظر گرفت(کوستابیله، ۲۰۲۴: ۱–۳).

بااین‌حال، پلتفرمی‌شدن را نمی‌توان معادل تحول دیجیتال دانست، زیرا همه سازمان‌های دیجیتال الزاماً پلتفرم نیستند و تحول دیجیتال می‌تواند از مسیرهای مختلفی غیر از ایجاد یا توسعه پلتفرم تحقق یابد(ویال، ۲۰۱۹؛ زو و همکاران، ۲۰۲۶). همچنین، شواهد حاصل از مرور دامنه‌ای زو و همکاران (۲۰۲۶) بر پایه ۱۵۲ مطالعه نشان می‌دهد که تحول دیجیتال مبتنی بر پلتفرم فرایندی خطی و یک‌جهته نیست، بلکه تحت تأثیر تعامل و تنش میان ابعادی همچون گشودگی در برابر کنترل، کارایی در برابر تاب‌آوری، و اشتراک‌گذاری داده در برابر حریم خصوصی[1] قرار دارد. در نهایت، مقاله زو و همکاران نشان می‌دهد که حاکمیت پلتفرمی نقش مهمی در هماهنگ‌کردن این تعارض‌ها و ایجاد ارزش برای ذینفعان دارد(زو و همکاران، ۲۰۲۶).

[1]openness versus control, efficiency versus resilience, and data sharing versus privacy

## تمایز حاکمیت شرکتی، حاکمیت پلتفرمی و حاکمیت شرکتی پلتفرمی

حاکمیت شرکتی به مجموعه روابط و سازوکارهایی مربوط است که میان هیئت‌مدیره، مدیریت، سهامداران و سایر ذینفعان شرکت برقرار می‌شود و از طریق آن جهت‌گیری راهبردی شرکت، نظارت بر مدیریت، پاسخ‌گویی، کنترل و مدیریت ریسک دنبال می‌شود(سازمان همکاری و توسعه اقتصادی[1]،۲۰۲۳: ۸). در این چارچوب، هیئت‌مدیره مسئولیت‌هایی همچون هدایت راهبردی، نظارت بر عملکرد مدیریت، اطمینان از وجود سازوکارهای مناسب کنترل و مدیریت ریسک و توجه به منافع ذینفعان را بر عهده دارد(سازمان همکاری و توسعه اقتصادی، ۲۰۲۳: ۳۴). همچنین، حاکمیت شرکتی را می‌توان مجموعه‌ای از سازوکارها و ترتیباتی دانست که از طریق آن‌ها نحوه هدایت و کنترل شرکت و روابط میان مدیران، مالکان و سایر ذینفعان تنظیم می‌شود و از منافع سرمایه‌گذاران در برابر مسائل ناشی از جدایی مالکیت و کنترل حمایت می‌شود(شلایفر و ویشنی[2]، ۱۹۹۷: ۷۳۷). این دیدگاه، مبنایی برای بررسی چگونگی بازطراحی سازوکارهای حاکمیت شرکتی در مواجهه با تحول دیجیتال و محیط‌های پلتفرمی فراهم می‌کند. در مقابل، حاکمیت پلتفرمی بیشتر به نحوه تنظیم تعاملات، مشارکت، دسترسی و رفتار بازیگران حاضر در پلتفرم و اکوسیستم آن مربوط می‌شود و موضوعاتی مانند قواعد مشارکت، دسترسی، کنترل، همکاری و سازوکارهای هماهنگی میان پلتفرم و کاربران یا مکمل‌ها را دربرمی‌گیرد(پن و همکاران، ۲۰۲۵؛ هالکن‌هویزر، فوردرر و هاینزل[3] ۲۰۲۰) ). مرور ادبیات هالکن‌هویزر و همکاران (۲۰۲۰) نشان می‌دهد که سازوکارهای حاکمیت پلتفرمی را می‌توان در چهار دسته کلی همکاری، تأمین منابع، کنترل و بازار طبقه‌بندی کرد. یانوفسکی، استیوز و باگوما[4](۲۰۱۸) حاکمیت پلتفرمی را الگویی برای هماهنگ‌سازی داده، خدمات، فناوری و بازیگران مختلف در بستر پلتفرم و ایجاد ظرفیت برای خلق ارزش مشترک می‌دانند؛ رویکردی که بر تحول روابط میان بازیگران و تعامل متقابل آنان تأکید دارد. این دیدگاه نشان می‌دهد که حاکمیت پلتفرمی فراتر از کنترل مستقیم بوده و به سازوکارهای هماهنگی و مشارکت میان بازیگران متکی است(یانوفسکی و همکاران، ۲۰۱۸ ). همچنین، لو، ژو، و فن[5](۲۰۲۳: ۳) نشان می‌دهند که

[1] OECD
[2] Shleifer & Vishny
[3] Halckenhaeusser , Foerderer and Heinzl
[4] Janowski , Estevez , Baguma
[5] Lu, , Zhou, and Fan

حاکمیت پلتفرمی صرفاً به سازوکارهای درون شرکت محدود نیست، بلکه تعامل میان شرکت پلتفرمی، دولت، بازار و جامعه را دربرمی‌گیرد و در سطوح حاکمیت داخلی، بیرونی و حکمرانی مشترک شکل می‌یابد. این دیدگاه، ضرورت توجه به روابط چندجانبه و ذینفعان مختلف را در طراحی سازوکارهای حاکمیت پلتفرمی تقویت می‌کند(لو و همکاران،۲۰۲۳: ۳).

بنابراین، حاکمیت پلتفرمی جایگزین حاکمیت شرکتی نیست، زیرا حتی شرکت‌های پلتفرمی همچنان با مسائل مربوط به مسئولیت هیئت‌مدیره، پاسخ‌گویی، کنترل داخلی، مدیریت ریسک و شفافیت شرکتی مواجه‌اند(کای، ۲۰۲۴؛ کای و هو، ۲۰۲۲).کای و هو(۲۰۲۲) استدلال می‌کنند که حاکمیت شرکتی می‌تواند زیربنای حاکمیت پلتفرمی باشد و در عین حال، الزامات جدید ناشی از مدل کسب‌وکار پلتفرمی باید در معماری حاکمیت شرکت مورد توجه قرار گیرد. فن‌ویک و ورمولن[1](۲۰۱۹)نشان می‌دهند که پلتفرمی‌شدن با تغییر در منطق خلق ارزش، تعاملات اکوسیستمی و نقش داده و فناوری، بازاندیشی در سازوکارهای سنتی حاکمیت شرکتی را ضروری می‌سازد؛ موضوعی که تداوم اهمیت حاکمیت شرکتی در محیط پلتفرمی را نیز تأیید می‌کند(فن‌ویک و ورمولن، ۲۰۱۹ ؛ کای و هو، ۲۰۲۲؛ کای، ۲۰۲۴). بر این اساس، با تلفیق حاکمیت شرکتی با حاکمیت پلتفرمی و اکوسیستمی، حاکمیت داده و فناوری و حاکمیت هوش مصنوعی، پژوهش حاضر مفهوم «حاکمیت شرکتی پلتفرمی» را به‌عنوان چارچوبی برای بازطراحی معماری حاکمیت شرکتی در محیط دیجیتال و پلتفرمی مفهوم‌پردازی می‌کند(کای، ۲۰۲۴؛ کوستابیله[2]، ۲۰۲۴).

## حاکمیت شرکتی پلتفرمی: گذار از حاکمیت شرکتی به حاکمیت اکوسیستم دیجیتال

تحول دیجیتال و پلتفرمی‌شدن، دامنه حاکمیت را از مرزهای شرکت به روابط میان شرکت، کاربران، مکمل‌ها، شرکا و سایر بازیگران اکوسیستم گسترش داده و ضرورت بازطراحی معماری حاکمیت شرکتی را ایجاد کرده است(کوستابیله، ۲۰۲۴: ۳-۱؛ کای، ۲۰۲۲؛ فن‌ویک و همکاران، ۲۰۱۹). در این پژوهش، حاکمیت شرکتی پلتفرمی به‌عنوان نظام یکپارچه ساختارهای حاکمیتی، حقوق تصمیم‌گیری، سازوکارهای کنترل و هماهنگی، قواعد تعامل ذینفعان،

[1] Fenwick & Vermeulen
[2] Costabile

حاکمیت داده و فناوری، حاکمیت هوش مصنوعی، شفافیت، پاسخگویی و مدیریت ریسک برای هدایت و نظارت بر شرکت پلتفرمی و اکوسیستم وابسته به آن تعریف می‌شود. بر این اساس، حاکمیت شرکتی پلتفرمی نه جایگزین حاکمیت شرکتی و نه مترادف حاکمیت پلتفرمی است، بلکه سازوکاری برای انطباق حاکمیت شرکتی با ویژگی‌های اکوسیستم‌های دیجیتال محسوب می‌شود(جیانگ و لی، ۲۰۲۴؛ کای،۲۰۲۲).

در این چارچوب، ساختار حاکمیت، دامنه حاکمیت و سازوکارهای کنترل، اعتماد، همکاری و بازبودن باید متناسب با ویژگی‌های پلتفرم و شرایط اکوسیستم تنظیم شوند(کوستابیله، ۲۰۲۴: ۴).همچنین، توزیع حقوق کنترل و حقوق تصمیم‌گیری میان مالک پلتفرم و سایر بازیگران، یکی از محورهای اساسی حاکمیت پلتفرمی است و می‌تواند به الگوهای یکپارچه، مشارکتی، تنظیم‌شده یا الگوریتمی منجر شود(اسپرینگر، راندهاوا، جووانوویچ، ریتالا، و پیلر[1]، ۲۰۲۵). افزون بر این، وابستگی فزاینده به داده، فناوری و الگوریتم‌ها، حاکمیت داده و هوش مصنوعی را به بخشی از معماری حاکمیت تبدیل کرده و الزامات جدیدی برای شفافیت، قابلیت ممیزی، پاسخگویی و نظارت انسانی ایجاد می‌کند(لاکس[2]، ۲۰۲۴؛ نوولی، تادئو و فلوریدی[3]، ۲۰۲۴؛ جیانگ و لی، ۲۰۲۴). ازاین‌رو، حاکمیت شرکتی پلتفرمی باید میان کنترل و استقلال، نوآوری و پاسخگویی، اشتراک‌گذاری داده و حفاظت از حریم خصوصی و خلق ارزش و توزیع ارزش در اکوسیستم تعادل برقرار کند(اسپرینگر و همکاران، ۲۰۲۵؛ کوستابیله، ۲۰۲۴: ۷). در نتیجه، حاکمیت شرکتی پلتفرمی در این پژوهش به‌عنوان یک معماری چندلایه و تعاملی برای پیوند حاکمیت شرکتی با حاکمیت پلتفرمی، اکوسیستمی، داده، فناوری و هوش مصنوعی و فراهم‌کردن زمینه گذار سازمان به وضعیت هوشمند مفهوم‌پردازی می‌شود.

## نظریه ذینفعان و حاکمیت پلتفرمی

در اکوسیستم‌های پلتفرمی، خلق ارزش را نمی‌توان صرفاً حاصل تعامل دوجانبه شرکت و مشتری دانست، بلکه پیکربندی روابط میان گروه‌های مختلف ذینفعان و سازوکارهای حاکمیتی بر شکل‌گیری و تداوم خلق ارزش مشترک اثرگذار است(زیاماری[4]، ۲۰۲۶).گسترش مرزهای

[1] Springer, , Randhawa, , Jovanovic, , Ritala, , & Piller
[2] Laux
[3] Novelli, Taddeo, & Floridi
[4] Zeamari

سازمان در محیط پلتفرمی باعث می‌شود ارزش‌آفرینی و تصمیم‌گیری شرکت به طیف گسترده‌تری از بازیگران وابسته باشد و در نتیجه، توجه به ذینفعان در طراحی سازوکارهای حاکمیتی اهمیت بیشتری پیدا کند(کوستابیله، ۲۰۲۴؛ کای، ۲۰۲۴). در پلتفرم‌های دیجیتال،کاربران، توسعه‌دهندگان، ارائه‌دهندگان خدمات، شرکای تجاری و سایر مشارکت‌کنندگان می‌توانند در فرایند خلق ارزش نقش داشته باشند و تصمیمات شرکت نیز می‌تواند بر منافع و حقوق این گروه‌ها اثر بگذارد(کای،۲۰۲۴؛ کای و هو، ۲۰۲۲).

از این منظر، حاکمیت شرکتی پلتفرمی نیازمند سازوکارهایی برای شناسایی منافع ذینفعان، دریافت اطلاعات و دیدگاه‌های آنان و پاسخ‌گویی نسبت به آثار تصمیمات پلتفرم است. بااین‌حال، مشارکت ذینفعان الزاماً به معنای اعطای حق رأی یا عضویت رسمی آنان در هیئت‌مدیره نیست و می‌تواند از طریق سازوکارهای اطلاعاتی، مشورتی، کمیته‌های تخصصی، مشارکت در فرایندهای تصمیم‌گیری یا سازوکارهای رسیدگی به شکایات نیز تحقق یابد.

## نظریه شبکه، حاکمیت اکوسیستم و سازوکارهای پلتفرمی

نظریه شبکه امکان تحلیل سازمان پلتفرمی را به‌عنوان مجموعه‌ای از روابط متقابل میان بازیگران فراهم می‌کند که در آن وابستگی‌های اطلاعاتی، اقتصادی و فناورانه فراتر از مرزهای رسمی شرکت گسترش می‌یابد(ویسکونتی[1]،۲۰۲۰: ۱۷۹). در چنین محیطی، پلتفرم صرفاً یک زیرساخت فنی نیست، بلکه نقطه اتصال مجموعه‌ای از بازیگران و روابط است که هماهنگی میان آنان بر خلق و توزیع ارزش اثر می‌گذارد(ویسکونتی، ۲۰۲۰؛ کوستابیله، ۲۰۲۴).

حاکمیت اکوسیستم پلتفرمی نیز ازاین‌رو به تعیین قواعد تعامل، تخصیص حقوق و مسئولیت‌ها، تنظیم دسترسی، هماهنگی بازیگران و ایجاد سازوکارهای کنترل و همکاری میان اعضای اکوسیستم مربوط می‌شود(کوستابیله، ۲۰۲۴؛ هالکن‌هویزر و همکاران، ۲۰۲۰). کوستابیله (۲۰۲۴) با تفکیک ساختار، سازوکار، دامنه، عوامل اقتضایی و پیامدها نشان می‌دهد که حاکمیت اکوسیستم را نمی‌توان به یک ابزار یا سازوکار منفرد تقلیل داد و طراحی آن باید متناسب با شرایط و ویژگی‌های اکوسیستم انجام شود(کوستابیله، ۲۰۲۴).

[1] Visconti

در محیط‌های پلتفرمی، حاکمیت می‌تواند از سازوکارهای متمرکز درون پلتفرم فراتر رفته و به‌صورت شبکه‌ای و با مشارکت بازیگران بیرونی در فرایندهای تصمیم‌گیری و سیاست‌گذاری شکل گیرد؛ رویکردی که ضمن افزایش ظرفیت مشارکت و پاسخگویی، چالش‌هایی را نیز برای توزیع مسئولیت و حفظ پاسخگویی ایجاد می‌کند(کاپلان، ۲۰۲۳). مطالعات جدید نیز بر چندلایه‌بودن حاکمیت در سازمان‌های پلتفرمی تأکید دارند و نشان می‌دهند که شرکت‌های دارای ساختارهای پلتفرمی ممکن است هم‌زمان با واحدهای داخلی، شرکای اصلی، توسعه‌دهندگان شخص ثالث و سایر بازیگران اکوسیستم تعامل داشته باشند و برای این سطوح به سازوکارهای حاکمیتی متفاوت نیاز داشته باشند(شریک، اوندروس، ویشه و کرچمار[1]، ۲۰۲۵). در چارچوب پیشنهادی پژوهش، نظریه ذینفعان مبنایی برای تحلیل منافع، حقوق و مسئولیت‌های شرکت در برابر گروه‌های متأثر از تصمیم‌های سازمان فراهم می‌کند؛ در مقابل، نظریه شبکه بر وابستگی متقابل بازیگران، روابط میان آن‌ها و جریان‌های اطلاعاتی و فناورانه در اکوسیستم تمرکز دارد. تلفیق این دو دیدگاه امکان می‌دهد حاکمیت شرکتی پلتفرمی هم از منظر پاسخ‌گویی شرکت در برابر ذینفعان و هم از منظر هماهنگی و تنظیم روابط شبکه‌ای تحلیل شود.

## حاکمیت داده و فناوری در معماری حاکمیت شرکتی پلتفرمی

افزایش وابستگی سازمان‌های دیجیتال به داده و فناوری موجب شده است که حاکمیت شرکتی دیگر نتواند موضوعات فناوری را صرفاً در سطح عملیاتی سازمان دنبال کند و لازم است پیامدهای داده و فناوری در سطح تصمیم‌گیری و نظارت شرکتی نیز مورد توجه قرار گیرد(جیانگ و لی، ۲۰۲۴: ۶۳). جیانگ و لی(۲۰۲۴: ۶۱) نشان می‌دهند که فناوری‌های دیجیتال می‌توانند ضمن افزایش کارایی و شفافیت حاکمیت، ساختارهای سنتی حاکمیت مبتنی بر هیئت‌مدیره را نیز با فرصت‌ها و ریسک‌های جدید مواجه کنند.

با گسترش اکوسیستم‌های داده‌ای و افزایش تبادل داده میان سازمان‌ها، حاکمیت داده با چالش‌های جدیدی مواجه شده و به یکی از الزامات اساسی حکمرانی در محیط‌های پلتفرمی

[1] Schreieck, Ondrus, Wiesche, & Krcmar

تبدیل شده است. بودندورف و بایر[1] (۲۰۲۵: ۱۴۷۷) بر ضرورت طراحی سازوکارهای حاکمیت داده برای مدیریت تبادل بین‌سازمانی داده و ایجاد اعتماد و هماهنگی میان بازیگران اکوسیستم تأکید می‌کنند. در اکوسیستم‌های دیجیتال، حاکمیت داده موضوعاتی مانند کیفیت داده، دسترسی، امنیت، حریم خصوصی، اشتراک‌گذاری و مسئولیت استفاده از داده را دربرمی‌گیرد و این موضوعات با طراحی و عملکرد اکوسیستم ارتباط متقابل دارند(وولز، مونش، لوهمولر و کوفنر[2]، ۲۰۲۵). شواهد حاصل از مطالعه وولز و همکاران (۲۰۲۵) نشان می‌دهد که حاکمیت داده در اکوسیستم‌های دیجیتال ماهیتی پویا و وابسته به پیچیدگی‌های نهادی دارد و می‌تواند به‌صورت یک فرایند کنترل و انطباق مستمر شکل گیرد(وولز و همکاران، ۲۰۲۵). از این رو، در چارچوب حاکمیت شرکتی پلتفرمی، رابطه میان حاکمیت شرکتی و حاکمیت داده و فناوری یک رابطه یک‌طرفه نیست، زیرا تصمیمات حاکمیتی می‌توانند بر معماری داده و فناوری اثر بگذارند و در مقابل، ویژگی‌های داده و فناوری نیز می‌توانند الزامات جدیدی برای نظارت، کنترل، گزارشگری و مدیریت ریسک شرکت ایجاد کنند.

## حاکمیت هوش مصنوعی و الگوریتمی

گسترش استفاده از الگوریتم‌ها و هوش مصنوعی در فرایندهای تصمیم‌گیری، حاکمیت شرکت‌های دیجیتال را با مسائل جدیدی در زمینه مسئولیت‌پذیری، شفافیت، توضیح‌پذیری، سوگیری، امنیت و نظارت انسانی مواجه می‌کند(موسلاین، ۲۰۲۵؛ طبسی، ۲۰۲۳: ۱۲). چارچوب مدیریت ریسک هوش مصنوعی، NIST[3] ویژگی‌هایی همچون اعتبار و قابلیت اتکا، ایمنی، امنیت و تاب‌آوری، پاسخ‌گویی و شفافیت، توضیح‌پذیری و تفسیرپذیری، حفاظت از حریم خصوصی و مدیریت سوگیری زیان‌بار را برای هوش مصنوعی قابل اعتماد مورد توجه قرار می‌دهد(طبسی،۲۰۲۳: ۲۱).

بر این اساس، حاکمیت هوش مصنوعی در سطح شرکت می‌تواند شامل تعیین مسئولیت‌ها، مستندسازی تصمیمات و مدل‌ها، ارزیابی ریسک، نظارت انسانی، پایش عملکرد و ایجاد امکان اصلاح یا توقف سیستم‌های هوش مصنوعی باشد(طبسی، ۲۰۲۳: ۲۲). NIST نیز حاکمیت را

[1] Bodendorf and Bayr
[2] Volz, Münch, Lohmüller, & Küffner
[3] National Institute of Standards and Technology (NIST)

یک کارکرد فراگیر در مدیریت ریسک هوش مصنوعی معرفی می‌کند که باید در سراسر چرخه عمر سیستم‌های هوش مصنوعی با فعالیت‌های شناسایی، اندازه‌گیری و مدیریت ریسک در ارتباط باشد(طبسی، ۲۰۲۳: ۲۲).

در محیط پلتفرمی، الگوریتم‌ها همچنین در تنظیم تعاملات میان ذینفعان نقش دارند و ازاین‌رو، حاکمیت الگوریتمی و حاکمیت ذینفعان نمی‌توانند کاملاً جدا از یکدیگر بررسی شوند(مولمان، گرگوری و هنفریدسون[1]، ۲۰۲۵: ۷۹۹). بنابراین، حاکمیت شرکتی پلتفرمی باید مسئولیت‌های مربوط به الگوریتم‌ها و هوش مصنوعی را در امتداد مسئولیت‌های هیئت‌مدیره، کنترل داخلی، مدیریت ریسک و پاسخ‌گویی سازمانی قرار دهد.

## سازمان هوشمند و جایگاه آن در چارچوب نظری پژوهش

سازمان هوشمند سازمانی است که با اتکا به دانش، فناوری‌های اطلاعاتی، یادگیری سازمانی، شبکه‌های ارتباطی و قابلیت انطباق، توانایی پاسخ‌گویی و سازگاری با محیط پیچیده و متغیر را توسعه می‌دهد(فیلوس، ۲۰۰۸: ۴۸). در این مفهوم، هوشمندی سازمانی صرفاً به ایجاد زیرساخت فناوری محدود نیست، بلکه به پیوند فناوری اطلاعات، شبکه‌سازی سازمانی، یادگیری و توسعه و به‌کارگیری دانش برای پاسخ‌گویی به فرصت‌ها و چالش‌های محیطی مربوط می‌شود (فیلوس، ۲۰۰۸ :۵۳-۵۰).

بر این اساس، در پژوهش حاضر سازمان هوشمند به‌عنوان یک وضعیت یا افق سازمانی مطلوب در نظر گرفته می‌شود و نه به‌عنوان مرحله قطعی و خودکار پس از پلتفرمی‌شدن. به بیان دیگر، وجود پلتفرم دیجیتال به‌تنهایی تضمین‌کننده شکل‌گیری سازمان هوشمند نیست و تحقق چنین وضعیتی به هماهنگی میان حاکمیت، قابلیت‌های دیجیتال، داده، فناوری، یادگیری سازمانی و سازوکارهای هوشمند تصمیم‌گیری وابسته است.

## مطالعات داخلی و جایگاه پژوهش حاضر

مطالعات داخلی، اگرچه تاکنون مفهوم «حاکمیت شرکتی پلتفرمی» را به‌طور مستقیم بررسی نکرده‌اند، برخی مؤلفه‌های مرتبط با آن را مورد توجه قرار داده‌اند. فتحعلی‌پور، شفیعی و

[1] Möhlmann, Gregory, & Henfridsson

شیبانی(۱۴۰۵) در مطالعه‌ای درباره تحول دیجیتال مؤسسات حسابرسی، بر توانمندی فناورانه و هوش مصنوعی، حکمرانی داده و الزامات حرفه‌ای و نظارتی تأکید کرده‌اند. رزمی و تنها (۱۴۰۵) نیز ارتباط حاکمیت داده، مدیریت دانش و تصمیم‌گیری راهبردی را در سازمان‌های مبتنی بر هوش مصنوعی بررسی کرده‌اند. همچنین، بشیر و راوی(۱۴۰۴: ۴۰) با مرور نظام‌مند ادبیات، مؤلفه‌هایی همچون شفافیت، توضیح‌پذیری، نظارت و پاسخگویی را در حکمرانی هوش مصنوعی شناسایی کرده‌اند؛ در حوزه حاکمیت شرکتی نیز عسگرپور و ابوطالبی(۱۴۰۳) بر اهمیت سازوکارهایی مانند استقلال هیئت‌مدیره و کمیته حسابرسی در ارتباط با شفافیت تأکید کرده‌اند. حسنی(۱۴۰۴) درهم‌تنیدگی حکمرانی شرکتی و حکمرانی پلتفرم‌های دیجیتال و نقش تنظیم‌گری پلتفرم‌ها را بررسی کرد و بر تعامل حاکمیت شرکتی و حکمرانی پلتفرمی تأکید داشت (حسنی، ۱۴۰۴). آطاهریان و همکاران (۱۴۰۴) نیز مسئولیت‌های پلتفرم‌ها را از منظر حکمرانی بر پلتفرم در ابعاد حقوقی، اقتصادی، امنیتی و فناورانه بررسی کردند(آطاهریان و همکاران، ۱۴۰۴). رحیمی‌پور و فیروزی(۱۴۰۴) با مقایسه حاکمیت داده و حکمرانی داده‌محور، چارچوبی چهارلایه برای طراحی سازمان‌های هوشمند ارائه کردند(رحیمی‌پور و فیروزی، ۱۴۰۴). همچنین، کیایی، بهزادی موزری و بارانی بناب(۱۴۰۳) با ارائه مدل حاکمیت داده در سازمان امور مالیاتی، چهار بعد مدیریت داده، زیرساخت، سازمانی و مدیریتی را برای حرکت به سوی نظام هوشمند شناسایی کردند(کیایی و همکاران، ۱۴۰۳). در مجموع، این مطالعات نشان می‌دهند که اجزای مرتبط با چارچوب پیشنهادی در ادبیات داخلی به‌صورت پراکنده وجود دارد، اما تاکنون در قالب یک معماری یکپارچه برای «حاکمیت شرکتی پلتفرمی» در سطح شرکت و اکوسیستم ترکیب نشده‌اند.

## یکپارچه‌سازی مبانی نظری و جایگاه حاکمیت شرکتی پلتفرمی

مرور ادبیات نشان می‌دهد که تحول دیجیتال، پلتفرمی‌شدن، حاکمیت شرکتی، حاکمیت اکوسیستم، حاکمیت داده و فناوری و حاکمیت هوش مصنوعی، حوزه‌هایی جدا از یکدیگر نیستند و در سازمان‌های دیجیتال به‌صورت متقابل بر یکدیگر اثر می‌گذارند(زو و همکاران، ۲۰۲۶: ۱؛ کوستابیله، ۲۰۲۴: ۳؛ جیانگ و لی، ۲۰۲۴). از این منظر، یافته مهم ادبیات جدید آن است که نمی‌توان رابطه میان تحول دیجیتال و حاکمیت را در قالب یک زنجیره ساده و خطی

از «تحول دیجیتال ← پلتفرمی‌شدن ← حاکمیت شرکتی پلتفرمی ← سازمان هوشمند» توضیح داد.

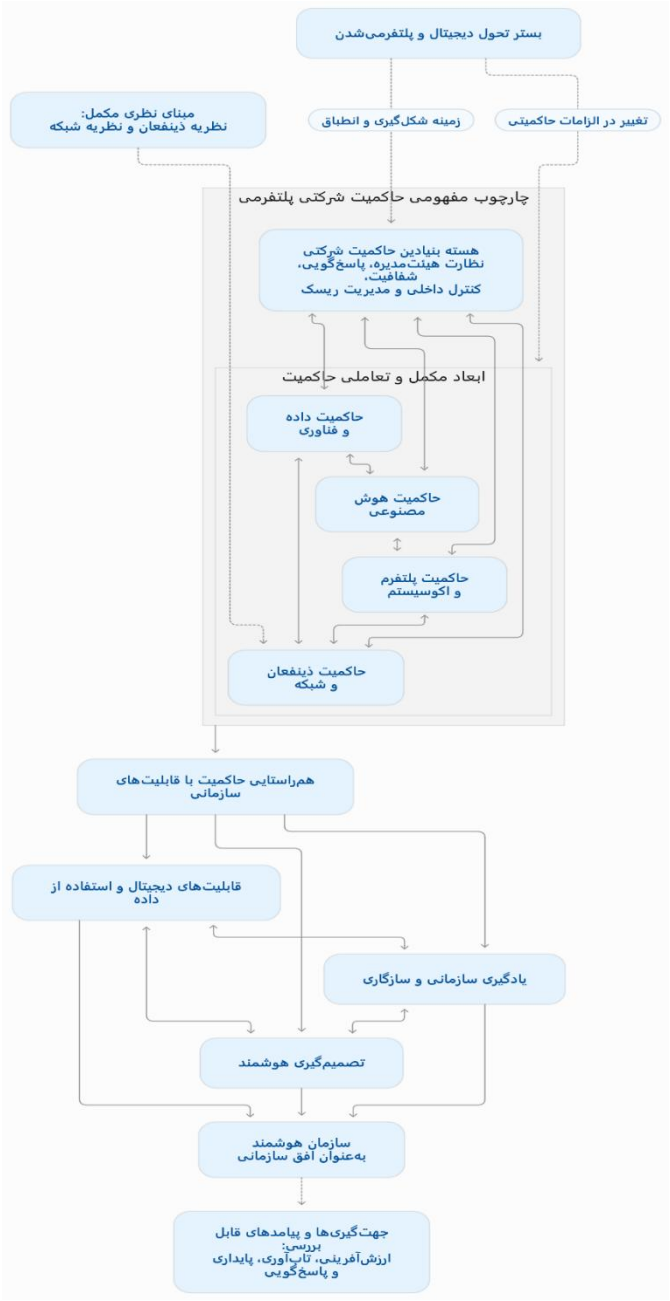
در مقابل، ادبیات از نوعی معماری تعاملی حمایت می‌کند که در آن حاکمیت شرکتی، حاکمیت اکوسیستم، داده و فناوری، هوش مصنوعی، ذینفعان و شبکه‌ها به‌طور هم‌زمان و متقابل با یکدیگر ارتباط دارند(کوستابیله، ۲۰۲۴: ۳؛ جیانگ و لی، ۲۰۲۴؛ شرایک و همکاران، ۲۰۲۵). کوستابیله (۲۰۲۴: ۳) با ارائه پنج مؤلفه ساختار، سازوکار، دامنه، عوامل اقتضایی و پیامدها، زمینه‌ای برای تحلیل چندبعدی حاکمیت اکوسیستم پلتفرمی فراهم می‌کند، در حالی که زو و همکاران (۲۰۲۶) با مرور ۱۵۲ مطالعه، بر ماهیت پویا و مبتنی بر تنش‌های متقابل در تحول دیجیتال مبتنی بر پلتفرم تأکید دارند(زو و همکاران، ۲۰۲۶: ۱).

بر این اساس، حاکمیت شرکتی پلتفرمی در پژوهش حاضر به‌عنوان یک معماری یکپارچه و تعاملی مفهوم‌پردازی می‌شود که در هسته آن سازوکارهای متعارف حاکمیت شرکتی، ازجمله نظارت هیئت‌مدیره، پاسخ‌گویی، شفافیت، کنترل داخلی و مدیریت ریسک، با حاکمیت اکوسیستم پلتفرمی، حاکمیت ذینفعان و شبکه، حاکمیت داده و فناوری و حاکمیت هوش مصنوعی پیوند می‌یابد. در این معماری، سازمان هوشمند به‌عنوان یک افق سازمانی حاصل از هم‌راستایی قابلیت‌های حاکمیتی، دیجیتال، داده‌ای، فناورانه و یادگیری سازمانی در نظر گرفته می‌شود و رابطه آن با پلتفرمی‌شدن، رابطه‌ای مفهومی و پیشنهادی است و نه یک رابطه علّی اثبات‌شده. همچنین، پایداری در این چارچوب با مفهوم سازمان هوشمند یکسان تلقی نمی‌شود، بلکه می‌تواند به‌عنوان یکی از پیامدها یا معیارهای ارزیابی عملکرد و مسئولیت‌پذیری سازمان در محیط دیجیتال مورد توجه قرار گیرد. نوآوری مفهومی پژوهش حاضر در ارائه چارچوبی یکپارچه برای پیوند دادن جریان‌های مرتبط با حاکمیت شرکتی، حاکمیت پلتفرمی و اکوسیستمی، حاکمیت داده و فناوری و حاکمیت هوش مصنوعی است. این چارچوب، صورت‌بندی مفهومی پیشنهادی پژوهش برای تحلیل معماری حاکمیت شرکت در محیط‌های دیجیتال و پلتفرمی است و به‌منزله نظریه‌ای مستقل و تثبیت‌شده یا مدلی تجربیِ اعتبارسنجی‌شده تلقی نمی‌شود.

**چارچوب مفهومی پیشنهادی حاکمیت شرکتی پلتفرمی و ارتباط آن با سازمان هوشمند**

بر مبنای یکپارچه‌سازی مبانی نظری و مرور ادبیات، پژوهش حاضر چارچوبی مفهومی برای تبیین حاکمیت شرکتی پلتفرمی و ارتباط آن با سازمان هوشمند ارائه می‌کند. در این چارچوب، حاکمیت شرکتی پلتفرمی به‌عنوان معماری یکپارچه و تعاملی در نظر گرفته می‌شود که سازوکارهای بنیادین حاکمیت شرکتی، شامل نظارت هیئت‌مدیره، پاسخ‌گویی، شفافیت، کنترل داخلی و مدیریت ریسک را با حاکمیت پلتفرم و اکوسیستم، حاکمیت ذینفعان و شبکه، حاکمیت داده و فناوری و حاکمیت هوش مصنوعی پیوند می‌دهد.

بر اساس چارچوب پیشنهادی، سازمان هوشمند پیامد قطعی پلتفرمی‌شدن نیست، بلکه افقی سازمانی است که تحقق آن به هم‌راستایی سازوکارهای حاکمیتی با قابلیت‌های دیجیتال، یادگیری سازمانی، سازگاری و تصمیم‌گیری هوشمند وابسته است. همچنین، ارزش‌آفرینی، تاب‌آوری، پایداری و پاسخ‌گویی می‌توانند به‌عنوان جهت‌گیری‌ها یا پیامدهای قابل بررسی این چارچوب مطرح شوند. این چارچوب ماهیتی مفهومی دارد و روابط آن به‌عنوان روابط علّی اثبات‌شده تلقی نمی‌شوند؛ ازاین‌رو، اعتبارسنجی تجربی و توسعه شاخص‌های ارزیابی آن به پژوهش‌های آتی واگذار می‌شود.




**شکل ۱.** چارچوب مفهومی پژوهش

منبع: تدوین پژوهشگران بر مبنای یکپارچه‌سازی ادبیات نظری و پیشینه پژوهش.

## بحث و نتیجه‌گیری

پژوهش حاضر با هدف تبیین چگونگی تحول حاکمیت شرکتی در مواجهه با تحول دیجیتال و پلتفرمی‌شدن و ارائه یک چارچوب مفهومی برای پشتیبانی از گذار سازمان به وضعیت هوشمند انجام شد. یکپارچه‌سازی ادبیات نشان داد که مسئله سازمان پلتفرمی، انتخاب میان «حاکمیت شرکتی» و «حاکمیت پلتفرمی» نیست؛ بلکه بازطراحی معماری حاکمیت شرکتی متناسب با محیطی است که در آن خلق ارزش، اطلاعات، تصمیم‌گیری و ریسک به شبکه‌ای از ذینفعان، داده و فناوری وابسته شده است. این نتیجه با یافته‌های کای (۲۰۲۴)، کای و هو (۲۰۲۲) و فنویک و همکاران (۲۰۱۹: ۱۷۳) درباره تداوم اهمیت حاکمیت شرکتی در محیط پلتفرمی و با یافته‌های جیانگ و لی (۲۰۲۴: ۶۱) درباره اثر هم‌زمان فناوری بر افزایش ظرفیت‌های حاکمیت و ایجاد ریسک‌ها و پیچیدگی‌های جدید همسو است. همچنین، چندبعدی بودن حاکمیت پلتفرمی در این پژوهش با نتایج پن و همکاران (۲۰۲۵) همخوانی دارد.

بر مبنای نظریه ذینفعان و نظریه شبکه، استنتاج مفهومی پژوهش حاکی از آن است که در سازمان‌های پلتفرمی، دامنه تحلیل حاکمیت از تمرکز صرف بر درون شرکت به بررسی شرکت در بستر اکوسیستم و روابط آن با کاربران، شرکا، ارائه‌دهندگان خدمات و سایر بازیگران گسترش می‌یابد؛ زیرا این بازیگران می‌توانند در فرایند خلق ارزش مشارکت داشته باشند و تصمیمات شرکت نیز بر منافع آنان اثر بگذارد. بااین‌حال، ترکیب و تحلیل مفهومی ادبیات نشان می‌دهد که مشارکت در خلق ارزش به‌خودی‌خود به معنای اعطای حق رأی یا عضویت در هیئت‌مدیره نیست و نوع و میزان مشارکت ذینفعان در سازوکارهای حاکمیتی باید متناسب با حقوق قانونی، میزان اثرپذیری، اهمیت تصمیم و سطح ریسک مربوط تعیین شود. این یافته با کاری و همکاران[1] (۲۰۲۵: ۲) نیز همخوان است که نشان می‌دهند در اکوسیستم‌های پلتفرمی شبکه‌محور، در صورت وجود ترتیبات مالکیت و حاکمیت مشترک، حقوق مالکیت و تصمیم‌گیری می‌تواند میان بازیگران شبکه توزیع شود. بنابراین، نوع ساختار مالکیت و ترتیبات حاکمیتی پلتفرم، اثرگذار بر میزان و شیوه مشارکت بازیگران مختلف در تصمیم‌گیری است. همچنین، این یافته با دیدگاه زیاماری (۲۰۲۶) همسو است که خلق ارزش در اکوسیستم پلتفرمی را پیامدی چندذینفعی و وابسته به ترتیبات حاکمیتی می‌داند؛ بااین‌حال، مشارکت در خلق ارزش

[1] Kari, , Bellin, , Matzner, , Gersch.

لزوماً به معنای برخورداری از حقوق حاکمیتی یکسان نیست و نحوه مشارکت باید متناسب با نقش و میزان اثرگذاری هر ذینفع تعیین شود.

نوآوری مفهومی پژوهش حاضر در صورت‌بندی و یکپارچه‌سازی چارچوبی برای پیوند دادن حاکمیت شرکتی با الزامات حاکمیت پلتفرم و اکوسیستم، حاکمیت داده و فناوری و حاکمیت هوش مصنوعی است. در این پژوهش، اصطلاح «حاکمیت شرکتی پلتفرمی» برای تبیین این چارچوب یکپارچه به کار گرفته می‌شود؛ چارچوبی که صورت‌بندی مفهومی پیشنهادی پژوهش است و نه نظریه‌ای مستقل و تثبیت‌شده یا مدلی که اعتبار آن به‌صورت تجربی آزمون شده باشد. بر اساس یکپارچه‌سازی مباحث حاکمیت شرکتی و الزامات محیط‌های دیجیتال و پلتفرمی، این مفهوم در پژوهش حاضر مسئولیت‌های بنیادین حاکمیت شرکتی، شامل هدایت راهبردی، نظارت، پاسخ‌گویی، مدیریت ریسک و کنترل را با الزامات حاکمیت پلتفرم و اکوسیستم، حاکمیت داده و فناوری و حاکمیت هوش مصنوعی پیوند می‌دهد. از این منظر، «حاکمیت شرکتی پلتفرمی» نه جایگزین حاکمیت شرکتی و نه مترادف حاکمیت پلتفرمی است، بلکه چارچوبی برای بازطراحی و انطباق معماری حاکمیت شرکتی با ویژگی‌ها و الزامات سازمان‌های فعال در محیط‌های دیجیتال و پلتفرمی محسوب می‌شود. بنابراین، چارچوب حاضر به‌جای مسیر ساده، تحول دیجیتال ← پلتفرمی‌شدن ← حاکمیت شرکتی پلتفرمی ← سازمان هوشمند، یک معماری تعاملی و چندلایه را پیشنهاد می‌کند که در آن حاکمیت شرکتی، اکوسیستم، داده، فناوری و هوش مصنوعی بر یکدیگر اثر متقابل دارند.

از منظر کاربردی، چارچوب پیشنهادی می‌تواند مبنایی برای بازنگری مسئولیت‌های هیئت‌مدیره، کنترل‌های داخلی، مدیریت ریسک، گزارشگری و سازوکارهای نظارت بر داده، فناوری و AI در شرکت‌های در حال پلتفرمی‌شدن باشد؛ بااین‌حال، این چارچوب ابزار استاندارد یا اعتبارسنجی‌شده اجرایی محسوب نمی‌شود. برای مدیران و فعالان حرفه‌ای، پیشنهادهای برگرفته از چارچوب مفهومی پژوهش آن است که ارزیابی وضعیت موجود، تعیین مسئولیت‌ها و کنترل‌های متناسب، اجرای آزمایشی و سپس پایش و یادگیری به‌صورت مرحله‌ای دنبال شود؛ برای قانون‌گذاران و نهادهای ناظر نیز توجه به مسئولیت هیئت‌مدیره در قبال ریسک‌های دیجیتال، امنیت و حریم خصوصی داده و کیفیت افشا می‌تواند در توسعه چارچوب‌های آتی حاکمیت شرکتی مورد توجه قرار گیرد. در بستر ایران نیز گذار به حاکمیت

دیجیتال مستلزم فراتر رفتن از افشای الکترونیکی و توجه هم‌زمان به حاکمیت داده، زیرساخت‌های یکپارچه اطلاعاتی، شفافیت و پاسخ‌گویی است. در این چارچوب، هوش مصنوعی می‌تواند ظرفیت نظارت، شناسایی ریسک و پشتیبانی از تصمیم‌گیری هیئت‌مدیره را افزایش دهد؛ مشروط بر آنکه استفاده از آن با سازوکارهای شفافیت، پاسخ‌گویی و نظارت انسانی همراه باشد (عبدالعظیمی، ۱۴۰۴). ازاین‌رو، حاکمیت دیجیتال را می‌توان یکی از الزامات زمینه‌ای برای تقویت شفافیت، پاسخ‌گویی و تاب‌آوری حاکمیت شرکتی در محیط کسب‌وکار ایران دانست.

در نهایت، سازمان هوشمند در این پژوهش مرحله‌ای قطعی و خودکار پس از پلتفرمی‌شدن نیست، بلکه به‌عنوان یک افق سازمانی مبتنی بر دانش، یادگیری، ارتباط و سازگاری در نظر گرفته می‌شود؛ ازاین‌رو، رابطه میان حاکمیت شرکتی پلتفرمی و سازمان هوشمند در این مطالعه صرفاً مفهومی و پیشنهادی است و نباید به‌عنوان رابطه‌ای علّی و تجربی تفسیر شود. مهم‌ترین محدودیت پژوهش، ماهیت مروری ـ مفهومی آن و نبود آزمون تجربی چارچوب پیشنهادی است؛ همچنین، ویژگی‌های متفاوت صنایع، بازیگران و محیط‌های نهادی می‌تواند بر نحوه شکل‌گیری و اجرای سازوکارهای حاکمیت پلتفرمی اثرگذار باشد. بنابراین، پژوهش‌های آینده می‌توانند ابتدا ابزار سنجش بلوغ حاکمیت شرکتی پلتفرمی را از طریق نظرخواهی از اعضای هیئت‌مدیره، حسابرسان، مدیران فناوری و مدیران داده توسعه و اعتبارسنجی کنند و سپس ارتباط آن را با پیامدهایی مانند کیفیت گزارشگری، اثربخشی کنترل داخلی، مدیریت ریسک، شفافیت، اعتماد ذینفعان، نوآوری و عملکرد سازمانی در صنایع و زمینه‌های مختلف بررسی کنند.

## ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

## منابع


آطاهریان، سینا، نریمانی، میثم، صاحبکار خراسانی، سیدمحمد، سرمست، عسگر، و بهرامی، علیرضا. (۱۴۰۴). دسته‌بندی مسئولیت‌های پلتفرم‌ها از منظر «حکمرانی بر پلتفرم»: مطالعه موردی پلتفرم‌های فروش و توزیع برخط دارو

بشیر، حسن؛ و راوی، محمدجواد.(۱۴۰۴). مرور نظام‌مند چارچوب‌ها و سازوکارهای حکمرانی.

حسنی، حسین. (۱۴۰۴). حکمرانی در پلتفرم‌های دیجیتال جهانی: مطالعه درهم‌تنیدگی حکمرانی شرکتی با حق حاکمیت دولت‌ها .*پژوهش‌نامه ایرانی سیاست بین‌الملل*.

رزمی، زهرا؛ و تنها، زهرا.(۱۴۰۵). کاربرد هستی‌شناسی در حاکمیت داده و مدیریت دانش در سازمان‌های مبتنی بر هوش مصنوعی .*تکنولوژی در کارآفرینی و مدیریت استراتژیک*.

راهبردی هوش مصنوعی در مطالعات سال‌های ۲۰۱۷–۲۰۲۵ .*فصلنامه علمی مطالعات فضای مجازی و رسانه‌های اجتماعی*.

رحیمی‌پور، مریم، و فیروزی، افشین. (۱۴۰۴). تحلیل چندمعیاره هم‌افزایی میان حاکمیت داده و حکمرانی داده‌محور: چارچوب تطبیقی برای طراحی سازمان‌های هوشمند .*نشریه حکمرانی متعالی*.

*عسگرپور، رسول؛ و ابوطالبی، حمید.(۱۴۰۳).تأثیر حاکمیت شرکتی بر عملکرد مالی شرکت‌ها از طریق متغیر واسطه‌ای شفافیت با استفاده از روش فراتحلیل .مدیریت دارایی و تأمین مالی*

*عبدالعظیمی، محمدعلی. (۱۴۰۴، ۲۲ آبان) .واقعیت‌های پنهان در سایه هوش مصنوعی؛ ریسک کمتر با حاکمیت دیجیتال در شرکت‌ها .روزنامه دنیای اقتصاد، شماره ۶۴۳۵، خبر شماره ۴۲۲۸۲۱۹ .*

فتحعلی‌پور، فرزانه؛ شفیعی، حسین؛ و شیبانی، عباس.(۱۴۰۵) طراحی الگوی تحول دیجیتال در مؤسسات حسابرسی با تأکید بر حکمرانی هوشمند .*مجله حکمرانی و شهر هوشمند*.

کیایی، مجتبی، بهزادی موزری، سعید، و بارانی بناب، صمد. (۱۴۰۳). ارائه مدل حاکمیت داده در سازمان امور مالیاتی کشور: مطالعه‌ای در نظام مالیاتی هوشمند .*پژوهشنامه مالیات*


## References


Ataharian, S., Narimani, M., Sahebkar Khorasani, S. M., Sarmast, A., & Bahrami, A. (2025). Categorization of platform responsibilities from the perspective of "governance over platforms": A case study of online drug sales and distribution platforms. (In Persian)

Asgarpour, R., & Aboutalebi, H. (2024). The effect of corporate governance on firms' financial performance through transparency as a mediating variable: A meta-analysis. *Asset Management and Financing*. (In Persian)

Bodendorf, F &. Bayr., c. (2025). Shaping platform governance principles to manage interorganizational data exchange. *Information Systems Journal*, *35*(5), 1477–1496. https://doi.org/10.1111/isj.12592

Bashir, H., & Rawi, M. J. (2025). A systematic review of artificial intelligence strategic governance frameworks and mechanisms in studies from 2017–2025. *Journal of Cyber Space and Social Media Studies*. (In Persian)

Caplan, R. (2023). Networked Platform Governance: The Construction of the Democratic Platform. *International Journal of Communication* 17, 3451–3472

Cai, Q. (2024). Corporate governance in platform governance: Reassessing stakeholderism in a disruptive era. *European Business Law Review*, *35*(6), 851–876. DOI: 10.54648/EULR2024045.

Cai, Q., & Hou, H. (2022). Hello platform governance; but never ending corporate governance. *European Company Law, 19*(2), 47–56. https://doi.org/10.54648/EUCL2022008

Costabile, C. (2024). Digital platform ecosystem governance of private companies: Building blocks and a research agenda based on a multidisciplinary, systematic literature review. *Data and Information Management, 8*(1), 100053. https://doi.org/10.1016/j.dim.2023.100053

Fenwick, M, & Vermeulen, E.(2019). A Sustainable Platform Economy & the Future of Corporate Governance.Lex Research Topics in Corporate Law & Economics Working Paper No. 2019-1, European *Corporate Governance Institute* (ECGI) - Law Working Paper No. 441/2019, Available at SSRN: https://ssrn.com/abstract=3331508 or http://dx.doi.org/10.2139/ssrn.3331508

Fenwick, M., McCahery, J. A., & Vermeulen, E. P. M. (2019). The end of "corporate" governance: Hello "platform" governance. *European Business Organization Law Review, 20*(1), 171–199. https://doi.org/10.1007/s40804-019-00137-z

Filos, E. (2008). Smart organizations in the digital age. In M. E. Jennex (Ed.), *Knowledge management: Concepts, methodologies, tools, and applications*. IGI Global. https://doi.org/10.4018/978-1-59904-933-5.ch005

Fathalipour, F., Shafiei, H., & Sheibani, A. (2026). Designing a digital transformation model in auditing institutions with an emphasis on smart governance. *Journal of Governance and Smart City*. (In Persian)

Jiang, W., & Li, T. (2024). Corporate governance meets data and technology. *Foundations and Trends in Finance, 14*(2), 61–136. DOI: 10.1561/0500000071.

Janowski T., Estevez E., Baguma R. (2018), Platform governance for sustainable development: Reshaping citizen-administration relationships in the digital age, *Government Information Quarterly*, Vol. 35, Iss. DOI: 10.1016/j.giq..09.002 http://creativecommons.org/licenses/by-nc-nd/4.0/

Halckenhaeusser, A, Foerderer, J, & Heinzl, A. (2020). Platform Governance Mechanisms: An Integrated Literature Review And Research Directions. *Published in Proceedings of the 28th European Conference on Information Systems* (ECIS), 2020, Online, June 15-17

Hasani, H. (2025). Governance in global digital platforms: A study of the entanglement of corporate governance with state sovereignty. *Iranian Political International Policy Research Quarterly*. (In Persian)

Kari, A., Bellin, P., Matzner, M., Gersch. (2025). Governing the emergence of network-driven platform ecosystems. *Electronic Markets, 35*, Article 4. https://doi.org/10.1007/s12525-024-00745-9

Kiaei, M., Behzadi Mozari, S., & Barani Bonab, S. (2024). Developing a data governance model for the Iranian National Tax Administration: A study of the smart tax system. *Tax Research Journal*. (In Persian)

Lu, P, Zhou, L and Fan, X. (2023). Platform governance and sociological Participation. *The Journal of Chinese Sociology* 10:3 https://doi.org/10.1186/s40711-023-00181-w

Laux, J. (2024). Institutionalised distrust and human oversight of artificial intelligence: Towards a democratic design of AI governance under the European Union AI Act. *AI & Society*,. https://doi.org/10.1007/s00146-023-01777-z

Möslein, F. (2025). European company law in the age of digital transformation: Artificial intelligence, data economy, and digital corporate governance. *ERA Forum, 26*, 629–646. https://doi.org/10.1007/s12027-025-00864-6.

Möhlmann, M., Gregory, R., & Henfridsson, O. (2025). Algorithmic stakeholder governance on content platforms: A lead role perspective. *Journal of Management Information Systems, 42*(3), 799–831. https://doi.org/10.1080/07421222.2025.2520177

Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: What it is and how it works. *AI & Society, 39*, 1871–1882. https://doi.org/10.1007/s00146-023-01635-y

OECD. (2023). *G20/OECD principles of corporate governance 2023*. OECD Publishing. https://doi.org/10.1787/ed750b30-en

Pan, Q., Luo, W., Liu, Z., & Zhang, J. Z. (2025). Digital platform governance: Literature review and research outlook. *Journal of Organizational Computing and Electronic Commerce, 35*(4), 407–431. https://doi.org/10.1080/10919392.2025.2502325

Razmi, Z., & Tanhā, Z. (2026). Application of ontology in data governance and knowledge management in artificial intelligence-based organizations. *Technology in Entrepreneurship and Strategic Management*. (In Persian)

Rahimipour, M., & Firoozi, A. (2025). Multi-criteria analysis of the synergy between data governance and data-driven governance: A comparative framework for designing smart organizations. *Journal of Transcendent Governance*. (In Persian)

Schreieck, M., Ondrus, J., Wiesche, M., & Krcmar, H. (2025). Platform governance for established companies. *California Management Review, 67*(4), 48–74. https://doi.org/10.1177/00081256251338251

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. *The Journal of Finance, 52*(2), 737–783. https://doi.org/10.1111/j.1540-6261.1997.tb04820.x

Springer, V., Randhawa, K., Jovanovic, M., Ritala, P., & Piller, F. T. (2025). Platform design and governance in industrial markets: Charting the meta-organizational logic. *Research Policy, 54*(6), 105236. https://doi.org/10.1016/j.respol.2025.105236

Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

Volz, F., Münch, C., Lohmüller, M., & Küffner, C. (2025). From data jungle to data governance in digital ecosystems: Empirical evidence from a multiple holistic case study. *Journal of Business Research, 201*, 115747. https://doi.org/10.1016/j.jbusres.2025.115747

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Visconti, R. (2020). Corporate Governance, Digital Platforms and Network Theory: information and risk-return sharing of connected stakeholders. MANAGEMENT CONTROL, (2), 1-26.

Zou, Y., Wu, T., & Wang, K. (2026). Governing digital platform ecosystems in enterprise digital transformation: A scoping review and dialectical systems framework. *Data Science and Management*, 100194. https://doi.org/10.1016/j.dsm.2026.100194

Zeamari, I. (2026). Value co-creation in digital platform ecosystems: A stakeholder-centric conceptual model. *Journal of Enterprise Information Management*, 1–26. https://doi.org/10.1108/JEIM-02-2026-0206

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.

# Table of Contents


**Academic Acceptance and Support for Integrating Data Analytics into Accounting Education: A Faculty Perspective Study** 1-28
Ali Rahmani, Samira Parmah and Zahra Mousavi

**IT Governance through a Novel Ranking Model for COBIT Information Technology Security Controls** 29-60
Saeed Rouhani and Mohammad Nikbakht

**Proposing an Exploratory Conceptual Framework for Algorithmic Governance, Intelligent Audit Supervision and Data-Driven Entrepreneurship Development: A Fuzzy Delphi Study in Kermanshah, Iran** 61-96
Bijan Rezaee, Arash Khademi and Rasoul Mohammadi

**Redefining Insurance Supervision in the Digital Era: A Conceptual Framework for Smart Supervisory Transformation** 97-126
Ameneh Khadivar, Leili Niakan and Naser Bafekr Sharak

**The Digital Transformation of the Internal Audit Function: A Qualitative Literature Review** 127-158
Neda Rasouli and Parsa Bahmanabadi

**Opening the Black Box: A Framework for Auditor Assurance Over the Explainability of AI Decisions in IT Risk Governance** 159-186
Farzad Evani and Donya Kazemi

**The Impact of Corporate Governance and Board Characteristics on Information Technology and Cybersecurity Risks: Evidence from Manufacturing Firms Listed on the Tehran Stock Exchange** 187-232
Maryam Ghasemiansaghi and Aghil Farhangian

**The Synergy Between Artificial Intelligence and Agile Auditing in Small and Medium-Sized Enterprises: A Systematic Interpretive Literature Review** 233-262
Saeed Alipour and Morteza Asadi

**Design and Validation of an Organizational Cyber Resilience Governance Framework Based on Artificial Intelligence and Risk Management: A Mixed-methods Approach to Information Technology Governance** 263-302
Amirhossein Kafi, Mohammadali Soltanshahi, Mojtaba Reessafari and Amirmohammad Kafi

**Emerging Digital Technologies in the Auditing Industry: Challenges and New Opportunities** 303-332
Kaveh Parandin, Kaveh Ghaderi and Avan Jamshidi

**Opportunities and Challenges of Artificial Intelligence in Enhancing Financial Reporting Quality: A Systematic Review of Existing Studies** 333-370
Gholamhossein Mikaeilou and Mahmood Nasiri

**Platform Corporate Governance in the Digital Age: An Integrative Conceptual Framework for Smart Organizations** 371-398
Masoome Kazemi, Ghodratallah Barzegar and Danial Hassanzadeh

graphs should be referred to by their number. Formulas should also be numbered and presented in two column tables with no border.

**6. Footnotes**

English terms and some explanations should be presented in four column tables (including the number and the content of the footnote) with no border. Footnotes should be numbered in text style and using EndNote in Microsoft Word.

**4. References and sources.**

To provide a sources and references list, APA sourcing should be used. At first, Persian list and then English list should be presented alphabetically and based on the last name of authors.

4.1. Book: last name, the author's full name. Publication year. Italic form of the book name, the translator's name, publication site, publisher's name.

4.2. Paper: last name, the author's full name. Publication date. The paper title. The publication name in Italic form, series number in Italic form, the beginning page number-the last page number of the paper.

4.3. Online papers: last name, the author's full name. Publication date. The paper title. The publication name in Italic form, series number in Italic form, the beginning page number-the last page number of the paper. From: the Website address.

4.4. Reports and other sources: sufficient information

- The name of two or more authors in the sources list should be separated by semicolon.
- The sources list does not require to be numbered. If there is two or more paper title or book name from an author, the publication date should also be considered in the listing order, so that the older book or paper should be listed before the newer one. To prevent from any confusion, there is no indentation before items of the list and if the item is longer than one line, the second and more lines start with special indentation of Hanging 0/5 cm.

**5. Graphs, Figures and formula**

Graphs and figures name should be written under and above them respectively. Graphs and figures should be placed into the text and after referring to them. They should be orderly numbered, for example figure 1 to … . Items written in figures should be in Farsi and / should be used, if required, instead of dot. In addition to writing variables name in Farsi, a column may be used to show English symbols of variables, as they are used in equations and models. The column titles should have centered alignment. The first line of figures which include titles of columns should be in "gray 2" color. Figures and

- Academic level, the employment place, and full address of the author responsible for correspondence.
- No nickname should be used for authors.

2.2. The first page includes the title and abstract in Farsi. The abstract should be provided in four paragraphs including the subject and aim of the article, research method, research findings, conclusion (totally 165 words), key words (maximum 5 words), and the classification code of JEL. The coding is designed for subject classification in economic literature, which is described in detail in .

2.3. The second page to the end include the following:

- The introduction including some paragraphs explaining the question, theoretical principles, the aim and its importance.
- Review of literature; Research hypotheses.
- Research method in addition to data collection tools, analysis techniques, and hypotheses testing model, variable definition, statistical society, sample volume and sampling method.
- Research findings in addition to a comparison between them and the findings of researches mentioned in the review of literature, and explanation of any conformity and non-conformity among them.
- Conclusion including a summary of the question and findings, overall conclusion, suggestions based on findings, and if required a suggestion for next researches.
- Sources and references.
- English abstract.

**3.APA sourcing:**

- The author's last name and the publication date should be mentioned in Farsi. They are not required in English at footnote. For more than one author, comma, and for more than one source, semicolon, should be used.
- Any sources referred to in the article text should be listed in detail in the sources and references part. No additional sources should be listed.
- Any explanation of terms and English form of words (except authors' name) should be presented in footnotes. No English words or terms should be used in the article text except formula and equation.

# Guide for Authors

**Ensure that the following items are present:**
One author has been assigned as the corresponding author with contact details: Email address, full personal address.
All necessary files have been uploaded: the manuscript must be prepared in Microsoft office word format.
All authors' information, especially their affiliations, are provided in Persian and English.

**Articles Development and Review Guideline**

Articles are published in the journal after being professionally judged and approved by the editorial board. To publish their articles in the journal, all professors and researches should consider the following points in their article's development.

**1.Article Format**
The articles are developed using software Word 2007; A4 papers; top, bottom, left and right margins 4, 6/5, 4/5 and 5 cm, respectively; Persian font B Nazanin, for the title and the authors of the paper in Bold style and center text with font sizes 16 and 12 respectively; Persian font should be B Zar for the abstract, body, footnotes, references, keywords and figures notes with font sizes 11, 12, 11,11, 10 and 10 respectively; line spacing 1 cm; before text in each paragraphs 0/3 cm; justify alignment; English font should be Times New Roman with the font size for the title 14 Bold, abstract 12, formula11, footnote 11, references 11, figures note 9, subject classification 8, figures title and diagrams 8 Italic and Bold; 6cm space before and after the figure and diagram and as center alignment; maximum 18 pages including sources and references; no page number. Typed article is sent through the system designed as jera.alzahra.ac.ir Pictures in the texts, if any, should be in gray color and high quality.

**2.Article Structure**
2.1. The cover should include:
- Full title
- Author or authors (the author responsible for correspondence should be marked by *).

**Journal of Information System and Technology Auditing**
Volume 2, No. 1, Biannually, Spring & Summer 2026

**Iranian Information Technology Audit Scientific Association**
**Director in Charge: A. Rahmani**, Professor, Alzahra University
**Editor in Chief: A. Rahmani**, Professor, Alzahra University
**Associate Editor: A. Khadivar**, Associate Professor, Alzahra University

**Editorial Board**
**N. Abdolvand,** IT Management, Associate Professor, Alzahra University
**R. Azmi,** Electronic, Associate Professor, Alzahra University
**A. Hasanzadeh,** IT Management, Professor, Tarbiat Modares University
**R. Hesarzadeh,** Accounting, Professor, Ferdowsi University of Mashhad
**M Keivanpour,** Computer Engineering, Professor, Alzahra University
**M. Khedmati,** Accounting/ IT Management, Associate Professor, Monash University
**A. Manian,** IT Management, Professor, University of Tehran
**J. Nazari,** Accounting, Professor, Simon Fraser University
**Z. Rezaee,** Accounting, Professor, The University of Memphis
**S. Rouhani,** IT Management, Associate Professor, Tehran University
**H. Yazdifar,** Accounting, Professor, University of Derby

Publisher: **Iranian Information Technology Audit Scientific Association**
Executive Director: **M. Amirykhah**
Editor: **A. Khazen, B. Parvizi**
Page Designer: **M. Amirykhah**

Publication Frequency: **Biannually**
e-ISSN: 3115-8773

**Address**: No. 58, Nourani Blvd., Farahzadi Blvd., Shahrak-e Gharb, Tehran, Iran.
1468973466
**Email**: journalofista@gmail.com

In the Name of God



**Iranian Information Technology Audit Scientific Association**

# Journal of Information System and Technology Auditing

**Spring & Summer 2026 - 2026, Vol 2, Number 1**

# Journal of Information System and Technology Auditing

Publisher
Iranian Information Technology Audit Scientific Association



e-ISSN: 3115-8773