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

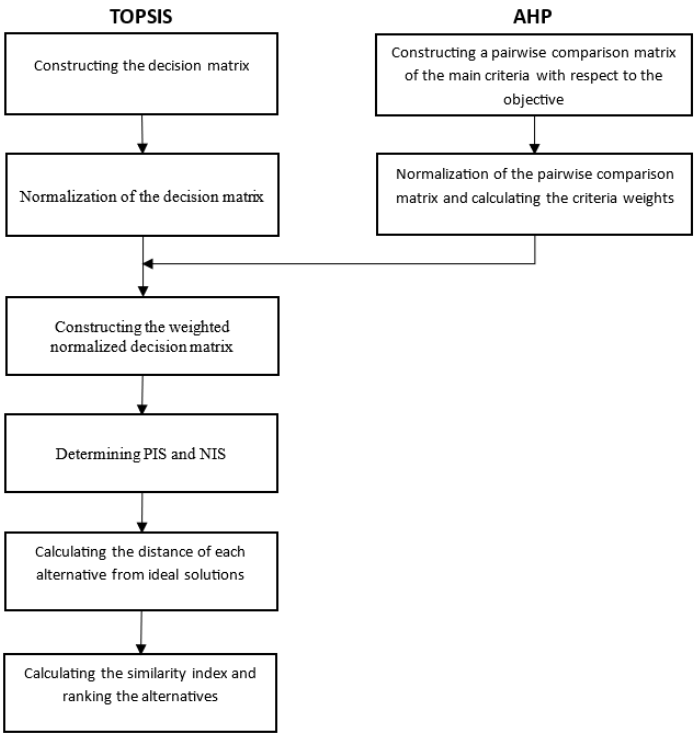
کنترل‌های امنیتی COBIT 2019 به‌عنوان گزینه‌ها

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.

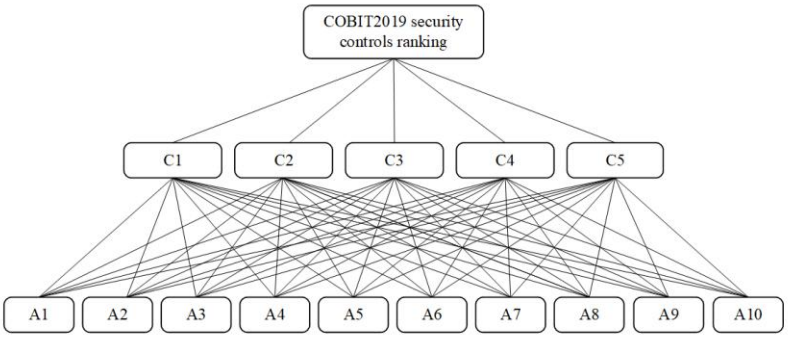
در مقابل، روش AHP به دلیل نیاز به ساخت ماتریس‌های مقایسه زوجی برای هر معیار و محاسبه مقدارCR ، فرایندی طولانی و پیچیده دارد. وزن‌دهی ماتریس‌ها توسط تصمیم‌گیرنده نیز یکی از چالش‌های این روش است.

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). 2. Filter incoming traffic, such as emails and downloads, to protect against unsolicited information (e.g., spyware, phishing emails). 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. 4. Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management 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 2. Implement network filtering mechanisms, such as firewalls and intrusion detection software. Enforce appropriate policies to control inbound and outbound traffic. 3. Apply approved security protocols to network connectivity 4. Configure network equipment in a secure manner 5. Encrypt information in transit according to its classification 6. Based on risk assessments and business requirements, establish and maintain a policy for the security of connectivity 7. Establish trusted mechanisms to support the secure transmission and receipt of information 8. Carry out periodic penetration testing to determine adequacy of network protection 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. 2. Define an ISMS in accordance with enterprise policy and the context in which the enterprise operates 3. Align the ISMS with the overall enterprise approach to the management of security 4. Obtain management authorization to implement and operate or change the ISMS. 5. Prepare and maintain a statement of applicability that describes the scope of the ISMS 6. Define and communicate Information security management roles and responsibilities 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 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. 3. Segregate, reduce to the minimum number necessary and actively manage privileged user accounts. Ensure monitoring on all activity on these accounts 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. 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 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 7. Maintain an audit trail of access to information depending upon its sensitivity and regulatory requirements 8. Perform regular management review of all accounts and related privileges
5	Manage endpoint security	1. Configure operating systems in a secure manner 2. Implement device lockdown mechanisms 3. Manage remote access and control (e.g., mobile devices, teleworking) 4. Manage network configuration in a secure manner

NO	Controls	Activities (ISACA, 2018)
		5. Implement network traffic filtering on endpoint devices 6. Protect system integrity 7. Provide physical protection of endpoint devices 8. Dispose of endpoint devices securely 9. Manage malicious access through email and web browsers. For example, block certain websites and deactivate click-through on links for smartphones 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 2. Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage securityrelated risk. 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 4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan 5. Implement information security and privacy training and awareness programs 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. 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 2. Define and communicate risk scenarios, so they can be easily recognized, and the likelihood and impact understood 3. Regularly review the event logs for potential incidents 4. Ensure that security-related incident tickets are created in a timely manner when monitoring identifies potential incidents. 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. 2. Ensure all personnel display properly approved identification at all times 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. 5. Manage requests to allow appropriately authorized access to the computing facilities. 6. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities. 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 2. Conduct ISMS audits at planned intervals. 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 4. Record actions and events that could have an impact on the effectiveness or performance of the ISMS 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 2. Ensure cryptographic controls are in place to protect sensitive electronically stored information 3. Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements 4. Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations. 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.