Business Intelligence Management Studies
Vol. 13, No.50, Winter 2025; P 49-97
ims.atu.ac.ir
DOI: 10.22054/ims.2024.76541.2401

ATU PRESS

ISSN: 2821-0964 eISSN: 2821-0816 Received: 12 November 2023 Revised: 01 October 2024 Accepted: 17 October 2024 Original Research

Hierarchical weighted Expert System for Information Security Assessment Based on ISO 27001 International Standard

Melika Armandi — M.Sc. from Alzahra University, Tehran, Iran

Mina Ranjbarfard — Department of Management, Faculty of Social Sciences and Economics, Alzahra University, Tehran, Iran

Zahra Taheri — lecturer at Alzahra University, Tehran, Iran

rcatr sc t

In this research, an expert system was designed and implemented based on the ISO/ICE27001 standard. In order to create the knowledge base of this expert system, control goals and criteria for evaluating these goals were extracted based on the ISO/ICE27001 standard, and the necessary information was collected to define the rules. Then, the approach of creating rules as well as the rules were confirmed through interviews with experts. The control objectives and evaluation criteria of the control objectives were using the Dematel technique along with the Dalala formula and WASPA method. In the next stage, the five main security objectives were chosen to continue the work due to their emphasis in the research literature. The specified goals were reviewed and confirmed during face-to-face interviews with experts. After designing the expert system, Visual Basic was used to implement the user interface and Excel 2016 was used for inference. The designed system is able to calculate the information security score according to the standard and also is able to calculate

Corresponding Author: m.ranjbarfard@alzahra.ac.ir

How to Cite: Armandi, M., Ranjbarfard, M., Taheri, Z. (2025). Hierarchical weighted Expert System for Information Security Assessment Based on ISO 27001 International Standard, *Journal of Business Intelligence Management Studies*, 13(50), 49-97. DOI: 10.22054/ims.2024.76541.2401

the information security score by applying the weight of the control objectives, the evaluation criteria of the control objectives and the percentage of realization of the main objectives of the information security. The resulted score is shown in three levels of critical status, average status and very good status to the user. Results of the system implementation in two Iranian organizations showed that the system with an average accuracy of 95% has the necessary accuracy and efficiency to evaluate information security.

Introduction

Information is a vital element for the survival of the organization and information security plays a decisive role in modern information organizations. Many organizations use successful global standards such as ISO/ICE27001 to ensure success in implementing and evaluating their information security management system. Organizations can become aware of the state of information security with the lowest cost and highest efficiency by using the intelligent information security audit system. In this research, an expert system with hierarchical coefficients to calculate the organization's information security score based on the ISO/ICE27001 standard was designed and implemented: considering the importance of control goals and evaluation criteria for these goals, as well as calculating the degree of achievement of the main security goals. In the design of this system, unlike other audit expert systems, the importance of information security evaluation criteria has not been considered equal. This system can be used in various organizations and industries for intra-organizational evaluations of information security status and determining corrective measures. Organization with ISO/ICE27001 certification can also use this system as an alternative to traditional audits to increase efficiency and reduce time and cost.

Literature review

ISO 27001 information security management standard

Information security management standards provide a security framework along with specialized techniques for implementing security in the information exchange space. The ISO 27001 international standard was prepared to provide requirements for the establishment, implementation, maintenance and continuous

improvement of an information security management system (Chang and Lee 2013).

The ISO 27001 standard has been able to provide a complete form of security processes and controls for the organization (Wallhoff 2004). Referring to the capabilities of various information security standards shows that ISO 27001 is a leader compared to other standards, especially in the field of information security management systems; (Susanto, Almunawar, and Tuan 2011).

Intelligent information security audit systems

An expert system uses human knowledge to solve problems that normally require human intelligence. Expert systems are designed in such a way that they acquire the intelligence and information available in the minds of experts and provide this knowledge to other members of the organization with the aim of solving problems. The main components of an expert system are its knowledge base and inference engine. The knowledge base contains the necessary knowledge to understand, explain and solve the problem, and it is the inference engine of the brain of the expert system that determines its reasoning method (Tripathi 2011).

Research Question(s)

≠ What are the control goals and evaluation criteria of the information security evaluation expert system?

What is the appropriate architecture of the expert system with coefficients to evaluate the organization's information security?

≠ How are the goals and control security evaluation criteria determined?

How is the main security goal determined for each control?

What is the method of inference in the expert system of evaluating the organization's information security?

Does the designed system have the necessary credibility to measure the organization's information security?

Methodology

This research is applied-developmental in terms of purpose, because by using the ISO 27001 international standard and in order to improve

and perfect the strategies, behaviors, methods, tools, devices, structures and patterns used by the organization. has designed the audit expert system. Also, the research is descriptive in terms of data and its strategy is design.

In order to create the knowledge base of this expert system, control goals, criteria for evaluating these goals and recommendations were extracted based on the ISO/ICE27001 standard, and the necessary information was collected to define the rules. Then, the approach of creating rules as well as the rules were confirmed through interviews with experts. The necessary information for ranking the control objectives and evaluation criteria of the control objectives was collected through a questionnaire and the weight of the control objectives and criteria was calculated using the Dematel technique along with the Dalala formula and WASPA method. In the next stage, the five main security objectives: authenticity, confidentiality, availability, accountability and auditability were chosen to continue the work due to their emphasis in the research literature. After determining which of the main security goals each control is aimed at, the specified goals were reviewed and confirmed during face-to-face interviews with experts. Then, using the information of these four stages, an expert system was designed to evaluate information security based on the ISO/ICE27001 standard. Visual Basic was used to implement the user interface and Excel 2016 was used for inference.

Discussion

In this research, the control objectives and information security evaluation criteria are extracted from the ISO 27001 standard, and the checklist used is completely in accordance with the standard, and the system has calculated the organization's information security score based on the standard. In addition, compared to previous researches, the presented system has special innovative aspects. The ranking of standard control goals and criteria has been done according to the opinion of experts, and the information security score has also been calculated by taking into account the weight of control goals and evaluation criteria. In addition, the main objectives of information security for each recommendation (control) have been determined according to the opinion of experts, and the designed system has also

evaluated the degree of realization of the main security objective in the organization.

It is worth mentioning that the method of assigning points to each control is based on interviews with security auditors in Iran, and the structure of the ISO 27001 standard does not specify a specific method for scoring, which has an impact on the creation of rules and the efficiency of the expert system.

Results

The designed system is able to calculate the information security score according to the standard and also is able to calculate the information security score by applying the weight of the control objectives, the evaluation criteria of the control objectives and the percentage of realization of the main objectives of the information security. The resulted score is shown in three levels of critical status, average status and very good status to the user. Results of the system implementation in two Iranian organizations showed that the system with an average accuracy of 95% has the necessary accuracy and efficiency to evaluate information security.

Keywords:Information Security Management System, Expert System, ISO27001 International Standard, Dematel Technique, Dalala Formula, WASPAS Method

مقاله پژوهشی تاریخ ارسال: ۱۴۰۲/۰۸/۲۱ تاریخ بازنگری: ۱۴۰۳/۰۷/۱۰ تاریخ پذیرش: ۱۴۰۳/۰۷/۲۶ ISSN: 2821-0964 eISSN: 2821-0816

مطالعات مدیریت کسب و کار هوشمند
سال سیزدهم، شماره ۵۰، زمستان ۱۴۰۳، ص ۴۹ تا ۹۷
ims.atu.ac.ir
DOI: 10.22054/ims.2024.76541.2401

سیستم خبره ضریب‌دار سلسله مراتبی جهت ارزیابی امنیت اطلاعات سازمان مبتنی بر استاندارد بین‌المللی ایزو ۲۷۰۰۱

ملیکا ارمندئی کارشناسی‌ارشد مدیریت فناوری اطلاعات، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران

مینا رنجبرفرد * عضو عیات علمی گروه مدیریت، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران

زهرا طاهری دکتری مهندسی صنایع، دانشکده مهندسی صنایع، دانشگاه تربیت مدرس، مدرس مدعو گروه مدیریت، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران

چکیده

بسیاری از سازمان‌ها برای موفقیت در پیاده‌سازی و ارزیابی سیستم مدیریت امنیت اطلاعات خود، از استانداردهای معتبر جهانی نظیر ایزو ۲۷۰۰۱ بهره می‌گیرند. در این پژوهش، یک سیستم خبره ضریب‌دار سلسله‌مراتبی جهت محاسبه امتیاز امنیت اطلاعات سازمان بر مبنای استاندارد بین‌المللی ایزو ۲۷۰۰۱ طراحی و پیاده‌سازی شده است. در این سیستم، بر خلاف سایر سیستم‌های خبره ممیزی موجود، میزان اهمیت معیارهای ارزیابی امنیت به صورت یکسان در نظر گرفته نشده است. اطلاعات لازم جهت ایجاد پایگاه دانش از مطالعات کتابخانه‌ای استخراج شده و همچنین اطلاعات لازم برای رتبه‌بندی اهداف کنترلی و معیارهای ارزیابی از طریق پرسشنامه گردآوری شده است. با به‌کارگیری تکنیک دیمتل به همراه فرمول دالالا و روش واسپاس، وزن اهداف کنترلی و معیارها محاسبه گردید. در مرحله بعد، پنج هدف اصلی امنیت شامل صحت، محرمانگی، در دسترس بودن، مسئولیت‌پذیری و قابلیت ممیزی به دلیل تأکید و تکرار بیشتر در ادبیات پژوهش انتخاب شدند. با استفاده از اطلاعات این چهار مرحله، سیستم خبره طراحی شد. جهت پیاده‌سازی رابط کاربری از زبان ویژوال بیسیک و برای استنتاج از اکسل ۲۰۱۶ استفاده شد. این

* نویسنده مسئول : m.ranjbarfard@alzahra.ac.ir

سیستم علاوه بر محاسبه امتیاز امنیت اطلاعات بر حسب استاندارد، قادر به محاسبه امتیاز امنیت با اعمال وزن اهداف کنترلی و معیارهای ارزیابی اهداف کنترلی و درصد تحقق اهداف اصلی امنیت است و نتایج را در سه سطح وضعیت بحرانی، متوسط و بسیار خوب نشان می‌دهد. اجرای سیستم در دو سازمان ایرانی نشان داد که سیستم با میانگین دقت ٪۹۵ دارای دقت و کارایی لازم جهت ارزیابی امنیت اطلاعات است. سایر نتایج در قالب بحث و نتیجه‌گیری در پژوهش ارائه شده است.

کلیدواژه‌ها: سیستم مدیریت امنیت اطلاعات، سیستم خبره، استاندارد بین‌المللی ایزو ۲۷۰۰۱، تکنیک دیمتل، فرمول دالالا، روش واسپاس.

۱. مقدمه

مدیریت متعارف و قدیمی امنیت اطلاعات پاسخگوی نیازهای ساختار فعلی نیست (Ganji et al. 2019). شاه‌بهرامی و همکارانش (۱۳۹۷) به نقل از «برودریک»[1] (۲۰۰۶) بیان می‌کنند که برای حل مسئله امنیت اطلاعات، سازمان‌ها نیازمند به‌کارگیری مجموعه گسترده‌ای از فناوری، دانش و قوانین سازمانی هستند. باید توجه داشت که فناوری به تنهایی قادر به حفاظت از سازمان نیست، چرا که امنیت اطلاعات یک مشکل صرفاً فنی نیست و اجزای کلیدی دیگر آن، شامل فرآیندها و کارکنان، خود یک مسئله مدیریتی و کسب‌وکار است (شاه‌بهرامی و همکاران، ۱۳۹۷). مدیریت امنیت اطلاعات، رویکردی برای پیاده‌سازی و نگهداری امنیت اطلاعات است که توسط سازمان‌ها اتخاذ می‌شود و متضمن تداوم کسب‌وکار و حداقل کردن آسیب‌های ناشی از حوادث امنیتی است که دارایی‌های اطلاعاتی سازمان را تهدید می‌کند (جعفرنژاد و تقوا، ۱۳۹۸). مدیریت امنیت اطلاعات را می‌توان به عنوان یک منبع ارزشمند در نظر گرفت که اثربخشی آن باید فراتر از سودهای مالی فوری یا عملکرد کلی شرکت به عنوان متغیر وابسته اصلی اندازه‌گیری شود (Mirtsch et al., 2021). سیستم مدیریت امنیت اطلاعات این امکان را فراهم می‌کند که سازمان‌ها بر مبنای ساختار خود، حاکمیت امنیتی برقرار کنند؛ به‌طوری‌که قوانین، مسئولیت‌ها، سیاست‌ها، رویه‌ها، فرآیندها و منابع به‌صورت دقیق در راستای مدیریت دارایی‌های اطلاعاتی تعریف شوند (Fonseca-Herrera, Rojas, and Florez, 2021). پژوهشی در سال ۲۰۲۳ به بررسی کاربردهای سیاست‌های مدیریت امنیت اطلاعات دیجیتال از نظر عملکرد و اجرا پرداخته است. در این پژوهش، بر اساس مطالعه نظام‌مند ادبیات این حوزه، نتایج و چالش‌های پیش‌روی کتابخانه‌ها در پیاده‌سازی این سیاست‌ها بررسی شده است (Farid, Warraich, and Iftikhar, 2023). با توجه به دنیایی که به‌طور فزاینده‌ای به هم پیوسته و شاهد فناوری‌های نوظهور است، نیاز است مطالعات حوزه سیستم‌های مدیریت امنیت اطلاعات تغییر مسیر یابند. افزایش قابل توجهی در تلاش‌های

1.. Broderic

تحقیقاتی لازم است تا بفهمیم سازمان‌ها چگونه می‌توانند دارایی‌های اطلاعاتی را ایمن کنند و استانداردهای اصلی بین‌المللی نظیر ایزو ۲۷۰۰۱ چه نقشی در ارائه راهنمایی در برابر این پیچیدگی روزافزون دارند (Culot et al., 2021). به دلیل محدودیت‌هایی که در زمان و حافظه انسان وجود دارد از یک سو و دشواری‌های ممیزی سیستم مدیریت امنیت اطلاعات در سازمان‌ها از سوی دیگر، سیستم‌های خبره هوشمند می‌توانند نقش مؤثری در تسهیل بررسی وضعیت امنیت اطلاعات در سازمان ایفا کنند. این سیستم‌ها به کارشناسان فناوری اطلاعات کمک می‌کنند تا به‌صورت خودکار در مورد وضعیت امنیت سازمان آگاهی کسب کنند و برای مقابله مناسب با مخاطرات موجود، بهترین تصمیم را اتخاذ کنند. استفاده از سیستم‌های هوشمند برای ممیزی امنیت اطلاعات منجر به بهینه‌سازی فرآیند ممیزی از منظر زمان و هزینه در مقایسه با فرآیند سنتی ممیزی می‌شود.

شایان ذکر است که سیستم‌های هوشمند ممیزی به سازمان‌ها در جهت تشخیص فرآیندهایی که نیاز به ملاحظات امنیتی بیشتری دارند، کمک قابل توجهی می‌کنند و کنترل فرآیندهای اجرایی در دوره‌های کوتاه‌مدت و به شکل ارزیابی‌های درون‌سازمانی می‌تواند به آسانی صورت گیرد. پس از ارزیابی‌های دوره‌ای و با تحلیل نتایج به‌دست‌آمده، امکان مهندسی مجدد فرآیندهای اجرایی سازمان و رعایت ملاحظات امنیتی در قالب تهیه و بازنگری فرآیند، خط‌مشی، آیین‌نامه، دستورالعمل، روش و فرم‌های اجرایی نیز وجود دارد. برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات، سازمان‌ها می‌توانند از روش‌ها و استانداردهای موفق جهانی در این زمینه بهره‌گیرند. پس از پیاده‌سازی سیستم مدیریت امنیت اطلاعات، انطباق آن با کنترل‌ها و الزامات استاندارد بین‌المللی بررسی می‌شود تا از کارایی هر چه بهتر و بهبود مستمر این سیستم اطمینان حاصل شود (واعظی‌نژاد، ۱۳۹۳).

استاندارد ایزو ۲۷۰۰۱، ابزاری ایده‌آل برای تأمین امنیت اطلاعات است اما باوجود توانمندی این ابزار و ضرورت مدیریت امنیت اطلاعات، بسیاری از سازمان‌های کوچک‌تر به‌علت زمان‌بر بودن و هزینه‌های پیاده‌سازی این استاندارد به روش‌های ناکارآمد و ناقص

روی می‌آورند. ازاین‌رو دو تن از پژوهشگران به نام «مرا-آمورس»۱ و «روا»۲، به بررسی رویکرد پیاده‌سازی ایزو ۲۷۰۰۱ به‌عنوان یک ابزار استراتژیک و به‌صورت پلکانی پرداخته‌اند (Mera-Amores and Roa, 2024). خفید و راکی از طریق یکپارچه‌سازی ISO 27002 و ISO27004 یک مدل ارزیابی برای نظام مدیریت امنیت اطلاعات ارائه کردند به‌طوری‌که راهنماهای ISO27002 را به پارامترهای ارزیابی تبدیل کردند و از ISO27004 برای اندازه‌گیری عملکرد استفاده کردند (Khafidh, Ruki 2024). در یک مطالعه موردی «کمال»۳ و همکارانش به ارزیابی و ممیزی امنیت اطلاعات بر اساس ایزو ۲۷۰۰۱ در یکی از سازمان‌های کشور اندونزی پرداخته‌اند. این پژوهشگران توانسته‌اند نقاط قوت و ضعف این سازمان را بر اساس ایزو ۲۷۰۰۱ شناسایی کرده و مسیر مشخصی برای بهبود وضعیت موجود ارائه کنند (Kamal, et al., 2024). «هرات» و دو تن از همکارانش برای کمک به مدیران ارشد در زمینه ارزیابی میزان پیشرفت استراتژی‌های امنیت اطلاعات در سازمان، پنج چارچوب حاکمیتی و کنترلی (COBIT، SABSA، ISG، ITIL و ISO 27000) را به کارت امتیازی متوازن امنیت اطلاعات (InfoSec BSC) نگاشت کرده و یک طراحی مفهومی از ابزار سنجش عملکرد امنیت اطلاعات برای استفاده مدیران ارشد توسعه داده‌اند (Herath, Herath and Cullum 2023). انجلینا و فیانتی از چارچوب COBIT19 برای ارزیابی سطح قابلیت‌های حاکمیت فناوری اطلاعات و کنترل‌های امنیت اطلاعات سازمان استفاده کردند (Angelina1, Fianty, 2024). با توجه به شکاف موجود میان مقررات و مجازات‌های تعریف‌شده در مقابل عدم تأمین امنیت اطلاعات و وضعیت موجود آن، «سورسا»۴ و «هلو»۵، شکست‌ها و اثرات امنیت اطلاعات و همچنین مؤثرترین کنترل‌ها را برای کاهش خطرات امنیت اطلاعات در سازمان‌ها شناسایی و بررسی کرده‌اند. نتایج این پژوهش هم از منظر نظری و هم از منظر عملی برای سازمان‌ها و ارزیابان ایزو

1. Mera-Amores
2. Roa
3. Kamal
4. Suorsa
5. Helo

۲۷۰۰۱ قابل بهره‌برداری است (Suora and Helo, 2023). «کولات» و همکارانش مطالعات جامعی در زمینه پژوهش‌های مربوط به استاندارد ایزو ۲۷۰۰۱ انجام داده‌اند. در این مقاله مضامین و مضامین فرعی پژوهش در پنج کانون پژوهشی گسترده شناسایی شده‌اند: ارتباط با سایر استانداردها، انگیزه‌ها، مسائل در اجرا، نتایج احتمالی و عوامل زمینه‌ای. زمینه‌های مطالعاتی آینده در این مقاله به بحث گذاشته‌شده و اطلاعات علمی مناسبی برای مدیرانی که قصد پیاده‌سازی این استاندارد را دارند، فراهم شده است. محققان نتیجه‌گیری کرده‌اند که بیشتر مطالعات جنبه‌های فنی این استاندارد را موردبررسی قرار داده و تعداد کمی از مقالات به رویکردهای مدیریتی در این زمینه توجه کرده‌اند و زمان آن رسیده که رویکردهای مدیریتی نیز بیشتر از پیش موردتوجه قرار گیرند (Culot et al. 2021). گنجی و همکارانش نیز در سال ۲۰۱۹ یک مرور ادبیات نظام‌مند در زمینه سیستم‌های مبتنی بر استاندارد ایزو ۲۷۰۰۱ انجام دادند، با این هدف که حدود نوآوری‌های در دسترس را برای کمک به سازمان‌ها و طرف‌های ذینفع در درک بهتر یا انطباق با این استاندارد تعیین کنند. واضح‌ترین یافته‌ای که از این مطالعه به دست می‌آید این است که پتانسیل قابل‌توجهی برای محققان برای بررسی سیستم مدیریت امنیت اطلاعات تحت یک رویکرد جامع وجود دارد، ادبیات فعلی فاقد انگیزه برای هدف‌گذاری ابتکارات جدید در زمینه سیستم مدیریت امنیت اطلاعات و استاندارد ایزو ۲۷۰۰۱ است (Ganji et al. 2019). بدین منظور با توجه به خلأهای ذکرشده، توسعه یک سیستم خبره هوشمند با در نظر گرفتن تأثیر واقعی هر هدف کنترلی و معیار ارزیابی در برقراری امنیت سازمان ضروری به نظر می‌رسد.

فرآیند ممیزی، یک فرآیند کارآمد، پیچیده، مرحله‌ای، زمان‌بر و پرهزینه است که نیازمند خلق نوآوری و پیشرفت می‌باشد. بررسی پژوهش‌های انجام‌شده در زمینه فرآیند ممیزی با استفاده از سیستم‌های هوشمند نشان می‌دهد که توجه به یکسان نبودن تأثیر معیارهای مختلف در برقراری سازمان امن، از جمله مسائل مهم و قابل تأمل است که تاکنون در هیچ پژوهشی در نظر گرفته نشده است. شرکت‌های فعال در زمینه خدمات

مدیریت امنیت اطلاعات در ایران و سایر کشورها از استانداردهای جهانی برای انجام ارزیابی‌های خود استفاده می‌کنند. ارزیابی بر اساس استاندارد، با توجه به یک سری اهداف کنترلی و معیارهای ارزیابی مرتبط انجام می‌شود که دارای دو ضعف عمده است: اول اینکه اهمیت اهداف کنترلی و معیارهای ارزیابی یکسان در نظر گرفته می‌شود و دوم اینکه در استفاده از استاندارد، اهداف اصلی امنیت اطلاعات در سازمان مورد نظر در نظر گرفته نمی‌شود. به منظور برطرف کردن این دو خلأ، این مقاله به طراحی و توسعه یک سیستم خبره در جهت بهبود ارزیابی امنیت اطلاعات سازمان پرداخته است. اگرچه سیستم‌های خبره بسیاری در حوزه امنیت اطلاعات توسعه داده شده‌اند، اما در تمام سیستم‌های موجود، اهمیت اهداف و کنترل‌های امنیتی یکسان در نظر گرفته شده است. در حالی که برخی اهداف و کنترل‌ها از تأثیر بالاتری در برقراری امنیت نسبت به بقیه برخوردارند و در صورت عدم اجرای صحیح، امنیت سازمان را با مخاطرات جدی‌تری روبرو می‌کنند. عدم وزن‌دهی به اهداف و معیارهای ارزیابی اهداف کنترلی، باعث توجه مناسب به هدف مورد نظر در برقراری امنیت شده و به جلوگیری از بروز چالش‌های پرریسک امنیتی کمک خواهد کرد.

با این وجود، تاکنون سیستم خبره‌ای با تکیه بر استاندارد بین‌المللی ISO/IEC 27001 و با ساختار ضریب‌دار سلسله‌مراتبی به منظور انجام خودکار فرآیند ممیزی امنیت اطلاعات سازمان ایجاد نشده است. همچنین، سیستم‌های طراحی‌شده قادر به بیان سطح امنیتی سازمان در هر یک از اهداف اصلی امنیتی نبوده‌اند. بنابراین، نیاز به ایجاد یک سیستم ارزیاب که بتواند با دقت بیشتر و خطای کمتر، ارزیابی را در فواصل کوتاه و با هزینه‌ای کمتر از ارزیابی ممیزان انسانی انجام دهد و سطح امنیتی سازمان را در هر یک از اهداف امنیتی بیان کند، احساس می‌شود. چنین سیستمی می‌تواند به سازمان در رسیدن به سطح امنیتی قابل قبول کمک قابل توجهی نماید.

بدین منظور، پس از بررسی ادبیات، اهداف امنیتی شامل صحت، محرمانگی، در دسترس بودن، مسئولیت‌پذیری و قابلیت ممیزی برای ادامه پژوهش انتخاب گردید. از این

رو، هدف اصلی این پژوهش طراحی یک سیستم خبره هوشمند ممیزی امنیت اطلاعات با ویژگی‌های فوق‌الذکر در نظر گرفته شده است.

پژوهش حاضر به توسعه یک سیستم خبره ضریب‌دار سلسله‌مراتبی به‌منظور انجام فرآیند ممیزی امنیت اطلاعات سازمان با تکیه بر استاندارد بین‌المللی ایزو ۲۷۰۰۱ می‌پردازد. این سیستم با بهینه‌سازی فرآیند ممیزی و سرعت بخشیدن به تشخیص وضعیت امنیت اطلاعات در سازمان، گامی در جهت نظام‌مند نمودن حفظ امنیت سازمان طبق استانداردهای جهانی برمی‌دارد و می‌تواند در بازه‌های کوتاه و بدون پیچیدگی، سطح امنیت سازمان را به تصویر بکشد و درصد تحقق مهم‌ترین اهداف امنیتی را محاسبه کند.

سؤالات پژوهش عبارتند از:

۱. اهداف کنترلی و معیارهای ارزیابی اهداف سیستم خبره ارزیابی امنیت اطلاعات کدام‌اند؟

۲. معماری مناسب سیستم خبره ضریب‌دار جهت ارزیابی امنیت اطلاعات سازمان چیست؟

۳. وزن اهداف و معیارهای ارزیابی امنیت کنترلی چگونه تعیین می‌شوند؟

۴. هدف اصلی امنیت برای هر کنترل چگونه تعیین شده است؟

۵. نحوه استنتاج در سیستم خبره ارزیابی امنیت اطلاعات سازمان چگونه است؟

۶. آیا سیستم طراحی‌شده دارای اعتبار لازم جهت سنجش امنیت اطلاعات سازمان می‌باشد؟

بنابراین، سازمان‌ها و صنایع مختلف برای ارزیابی‌های درون‌سازمانی وضعیت امنیت اطلاعات و انجام اقدامات اصلاحی در جهت بهبود وضعیت امنیت اطلاعات، و همچنین شرکت‌های دارای پروانه گواهی ایزو ۲۷۰۰۱ برای انجام ممیزی با کمک سیستم خبره، با هدف افزایش کارایی و کاهش زمان و هزینه، بهره‌برداران از نتایج این پژوهش هستند.

۲. مرور ادبیات

۲-۱. استاندارد مدیریت امنیت اطلاعات ایزو ۲۷۰۰۱

استانداردهای مدیریت امنیت اطلاعات یک چارچوب امنیتی همراه با فن‌های تخصصی برای پیاده‌سازی امنیت در فضای تبادل اطلاعات فراهم می‌کنند. استاندارد بین‌المللی ایزو ۲۷۰۰۱ به‌منظور ارائه الزاماتی برای استقرار، پیاده‌سازی، نگهداری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات تهیه‌شده است. این استاندارد برای پیاده‌سازی در انواع سازمان‌های دولتی، خصوصی، بزرگ و یا کوچک مناسب است. این استاندارد اظهار می‌دارد که در هر ناحیه، ممیز باید اوضاع کنونی را با توجه به معیارها یا استانداردهای امنیتی که می‌تواند سازمان را به بهترین نحو محافظت کنند، ارزیابی نماید (Chang and Lee 2013).

استاندارد ایزو ۲۷۰۰۱ توانسته شکل کاملی از فرآیندها و کنترل‌های امنیتی را برای سازمان فراهم آورد (Wallhoff 2004). اشاره به قابلیت استانداردهای مختلف امنیت اطلاعات نشان می‌دهد که ایزو ۲۷۰۰۱ نسبت به سایر استانداردها، به‌ویژه در زمینه سیستم‌های مدیریت امنیت اطلاعات پیشرو است؛ بنابراین این استاندارد نسبت به دیگر استانداردهای امنیتی به‌خوبی شناخته‌شده و به‌آسانی اجرا می‌شود، همین موضوع موجبات پذیرش آن توسط ذی‌نفعان را فراهم می‌سازد (Susanto, Almunawar, and Tuan 2011). با توجه به اینکه هدف پژوهش حاضر طراحی سیستم خبره ممیزی امنیت اطلاعات در سازمان است به دلایل زیر استاندارد ایزو ۲۷۰۰۱ برای ادامه پژوهش انتخاب شده است:

- استاندارد ایزو ۲۷۰۰۱ مهم‌ترین و پرمراجعه‌ترین استاندارد مدیریت امنیت اطلاعات است.
- استاندارد ایزو ۲۷۰۰۱ زمینه مناسبی برای بهره‌گیری از رویکرد حفاظت سازمانی فراهم کرده است و به تمام سازمان‌ها با هراندازه، ساختار، فرهنگ‌سازمانی و هر سطح بلوغی کمک می‌کند تا با پیاده‌سازی و استقرار سیستم مدیریت امنیت اطلاعات فرآیندهای امنیتی خود را متناسب با الزامات خویش به نحو مطلوبی بهبود ببخشند.

استاندارد ایزو ۲۷۰۰۱ می‌تواند توسط مرجع تائید شده ایزو مورد ممیزی قرار بگیرد و سازمان‌های مورد تائید موفق به اخذ گواهینامه معتبر شوند.

نسبت به سایر استانداردها پوشش کامل‌تری در فرآیندها و کنترل‌های امنیتی دارد.

گستردگی استفاده از این استاندارد در سطح جهان قابل‌توجه است.

به دلیل اجرا و پیاده‌سازی آسان‌تر نسبت به استانداردهای دیگر، مقبولیت بهتری توسط ذی‌نفعان دارد.

هرساله تعداد گواهینامه‌های صادرشده استاندارد ایزو ۲۷۰۰۱ توسط سازمان‌ها رشد صعودی قابل‌توجهی داشته است.

۲-۲. سیستم‌های هوشمند ممیزی امنیت اطلاعات

سیستم خبره از دانش انسانی برای حل مسائلی استفاده می‌کند که معمولاً به هوش انسانی نیاز دارد. سیستم‌های خبره به‌گونه‌ای طراحی شده‌اند که هوش و اطلاعات موجود در عقل متخصصان را کسب کرده و این دانش را باهدف حل مشکل در اختیار سایر اعضای سازمان قرار دهند. اجزای اصلی یک سیستم خبره، پایگاه دانش و موتور استنتاج آن هستند. پایگاه دانش شامل دانش ضروری برای فهم، تبیین و حل مسئله بوده و موتور استنتاج مغز سیستم خبره است که روش استدلال آن را تعیین می‌کند (Tripathi 2011). در مطالعات متعددی بر اهمیت و منافع حاصل از جایگزینی ممیزی امنیت اطلاعات با استفاده از سیستم‌های هوشمند که موضوع این پژوهش نیز هست، تأکید شده است. یکی از این مطالعات بیان می‌کند سیستم‌های خبره در باب جایگزینی با متخصص انسانی مزایای قابل‌توجهی به همراه خواهند داشت. (Atymtayeva et al. 2012). راقاوندار و همکاران با استفاده از هوش مصنوعی به طراحی و توسعه یک سیستم پردازش دانش هوشمند برای بهینه‌سازی امنیت سیستم نرم‌افزاری پرداختند (Raghavendra et al. 2023). پلتفرمی بر پایه اینترنت اشیاء و هوش مصنوعی برای مدیریت امنیت اطلاعاتی سازمانی طراحی شده است. این پلتفرم چهار بخش را پوشش می‌دهد که عبارت‌اند از مدیریت داده‌کاوی اینترنت اشیاء، مدیریت تجهیزات، مدیریت کلید و مدیریت پایگاه داده. این محققان پلتفرم

مدیریت امنیت اطلاعات طراحی‌شده را در بخش‌های آزمون هم‌زمانی، آزمون استرس، آزمون داده‌های بزرگ و آزمون امنیتی مورد آزمایش قرار داده‌اند که نتایج نشان‌دهنده عملکرد مناسب و پایدار آن است (Sun and Bai 2022). «هنتی» و همکارانش سیستم هوشمندی بر مبنای چندین اصل شامل، مدیریت امنیت اطلاعات، ارتباط شبکه‌ای خودکار، علم کامپیوتر، هوش مصنوعی، تئوری کنترل مدرن، آمارها، علوم اجتماعی، تئوری سازمانی و رفتارها، علم مدیریت، استراتژی‌های تجاری، تحلیل ریسک و اقتصاد طراحی کرده‌اند (Hentea 2007). «سندی» و همکارانش برای ارزیابی مخاطرات امنیت اطلاعات بر پایه استاندارد ایزو ۲۷۰۰۱ و با ترکیب روش‌های فازی یک سیستم هوشمند طراحی کرده‌اند. در این تحقیق برای طبقه‌بندی دارایی‌ها از مدل زکمن استفاده‌شده و از سه دیدگاه کسب‌وکار، دیدگاه منطقی و دارایی‌های فیزیکی به بررسی دارایی‌ها با استفاده از مفهوم مثلث طلایی امنیت (محرمانه بودن، یکپارچگی و در دسترس بودن) پرداخته شده است. خروجی ارزیابی، جدولی شامل ارزش دارایی، اثر آسیب‌پذیری و اثر تهدید همراه با میزان ریسک محاسبه‌شده است (Sendi et al. 2010). پژوهش «گوزتپ» نیز به ارائه یک سیستم خبره برای امنیت سایبری با استفاده از قوانین فازی اختصاص دارد. محقق پس از مصاحبه با خبرگان سایبری و مدیران سیستم، ورودی و خروجی سیستم را مشخص کرده است. پایگاه دانش بر مبنای اطلاعاتی از قبیل تهدیدات، پروفایل‌های تروریستی و یا تکنیک‌های حملات سایبری عمل می‌کند (Goztepe 2012). در پژوهش «کوژاخمت» و دیگران از یک سیستم خبره فازی در ممیزی امنیت اطلاعات مبتنی بر استاندارد بین‌المللی ایزو ۲۷۰۰۱: ۲۰۰۵ استفاده شده است. سیستم خبره ارائه‌شده به‌صورت تعامل پرسش و پاسخ بین کاربر و سیستم بوده و پاسخ‌های کاربر را در مورد سؤالات ممیزی، تجزیه‌وتحلیل کرده و نتیجه را در قالب یک توصیه ارائه می‌کند. این پژوهش برای خودکار کردن برخی از روش‌های ممیزی مانند شناسایی موارد نقض امنیتی بالقوه از طریق بررسی لاگ[1]های سیستم استفاده کرده است (Kozhakhmet et al. 2012). «کاناتف» و

1. log

همکارانش یک سیستم خبره فازی مدیریت امنیت اطلاعات توسعه داده‌اند. این سیستم مبتنی بر استانداردهای بین‌المللی بوده و به‌صورت خودکار اطلاعات را جمع‌آوری و آن‌ها را با منطق فازی را تجزیه‌وتحلیل کرده و توصیه‌هایی را بر اساس نتایج ارائه می‌کند. (Kanatov, Atymtayeva, and Yagaliyeva 2014). در پژوهشی که توسط «بارتوس» و همکاران انجام‌شده یک ابزار فازی برای تحلیل ریسک در زمینه امنیت اطلاعات ارائه شده است. پایگاه دانش حاصل گردآوری اطلاعات توسط مصاحبه هدفمند با روش دلفی با خبرگان حوزه امنیت بوده و قوانین به شکل اگر-آنگاه برای انجام تصمیم‌گیری استفاده می‌شود (Bartos et al. 2014). در پژوهش دیگری یک سیستم خبره برای ارزیابی امنیت با استفاده از منطق فازی برای این مهم طراحی‌شده که بر اساس مفهوم فناوری و تکنیک-های هوش مصنوعی قادر به تشخیص شرایط مشکوک است (Rkaur, Rani, and Garg, 2016). «لاخنو» و همکارانش یک سیستم خبره تطبیقی برای امنیت اطلاعات با استفاده از روش خوشه‌بندی ویژگی‌های ناهنجار و حملات سایبری ارائه کرده‌اند. در چارچوب نظری پژوهش، پارامترهای شناخته‌شده آماری و خوشه‌ای برای تهدیدات اینترنتی، ناهنجاری‌ها و حملات سایبری و نیز اشتباهات نوع سوم در طی روش آموزش سیستم خبره موردتوجه قرارگرفته است. برای ارزیابی اثربخشی عملکرد فرآیند آموزش سیستم خبره از مفهوم آنتروپی و فاصله اطلاعاتی در هنگام خوشه‌بندی استفاده‌شده است. مدل ارائه‌شده سطح تشخیص طبقه‌بندی حملات رایج سایبری را از ۷۶٫۵٪ به ۹۹٫۱٪ رسانده است. در سطح اثربخشی، شناخت خوشه‌ها با استفاده از الگوریتم ژنتیک و ترکیبی از شبکه‌های عصبی انجام‌گرفته است (Lakhno et al. 2016).

برخی از مقالات به ارزیابی ریسک سیستم مدیریت امنیت اطلاعات سازمان‌ها پرداخته‌اند. ازجمله مقاله «فوتیس»، «چاتزیدیمیتریو» و «کاماریوتو» که چارچوبی برای ارزیابی ریسک فرآیندهای مدیریت امنیت اطلاعات سازمان‌های تجاری در تطابق با استاندارد ایزو ۲۷۰۰۱، ارائه کرده است. در این مقاله علاوه بر فرآیند ارزیابی ریسک، مدیریت تنظیمات ضروری برای دستیابی به عملکردهای مطابق با استانداردهای امنیت

اطلاعـات و مشـکلات و چالش‌هـای پـیش رو موردبحـث قـرار گرفتـه اسـت (Fotis, Chatzidimitriou and Kamariotou 2022). در پـژوهش دیگـری یـک رویکـرد تصمیم‌گیری چندمعیاره گروهی[1] برای ارزیابی مدیریت امنیت اطلاعات پیشنهاد شده است. مدل پیشنهادی این محققان از ابزار فازی پیچیده شهودی استفاده می‌کنـد کـه ابـزار مناسـبی برای مسائلی است که علاوه بر عدم قطعیت، با تناوب نیز روبرو هستند (Azam, Ali khan and Yang, 2022). «ساها» و همکارانش یک چارچوب اطلاعاتی مبتنـی بـر هستان‌شناسـی را برای انطبـاق بـا اسـتانداردهای کوبیـت ۴ و ایـزو ۱۷۷۹۹، بـه‌عنوان یـک راه‌حـل ممیـزی خودکار به‌جای ممیزی دستی ارائه کرده‌انـد. آن‌هـا بـا اجـرای ایـن چـارچوب در حـوزه‌ی بانکی و در شرایط واقعی بررسی کردند که استانداردهای امنیتی به‌درستی اجرا شـده‌اند، یـا به دلیل مسائلی مانند مشکلات سیستمی و سهل‌انگاری کارکنان نقض مـی‌شـوند (Saha et al. 2013). «چانگ» و «لی» (۲۰۱۳) در پژوهش خود به ارزیابی ریسـک سیسـتم اطلاعـاتی حضوروغیاب در یک سازمان دولتی پرداخته‌اند. این مطالعه با ترکیـب اسـتاندارد مـدیریت امنیت اطلاعات ایزو ۲۷۰۰۱ و استاندارد تکنیک‌های امنیتی فنـاوری اطلاعـات[2] بـه ارزیـابی ریسک‌های امنیتی سیستم حضوروغیاب پرداخته است. سـه متغیـر ارزیـابی دارایـی، سـطوح تهدید و سطح آسیب‌پذیری به‌عنوان ورودی‌های سیستم فازی استفاده شده‌انـد. نتیجـه‌بخش خروجی محاسبه ریسک است که به تصمیم‌گیری در بازار و تعیین قابل‌قبول بودن ریسـک-ها کمک می‌کند. با استفاده از درخت رگرسـیون دقـت خروجـی سیسـتم برابـر بـا ۹۷,۵۶۸ محاسبه‌شـده اسـت (Chang and Lee 2013). «سـیهوی» و همکـارانش ابـزاری را توسـعه دادند که با کمک استاندارد ایزو ۲۷۰۰۲ به ارزیابی امنیت اطلاعات می‌پردازد. ایـن سیسـتم در دو سطح مدیر و کارمند فناوری اطلاعات و با دو دسته سؤال متفاوت اجـرا می‌شـود. در طراحی این سیستم فهرستی از خطرات احتمالی که سازمان به‌طور بـالقوه امکـان مواجهـه بـا آن‌ها را خواهد داشت و سطح احتمال و اثر هرکدام نشان داده شده است. بـا ترکیـب نتـایج حاصل از تجزیه‌وتحلیل، ارتباط بین احتمال خطـر و سـطح تـأثیر هـر ریسـک به‌دسـت‌آمده

1. Multi Criteria Group Decision Making
2. ISO/IEC 27005:2008

است. سیستم یادشده در بهینه‌سازی تصمیم‌گیری‌های امنیتی و در اولویت‌بندی خطرات بحرانی که امنیت سازمان را تهدید می‌کنند مؤثر است (Sihwi, Andriyanto, Anggrainingsih 2016). مطالعه «پیچ» و «گرودزکی» یک سیستم امنیتی دارای امکاناتی نظیر رمزنگاری، حساس بودن به مزاحمت‌ها، عمرمحدود کلیدها و غیره ارائه می‌کند. تمرکز این پژوهشگران بر خودکارسازی مدل امنیتی ارائه شده بوده و در طول ارزیابی تغییرات تمام عوامل منتخب به‌عنوان ویژگی‌های امنیتی در حین اجرای پروتکل بررسی می‌شوند. درواقع این سیستم قادر به تغییر سطح امنیتی است. شاخص اصلی ارزیابی، پارامتر زمان بوده که با علامت‌گذاری طول عمر عناصر (کلیدها، پیام و غیره) معرفی می‌شود. هنگامی‌که ارزش زمان فعالیت یک عنصر بیش از طول عمر آن باشد، ارتباط امنیتی قطعاً تهدید می‌شود. درنهایت پژوهشگران با پیشنهاد یک‌زمان خودکار برای بررسی انواع تهدیدها، از خطرات قابل‌توجهی جلوگیری کرده‌اند. این رویکرد می‌تواند برای شناسایی هکرها و ورود غیرمجاز به سیستم کاربرد قابل‌توجهی داشته باشد (Piech and Grodzki 2017). «پرونشا» و «بوربینها» یک مدل بلوغ برای برنامه‌ریزی، اجرا، نظارت و بهبود سیستم مدیریت امنیت اطلاعات مبتنی بر استاندارد ایزو ۲۷۰۰۱ توسعه داده‌اند. هدف این مدل ارائه ابزار ارزیابی برای سازمان‌ها به‌منظور شناخت سطح بلوغ فعلی سیستم مدیریت امنیت اطلاعات و برنامه‌ریزی برای دستیابی به سطح بلوغ هدف است. در این مقاله نتایج به‌کارگیری مدل در پنج سازمان به بحث گذاشته شده است (Proenca and Borbinha 2018).

«فونسکا-هررا» و همکارانش مدلی برای سیستم مدیریت امنیت اطلاعات ارائه کرده و آن را در یک شرکت واقعی پیاده‌سازی کرده‌اند. مدل پیشنهادی که در سازمان‌های مختلف قابل‌استفاده است، می‌تواند مبنایی برای پیاده‌سازی و درنتیجه کسب گواهی ایزو ۲۷۰۰۱ باشد. هدف محققان ارائه مدلی بوده که سازمان را در پیاده‌سازی نظام‌مند و مکفی کنترل‌ها، رویه‌ها و سیاست‌های موردنیاز برای دستیابی به یکپارچگی، محرمانه بودن و در دسترس بودن دارایی‌های اطلاعاتی، توانمند سازد. نتایج پیاده‌سازی این مدل نیز

رضایت‌بخش بوده است (Fonseca-Herrera, Rojas, and Florez 2021). «میرچ» و همکارانش (۲۰۲۱) با پیمایش داده‌های مربوط به ۱۲۵ شرکت دارای گواهینامه ایزو ۲۷۰۰۱ در آلمان به بررسی انگیزه‌ها، تأثیرات تجربه‌شده و موانع اجرای این استاندارد پرداخته‌اند. نتایج این مطالعه نشان می‌دهد که این استاندارد را می‌توان به‌عنوان یک نوآوری سازمانی پیشگیرانه موردتوجه قرار داد که باوجود عدم منافع مالی فوری، توانایی جلوگیری از پیامدهای نامطلوب را دارد (Mirtsch et al. 2021).

در مطالعات داخل کشور شیخ‌ابومسعودی و همکارانش به ارزیابی سیستم‌های اطلاعات مدیریت زیرمجموعه دانشگاه علوم پزشکی اصفهان، بر اساس استاندارد ایزو ۲۷۰۰۱ پرداخته‌اند. این محققان با بهره‌گیری از چک‌لیست بین‌المللی مبتنی بر این استاندارد، داده‌های موردنیاز برای ارزیابی خود را از طریق مصاحبه، مشاهده و گردآوری مستندات از مراکز رایانه دانشکده‌ها، بیمارستان‌های زیرمجموعه و مراکز اطلاعات و آمار جمع‌آوری کرده و بر اساس نتایج به‌دست‌آمده توصیه‌های کاربردی برای افزایش سطح امنیت اطلاعات در مجموعه موردبررسی خود ارائه کرده‌اند (شیخ‌ابومسعودی و همکاران، ۱۳۹۴). میدانی و همکارانش بررسی مشابهی در خصوص امنیت سیستم‌های اطلاعاتی بیمارستانی ارائه کرده‌اند. این بررسی نیز بر مبنای استاندارد ایزو ۲۷۰۰۱ و «هیپا[1]» که استانداردی در زمینه سیستم‌های اطلاعاتی بیمارستانی است و به روش دلفی در چهار بیمارستان دولتی که از سیستم‌های اطلاعاتی متفاوتی استفاده می‌کردند، انجام شده است. یافته‌های این مطالعه نشان می‌دهد که در بیمارستان‌های موردبررسی، امنیت مدیریتی و امنیت فیزیکی در سطح پایین و امنیت فنی در سطح متوسطی قرار دارد (میدانی و همکاران، ۱۳۹۶). این دو پژوهش، مطالعات موردی هستند که باوجود دقت عمل در گردآوری و تحلیل داده‌ها، نتایج قابل بهره‌برداری در سایر زمینه‌ها ارائه نمی‌کنند. شاه‌بهرامی و همکارانش در پژوهش خود به شناسایی و اولویت‌بندی عوامل تأثیرگذار بر سیستم مدیریت امنیت اطلاعات پرداخته‌اند. این محققان پارامترهای تأثیرگذار را به دو دسته

1. HIPAA

عوامل نرم و عوامل سخت تقسیم‌بندی نموده و با رویکرد تحلیل سلسله مراتبی فازی به اولویت‌بندی آن‌ها پرداخته‌اند. در بین عوامل اصلی، عوامل نرم در رتبه اولویت اول و عوامل سخت در رتبه اولویت دوم قرار دارد. عوامل اصلی نرم به دو دسته عامل فرعی مدیریتی و فرهنگی و عوامل سخت به عوامل فرعی فنی و مالی تقسیم شدند. اولویت‌بندی عوامل فرعی نیز به ترتیب اهمیت عبارت است از: عوامل مدیریتی، فرهنگی، فنی و مالی (شاه‌بهرامی و همکاران، ۱۳۹۷). اولویت‌بندی ارائه شده توسط این محققان تنها بر اساس یک مورد مطالعاتی (سازمان تأمین اجتماعی گیلان) است و به همین دلیل از قابلیت تعمیم کافی برای کسب‌وکارهای مختلف برخوردار نیست. آفتابی نیز در پایان‌نامه خود به موضوع مدیریت امنیت اطلاعات پرداخته است. در این پژوهش تلاش شده تا یک مدل توصیفی و کمی به کمک شبیه‌سازی که هم‌زمان سطوح کلان و خرد را باهم در نظر می‌گیرد تشکیل‌شده و با توجه به نتایج حاصل، سیاست‌گذاری امنیتی جهت تخصیص منابع موردنیاز صورت گیرد. مدل متشکل از سه نوع عامل مهاجم درون سازمان، مهاجم برون‌سازمانی و سازمان موردنظر می‌باشد که یک مدل ترکیبی از مدل‌های عامل مبنا و پویاشناسی سیستم است. به‌منظور اتخاذ تصمیم در تخصیص سرمایه روی هریک از کنترل‌های امنیتی مقابله با تهدیدات داخل و خارج سازمان با بهره بردن از شبیه‌سازی مونتکارلو نتایج حاصل از سناریوهای مختلف به‌صورت میانگین موردبررسی قرار گرفته است (آفتابی ۱۳۹۷). رویکرد این پژوهش اگرچه رویکرد بدیعی است اما از قابلیت بررسی جزءبه‌جزء مسائل امنیتی موجود سازمان، شناسایی نقاط ضعف و پیشنهاد راه‌حل برای آن‌ها برخوردار نیست. جعفرنژاد و تقوا به بررسی و شناسایی عوامل مؤثر در پیاده‌سازی هم‌زمان آی‌تی‌آی‌ال (ITIL) و سیستم امنیت اطلاعات با رویکرد تداوم خدمات فناوری اطلاعات پرداخته‌اند. این محققان فرضیه خود مبنی بر تأثیر پیاده‌سازی آی‌تی‌آی‌آل و سیستم امنیت اطلاعات در تداوم خدمات فناوری اطلاعات را بر اساس اطلاعات به‌دست‌آمده از پرسشنامه‌های خود و به‌وسیله آزمون‌های آماری تأیید کرده و در گام دوم عوامل کلیدی و مؤثر در اجرا و پیاده‌سازی موفق سیستم تداوم خدمات فناوری اطلاعات و میزان تأثیر هر

یک مشخص کردند (جعفرنژاد و تقوا ۱۳۹۸). آزادبیگی در پایان‌نامه خود به بررسی راهکارهایی برای افزایش امنیت شبکه‌های رایانه‌ای سازمان‌ها بر اساس استاندارد ایزو ۲۷۰۰۱ پرداخته است. در این تحقیق تلاش شده آسیب‌پذیری‌ها و تهدیدات امنیتی شبکه‌ها در ابعاد مختلف فنی و اجرایی بر اساس کنترل‌های این استاندارد شناسایی و راهکارهایی عملیاتی جهت رفع آن‌ها پیشنهاد شود (آزادبیگی ۱۳۹۸). با توجه به اینکه تحقیق انجام‌شده همه ابعاد شبکه‌های رایانه‌ای را در می‌گیرد، در این زمینه همه عوامل را پوشش داده ولی مدیریت امنیت اطلاعات در هر سازمان مقوله‌ای فراتر از بررسی امنیت شبکه‌ها است. اخوان، امین موسوی و سرآبادانی در پژوهش خود، با استفاده از روش فراترکیب و مطالعه منابع مرتبط با امنیت اطلاعات، به شناسایی عوامل کلیدی موفقیت در پیاده‌سازی مدیریت امنیت اطلاعات پرداخته و این عوامل را بر اساس حوزه‌های تمرکز حاکمیت امنیت اطلاعات، طبقه‌بندی کرده‌اند (اخوان، امین موسوی و سرآبادانی ۱۴۰۲).

۳. روش پژوهش

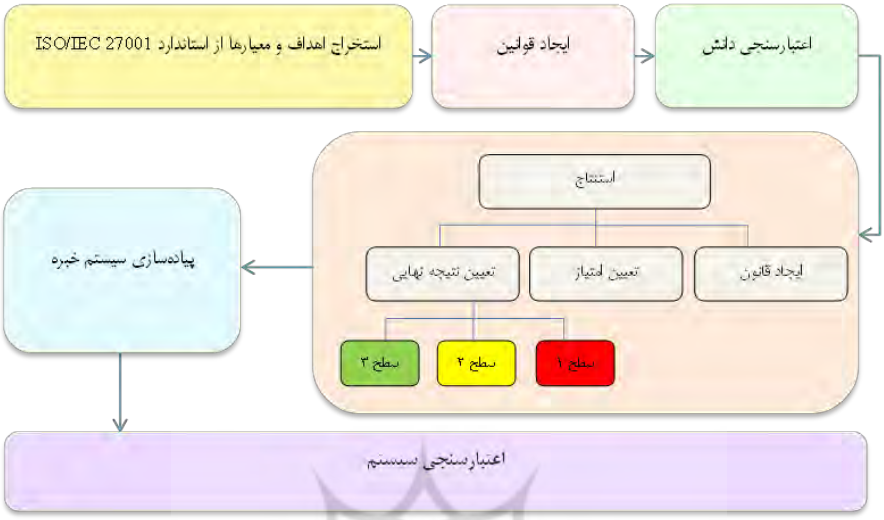
این پژوهش ازلحاظ هدف، کاربردی- توسعه‌ای است زیرا با بهره‌گیری از استاندارد بین-المللی ایزو ۲۷۰۰۱ و به‌منظور بهبود و به کمال رساندن استراتژی‌ها، رفتارها، روش‌ها، ابزارها، وسایل، ساختارها و الگوهای مورداستفاده سازمان‌ها، به طراحی سیستم خبره ممیزی پرداخته است. همچنین پژوهش ازنظر داده، توصیفی بوده و استراتژی آن طراحی است.

۳-۱. مراحل انجام پژوهش

توسعه سیستم‌های خبره در شش مرحله انجام داده می‌شود: ۱. کسب دانش، ۲. بازنمایی دانش؛ فرآیند سازمان‌دهی دانش کسب‌شده و مبنای ایجاد پایگاه دانش، ۳. اعتبارسنجی دانش؛ فرآیند تائید پایگاه دانش ایجادشده، ۴. استنتاج؛ به معنی طراحی الگوریتمی برای نتیجه‌گیری، ۵. پیاده‌سازی سیستم خبره و ۶. اعتبارسنجی (Sihwi, Andriyanto, Anggrainingsih 2016). ازاین‌رو ابتدا بر اساس اهداف پژوهش به بررسی ادبیات

موضوع پرداخته‌شده و پس‌ازآن اهداف کنترلی، معیارهای ارزیابی و توصیه‌های (کنترل‌های) استاندارد جهت طراحی سیستم خبره بر اساس استاندارد ایزو ۲۷۰۰۱ شناسایی شدند. بدین شکل اطلاعات لازم جهت ایجاد پایگاه دانش جمع‌آوری شدند. سپس با استفاده از این اطلاعات قواعد سیستم موردنظر تدوین شدند. بدین ترتیب به ازای هر توصیه (کنترل) در استاندارد یک قانون مستقل و درمجموع ۱۳۷ قانون ایجاد شد. پس از ساخت قوانین، رویکرد ایجاد قانون و قوانین ایجادشده از طریق مصاحبه حضوری به تائید ۳ نفر از خبرگان حوزه ممیزی امنیت اطلاعات رسید.

در مرحله بعدی اطلاعات لازم برای رتبه‌بندی و وزن دهی اهداف کنترلی و معیارهای ارزیابی اهداف، از طریق پرسشنامه نظرسنجی خبرگان گردآوری‌شده و با استفاده از تکنیک دیمتل و تکنیک واسپاس تحلیل شدند. به‌این‌ترتیب وزن اهداف کنترلی و معیارهای ارزیابی اهداف کنترلی به دست آمد. پس از مشخص کردن هدف اصلی امنیتی برای هر کنترل، اهداف مشخص‌شده طی مصاحبه حضوری با خبرگان بررسی و تائید شدند. در ادامه پژوهش با توجه به اطلاعات به‌دست‌آمده، سیستم خبره‌ای به‌منظور ارزیابی امنیت اطلاعات سازمان طراحی گردید. جهت پیاده‌سازی رابط کاربری در این سیستم خبره از زبان ویژوال بیسیک و جهت پیاده‌سازی الگوریتم استنتاج از نرم‌افزار اکسل ۲۰۱۶ استفاده شد. درنهایت به‌منظور بررسی عملکرد، سیستم طراحی‌شده در دو سازمان ایرانی با حوزه فعالیت توسعه نرم‌افزار اجراشده و نتیجه با نتایج ممیزی انسانی مقایسه شدند. لازم به ذکر است که یکی از سازمان‌های مذکور موفق به کسب گواهی ایزو ۲۷۰۰۱ شده و سازمان دیگر در کسب گواهی ناکام مانده بود. مراحل انجام پژوهش در شکل ۱ نشان داده شده است.



شکل ۱. مراحل اصلی پژوهش در طراحی سیستم خبره

۳-۲. جمع‌آوری داده‌ها

جامعه آماری تحقیق حاضر، افراد خبره در زمینه امنیت فناوری اطلاعات و ارزیابی ریسک فناوری اطلاعات در استان تهران و سازمان‌هایی که دارای تجربه ممیزی امنیت اطلاعات هستند، می‌باشد. نمونه آماری شامل دوازده نفر از خبرگان و ممیزان امنیت اطلاعات بوده و به دلیل محدود بودن جامعه آماری و کمبود خبرگان آشنا به موضوع، روش نمونه‌گیری از نوع نمونه‌گیری غیراحتمالی در دسترس است.

برای طراحی سیستم خبره در مرحله نخست به دلیل استفاده از استاندارد ایزو ۲۷۰۰۱ اطلاعات موجود ازجمله اهداف کنترلی و معیارهای ارزیابی اهداف به همراه توصیه‌های استاندارد ایزو ۲۷۰۰۱ از سایت www.iso.org گردآوری شد. در مرحله دوم جهت اعتبارسنجی قواعد ایجادشده ازنظر خبرگان با استفاده از مصاحبه بهره برده شد. در مرحله سوم برای گردآوری نظر خبرگان به‌منظور رتبه‌بندی و وزن‌دهی اهداف کنترلی و معیارهای ارزیابی، از ابزار پرسشنامه استفاده شد. در مرحله چهارم از کسب اطلاعات، پس از مشخص کردن هدف اصلی امنیت برای هر کنترل، اهداف مشخص‌شده طی مصاحبه

حضوری با خبرگان بررسی و تائید شدند. مشخصات روش‌ها و ابزارهای جمع‌آوری اطلاعات پژوهش در جدول ۱ و مشخصات خبرگان در جدول ۲ آورده شده است. به‌منظور سنجش روایی پرسشنامه جمع‌آوری اطلاعات برای تعیین وزن اهداف کنترلی و پرسشنامه تعیین وزن معیارهای ارزیابی اهداف کنترلی، ۳ نفر از خبرگان در حوزه ممیزی استاندارد ایزو ۲۷۰۰۱ پرسشنامه را موردبررسی قرار دادند. نتیجه بررسی خبرگان نشان داد هر دو پرسشنامه از اعتبار لازم برخوردار هستند. برای بررسی پایایی پرسشنامه تحقیق از روش آلفای کرونباخ بر اساس اطلاعات گردآوری‌شده از خبرگان پژوهش (۱۲ نفر) استفاده شد. نتایج به‌دست‌آمده نشان داد که آلفای کرونباخ برای پرسشنامه تحقیق در حالت کلی برابر با ۰,۹۳۰ است. این مقدار نشان‌دهنده‌ی آن است که پرسشنامه مورداستفاده، از قابلیت اعتماد و یا به‌عبارت‌دیگر از پایایی لازم برخوردار است.

جدول ۱. مشخصات روش‌ها و ابزار جمع‌آوری اطلاعات

ردیف	ابزار / روش	هدف	خروجی	اطلاعات منابع/ خبرگان
۱	منابع کتابخانه‌ای	شناسایی شیوه ارزیابی امنیت اطلاعات از مطالعات کتابخانه‌ای	اهداف کنترلی، معیارهای ارزیابی اهداف و توصیه (کنترل) ها	سایت iso.org
۲	مصاحبه حضوری	تائید رویکرد ایجاد قانون و ۱۳۷ قانون ایجادشده	تائید خبرگان	۳ نفر (ممیز استاندارد ایزو ۲۷۰۰۱)
۳	پرسشنامه اول	گردآوری اطلاعات جهت رتبه-بندی اهداف کنترلی	وزن اهداف کنترلی	۱۲ نفر (خبرگان حوزه امنیت اطلاعات)
۴	پرسشنامه دوم	گردآوری اطلاعات جهت وزن دهی معیارهای ارزیابی اهداف کنترلی	وزن معیارهای ارزیابی اهداف کنترلی	۱۲ نفر (خبرگان حوزه امنیت اطلاعات)
۵	مصاحبه حضوری	تعیین هدف اصلی امنیت برای هر توصیه (کنترل) استاندارد	مشخص شدن یک هدف اصلی امنیت برای هر توصیه	۳ نفر (خبرگان حوزه امنیت اطلاعات)

برای جمع‌آوری اطلاعات از دانش و تجربه ۱۲ نفر از خبرگان حوزه امنیت اطلاعات و ارزیابی ریسک استفاده شده است. مشخصات خبرگان در جدول ۲ آورده شده است.

جدول ۲. مشخصات مصاحبه‌شوندگان

ردیف	جنسیت	سمت	سابقه کاری	تحصیلات
۱	خانم	-مدیر تیم امنیت و تست نفوذ اپلیکیشن شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت -دارای تجربه ممیزی ISMS	بین ۱۰ تا ۱۵ سال	دکتری
۲	آقا	-سرپرست تیم امنیت و تست نفوذ اپلیکیشن شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت -دارای تجربه ممیزی ISMS	بین ۱۰ تا ۱۵ سال	کارشناسی
۳	خانم	کارشناس ارشد امنیت تیم عملیات شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۵ تا ۱۰ سال	کارشناس ارشد
۴	آقا	کارشناس ارشد امنیت تیم عملیات شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۵ تا ۱۰ سال	کارشناس ارشد
۵	آقا	کارشناس ارشد تیم امنیت و تست نفوذ اپلیکیشن شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۵ تا ۱۰ سال	کارشناسی
۶	آقا	کارشناس ارشد تیم امنیت و تست نفوذ اپلیکیشن شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۵ تا ۱۰ سال	کارشناسی
۷	خانم	-کارشناس ارشد امنیت تیم عملیات شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت - دارای تجربه ممیزی ISMS	بین ۵ تا ۱۰ سال	کارشناسی‌ارشد
۸	خانم	کارشناس امنیت تیم عملیات شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۳ تا ۵ سال	کارشناس ارشد
۹	خانم	کارشناس امنیت تیم عملیات شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۳ تا ۵ سال	کارشناسی
۱۰	خانم	کارشناس تیم امنیت و تست نفوذ اپلیکیشن شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۳ تا ۵ سال	کارشناسی
۱۱	آقا	کارشناس تیم امنیت و تست نفوذ اپلیکیشن شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۱ تا ۳ سال	کارشناسی
۱۲	آقا	کارشناس تیم امنیت و تست نفوذ اپلیکیشن شرکت ارائه‌کننده راهکارهای جامع بانکی و پرداخت	بین ۱ تا ۳ سال	کارشناسی

در این بخش به بیان تفصیلی مراحل توسعه سیستم خبره ارزیابی امنیت اطلاعات در این پژوهش پرداخته می‌شود.

٤-١. استخراج اهداف و معیارها

در نخستین گام از توسعه سیستم، پس از مطالعه منابع کتابخانه‌ای و نسخه اصلی استاندارد ایزو ۲۷۰۰۱ نسخه ۲۰۱۳ ارائه شده در سایت www.iso.org، ۱۴ هدف کنترلی، ۳۸ معیار ارزیابی اهداف، همراه با ۱۳۷ توصیه (کنترل) استخراج شدند. در جدول ۳ اهداف کنترلی مطابق استاندارد و در جدول ۴ معیارهای ارزیابی اهداف نشان داده شده‌اند.

جدول ۳. اهداف کنترلی استاندارد

ردیف	کد	هدف کنترلی استاندارد	ردیف	کد	هدف کنترلی استاندارد
۱	A1	خط‌مشی امنیت اطلاعات	۸	A8	امنیت عملیات
۲	A2	ساختار امنیت اطلاعات	۹	A9	امنیت ارتباطات
۳	A3	امنیت منابع انسانی	۱۰	A10	نگهداری سیستم
۴	A4	مدیریت دارایی‌ها	۱۱	A11	روابط تأمین‌کنندگان
۵	A5	کنترل دسترسی	۱۲	A12	مدیریت رخدادها
۶	A6	رمزگذاری	۱۳	A13	مدیریت تداوم
۷	A7	امنیت فیزیکی و محیطی	۱۴	A14	انطباق

جدول ٤. معیارهای ارزیابی اهداف کنترلی استاندارد

ردیف	کد	معیار ارزیابی اهداف کنترلی	ردیف	کد	معیار ارزیابی اهداف کنترلی
۱	B1	خط‌مشی‌هایی برای امنیت اطلاعات	۲۰	B20	رویه‌های عملیاتی و مسئولیت‌ها
۲	B2	نقش‌ها و مسئولیت‌های امنیت اطلاعات	۲۱	B21	حفاظت در برابر بدافزارها
۳	B3	ارتباط با مقامات	۲۲	B22	پشتیبان گیری
۴	B4	تماس با گروه‌های خاص	۲۳	B23	واقعه‌نگاری و پایش
۵	B5	امنیت اطلاعات در مدیریت پروژه‌ها	۲۴	B24	کنترل نرم‌افزارهای عملیاتی
۶	B6	استفاده از تلفن همراه	۲۵	B25	مدیریت آسیب‌پذیری فنی
۷	B7	دورکاری	۲۶	B26	ملاحظات ممیزی سیستم‌های اطلاعاتی
۸	B8	گزینش	۲۷	B27	کنترل شبکه
۹	B9	در حین خدمت	۲۸	B28	انتقال اطلاعات

ردیف	کد	معیار ارزیابی اهداف کنترلی	ردیف	کد	معیار ارزیابی اهداف کنترلی
۱۰	B10	خاتمه اشتغال	۲۹	B29	الزامات امنیتی سیستم‌های اطلاعاتی
۱۱	B11	مسئولیت دارایی‌ها	۳۰	B30	امنیت در فرآیندهای توسعه و پشتیبانی
۱۲	B12	طبقه‌بندی اطلاعاتی	۳۱	B31	داده‌های آزمون
۱۳	B13	مدیریت رسانه	۳۲	B32	امنیت اطلاعات در روابط با تأمین‌کنندگان
۱۴	B14	نیازمندی‌های تجاری کنترل دسترسی	۳۳	B33	مدیریت تحویل خدمات تأمین‌کنندگان
۱۵	B15	مدیریت دسترسی کاربران	۳۴	B34	مدیریت و بهبود رخدادهای امنیت اطلاعات
۱۶	B16	مدیریت دسترسی به سیستم و برنامه‌ها	۳۵	B35	تداوم امنیت اطلاعات
۱۷	B17	سیاست در استفاده از کنترل رمزنگاری	۳۶	B36	افزونگی
۱۸	B18	نواحی امن	۳۷	B37	انطباق با الزامات قانونی و قراردادی
۱۹	B19	تجهیزات	۳۸	B38	بازنگری‌های امنیت اطلاعات

٤-۲. ایجاد قوانین سیستم

در مرحله بعدی دانش گردآوری‌شده بازنمایی شده و قوانین سیستم به‌صورت اگر-آنگاه ایجاد شدند. به‌عنوان‌مثال در بخش اهداف کنترلی استاندارد، هدف امنیت منابع انسانی با معیار ارزیابی گزینش، دارای کنترلی به این صورت می‌باشد: «آیا بررسی سابقه برای تمامی گزینه‌های استخدام انجام می‌شود؟»

پاسخ به این سؤال به‌صورت بله/خیر است و با توجه به رویکرد کمی انتخاب‌شده برای پژوهش موردنظر پاسخ بله امتیاز ۱ و پاسخ خیر امتیاز ۰ می‌گیرد. بدین ترتیب قانون ایجادشده برای کنترل به‌صورت زیر به دست می‌آید:

If Employee Background Checked Then point=1 Else point=0

بدین ترتیب به ازای هر کنترل در چک‌لیست استاندارد، یک قانون مستقل و درمجموع ۱۳۷ قانون ایجاد شد. قوانین ایجادشده از طریق مصاحبه حضوری به تائید سه تن از خبرگان حوزه ممیزی امنیت اطلاعات رسید.

در مرحله بعدی، برای تعیین وزن لایه اهداف کنترلی و معیارهای ارزیابی دو پرسشنامه تدوین و در اختیار خبرگان حوزه امنیت اطلاعات قرار گرفت. پس از توزیع پرسشنامه در میان خبرگان حوزه امنیت اطلاعات، نظر دوازده تن از خبرگان گردآوری

شد. سپس به‌منظور تحلیل اطلاعات برای وزن دهی لایه اهداف کنترلی، از تکنیک دیمتل به همراه فرمول دالالا و برای وزن دهی لایه معیارهای ارزیابی از تکنیک واسپاس استفاده شد. در ادامه به‌صورت گام‌به‌گام استخراج وزن دو لایه شرح داده شده است.

٤-٣. محاسبه وزن لایه‌ها

١-٣-٤. محاسبه وزن اهداف کنترلی استاندارد

به‌منظور اولویت‌بندی اهداف کنترلی استاندارد ایزو ۲۷۰۰۱ از تکنیک دیمتل استفاده شد. این تکنیک یک روش ارزیابی تصمیم است که در سال ۱۹۷۱ توسط Fonteal و Gabus برای حل مسائل پیچیده تصمیم‌گیری توسعه داده شده است. این روش به‌منظور کشف رابطه علت و معلولی میان معیارها و شناسایی عوامل تأثیرگذار که بیشترین تأثیر را در روند تصمیم‌گیری دارد دنبال می‌شود. (Deepak et al., 2018).

این تکنیک شامل مراحل زیر می‌باشد:

۱. ساخت ماتریس ارتباط مستقیم بر اساس نظرات خبرگان
۲. نرمال کردن ماتریس ارتباط مستقیم
۳. محاسبه ماتریس ارتباطات کامل معیارها
۴. تشکیل نگاشت روابط شبکه

با توجه به میانگین نظرات ۱۲ خبره، نتیجه نهایی در جدول ۵ نشان داده شده است.

به‌منظور تعیین نگاشت روابط شبکه از دو بردار R و J استفاده می‌شود که به ترتیب مجموع ردیف‌ها و ستون‌های ماتریس T می‌باشد که از روابط زیر محاسبه می‌شوند:

$$R = [R_i]n*1 = \left[\sum_{j=1}^{n} t_{ij}\right]_{n*1}$$

$$J = [J_j]n*1 = \left[\sum_{i=1}^{n} t_{ij}\right]_{1*n}$$

R_i به معنی مجموع i مین ردیف ماتریس T و نشان‌دهنده مجموع تأثیرات مستقیم و غیرمستقیم معیار I بر دیگر معیارهاست. Jj به معنی j امین ستون ماتریس T و نشان‌دهنده مجموع تأثیرات مستقیم و غیرمستقیم است که دیگر معیارها بر معیار j می‌گذارند.

شاخص $R_i + J_j$ بیانگر میزان اهمیت (شدت) معیار i ام می‌باشد. شاخص $R_i - J_j$ نشان‌دهنده تأثیرگذاری و یا تأثیرپذیری معیار i می‌باشد. در حالت کلی، چنانچه $R_i - J_j$ مثبت باشد (i=j)، معیار i ام جز دسته معیارهای علی یا تأثیرگذار است. چنانچه $R_i - J_j$ منفی باشد (i=j)، معیار i ام جزء گروه معیارهای تأثیرپذیر است. به همین صورت میزان شاخص R و J را محاسبه می‌نماییم. نمودار سببی بر پایه دو شاخص مذکور قابل ترسیم بوده که به نقشه روابط شبکه معروف است. با توجه به این نقشه می‌توان تصمیم گرفت که چگونه ابعاد و معیارها را می‌توان بهبود داد (Jeepak et al., 2018).

جدول ۵. ماتریس نتیجه تکنیک دیمتل

تأثیرگذار/پذیر	R-J	R+J	J	R	نتیجه
تأثیرگذار	1.8354	1.8354	0	1.8354	خط‌مشی امنیت اطلاعات
تأثیرگذار	0.27	1.8472	0.7886	1.0586	ساختار امنیت اطلاعات
تأثیرگذار	0.1179	1.9912	0.9366	1.0545	امنیت منابع انسانی
تأثیرگذار	0.1619	1.9399	0.889	1.0509	مدیریت دارایی‌ها
تأثیرگذار	0.2307	1.6102	0.6897	0.9205	کنترل دسترسی
تأثیرگذار	0.2755	1.4989	0.6117	0.8872	رمزگذاری
تأثیرپذیر	-0.1656	1.8818	1.0237	0.8581	امنیت فیزیکی و محیطی
تأثیرپذیر	-0.2461	1.9355	1.0908	0.8447	امنیت عملیات
تأثیرپذیر	-0.4397	2.1174	1.2785	0.8388	امنیت ارتباطات
تأثیرپذیر	-0.4466	2.0451	1.2459	0.7993	نگهداری سیستم
تأثیرپذیر	-0.2191	1.5352	0.8771	0.6581	روابط تأمین‌کنندگان
تأثیرپذیر	-0.349	1.6189	0.9839	0.635	مدیریت رخدادها
تأثیرپذیر	-0.6505	1.914	1.2822	0.6317	مدیریت تداوم
تأثیرپذیر	-0.3748	1.6211	0.9979	0.6231	انطباق

سپس وزن اهداف کنترلی با استفاده از تکنیک دیمتل به همراه فرمول دالالا محاسبه‌شده و با روش خطی نرمال شده‌اند. نتایج در جدول ۶ نشان داده شده است. تکنیک دیمتل یک

روش ارزیابی تصمیم است که در سال ۱۹۷۱ توسط «فونتیل»[1] و «گابوس»[2] برای حل مسائل پیچیده تصمیم‌گیری توسعه داده شده است. این روش به‌منظور کشف رابطه علت و معلولی میان معیارها و شناسایی عوامل تأثیرگذار که بیشترین تـأثیر را در رونـد تصـمیم‌گیـری دارد دنبال می‌شود (Singhal et al., 2018).

پس از تعیین رتبه‌بندی اهداف با روش DEMATEL با فرمـول DALALA وزن هـر معیار به‌صورت محلی طبق فرمول زیر محاسبه می‌شود و برای محاسـبه وزن نهـایی از روش خطی برای نرمال کردن وزن‌ها به شکلی که جمع اوزان برابر یـک باشـد اسـتفاده مـی‌شـود (Sfaei & Homayounzadeh, 2017):

$$W_i = \sqrt{(D_i + R_i)^2 + (D_i + R_i)^2}$$

$$W_f = \frac{w_i}{\sum_{i=1}^{n} w_i}$$

جدول ٦. محاسبه وزن معیارها با فرمول دالالا

(R-J)^2	(R+J)^2	Weight	Normal Weight	نتیجه
3.368693	3.368693	2.59564757	0.09779134	خط‌مشی‌های امنیت اطلاعات
0.0729	3.412148	1.86682828	0.07033299	مدیریت دارایی‌ها
0.0139	3.964877	1.99468741	0.07515010	ساختار امنیت اطلاعات
0.026212	3.763212	1.94664419	0.07334006	کنترل دسترسی
0.053222	2.592744	1.62664272	0.06128397	رمزگذاری
0.0759	2.246701	1.52400835	0.05741720	امنیت منابع انسانی
0.027423	3.541171	1.88907242	0.07117104	انطباق
0.060565	3.74616	1.95108315	0.07350730	امنیت فیزیکی و محیطی
0.193336	4.483383	2.16257228	0.08147518	امنیت ارتباطات
0.199452	4.182434	2.09329539	0.07886516	امنیت عملیات
0.048005	2.356839	1.55075590	0.05842492	مدیریت تداوم امنیت اطلاعات
0.121801	2.620837	1.65609124	0.06239344	روابط تأمین کنندگان

1. Fonteal
2. Gabus

(R-J)^2	(R+J)^2	Weight	Normal Weight	نتیجه
0.42315	3.663396	2.02152078	0.07616105	اکتساب، توسعه و نگهداری از سیستم
0.140475	2.627965	1.66386305	0.06268625	مدیریت رخدادهای امنیت اطلاعات
			1.00	

۲-۳-٤. محاسبه وزن لایه معیارهای ارزیابی اهداف کنترلی

در استاندارد ISO/IEC 27001 ۱۴ هدف کنترلی همراه با ۳۸ معیار برای ارزیابی اهداف کنترلی و ۱۳۷ توصیه (کنترل) وجود دارد، میزان اهمیت این اهداف و معیارها در مقایسه با هم یکسان در نظر گرفته‌شده درصورتی‌که طبق مصاحبه با خبرگان اهمیت این اهداف و معیارها یکسان نبوده و برخی از تأثیر بالاتری در برقراری امنیت نسبت به بقیه برخوردار هستند و در صورت عدم اجرای صحیح، امنیت سازمان را با مخاطرات جدی‌تری روبرو می‌کنند.

همچنین با توجه به اینکه ضرایب با توجه به ماهیت هر سازمان می‌تواند متفاوت باشد تا حد ممکن از خبرگان و مصاحبه‌شوندگان خواسته‌شده تا این مورد را لحاظ کنند تا از پژوهش بتوان در زمینه‌های بیشتری به‌صورت عملی بهره برد.

برای اولویت‌بندی معیارهای ارزیابی اهداف کنترلی استاندارد ایزو ۲۷۰۰۱ از روش واسپاس استفاده شده است. تکنیک واسپاس (ارزیابی محصول جمع شده با وزن) یکی از روش‌های تصمیم‌گیری چندشاخصه است که در سال ۲۰۱۲ توسط آقای Zavadskas و همکاران در پژوهشی معرفی شد. این روش ترکیبی از دو روش مدل مجموع وزنی و مدل محصول وزنی می‌باشد و نسبت به مدل‌های مستقل از دقت بالاتری برخوردار است (Zavadskas et al., 2012).

با توجه به نظرات گردآوری‌شده در مرحله نخست ماتریس تصمیم تشکیل داده شده، پس‌ازآن در گام دوم با توجه به اینکه تمام معیارها دارای نقش مثبت در تصمیم‌گیری هستند، ماتریس نرمال محاسبه‌شده است. در ادامه نتیجه نهایی با محاسبه اهمیت نسبی هر گزینه طبق روش میانگین جمعی موزون و میانگین ضربی موزون، محاسبه لاندا بهینه و محاسبه معیار مشترک برای هر گزینه انجام شده است و نتیجه در جدول ۷ نشان داده شده

است، علاوه بر محاسبه نتیجه به‌منظور تسهیل در محاسبه امتیاز امنیت اطلاعات، ضرایب معیارهای ارزیابی محاسبه‌شده با روش خطی و فرمول زیر نرمال شده‌اند:

$$\text{Normal Score} = \frac{Score_i}{\sum Score_i}$$

جدول ۷. ماتریس نتیجه تکنیک واسپاس

نتیجه	WSM	WPM	Q1	Q2	Landa	Score	Normal Score
B1	12	1	0.03	0.03	0.5	6.50000000	0.076923077
B2	11	0.316406	0.025625	0.003003	0.104909	1.43721585	0.072994603
B3	3.75	4.77E-07	0.003281	6.82E-15	2.08E-12	0.00000048	1.44724E-12
B4	3.75	4.77E-07	0.003281	6.82E-15	2.08E-12	0.00000048	1.44724E-12
B5	7.75	0.002781	0.013594	2.32E-07	1.71E-05	0.00291313	1.1898E-05
B6	3.75	4.77E-07	0.003281	6.82E-15	2.08E-12	0.00000048	1.44724E-12
B7	3.5	2.38E-07	0.002813	1.71E-15	6.06E-13	0.00000024	4.21649E-13
B8	7.25	0.000927	0.012344	2.58E-08	2.09E-06	0.00094211	0.002218425
B9	4.75	7.63E-06	0.005156	1.75E-12	3.39E-10	0.00000763	3.59831E-07
B10	4.5	3.81E-06	0.004688	4.37E-13	9.31E-11	0.00000382	9.88207E-08
B11	10.75	0.237305	0.024531	0.001689	0.06443	0.91464110	0.070442931
B12	10.5	0.177979	0.023438	0.00095	0.038966	0.58018468	0.042602503
B13	4	9.54E-07	0.00375	2.73E-14	7.28E-12	0.00000095	7.95941E-12
B14	7	0.000618	0.011563	1.15E-08	9.91E-07	0.00062492	0.001585803
B15	10.25	0.133484	0.022344	0.000535	0.023364	0.36985064	37.38718556
B16	10	0.100113	0.02125	0.000301	0.013952	0.23823743	22.32605774
B17	9.75	0.075085	0.020156	0.000169	0.008321	0.15559147	0.053479796
B18	4.5	3.81E-06	0.004688	4.37E-13	9.31E-11	0.00000382	2.43717E-05
B19	6.75	0.000412	0.010781	5.09E-09	4.72E-07	0.00041518	0.123560209
B20	9.5	0.050056	0.019375	7.52E-05	0.003865	0.08657785	0.044641903
B21	9.75	0.075085	0.020156	0.000169	0.008321	0.15559147	0.096110033
B22	6	0.000137	0.008125	5.66E-10	6.96E-08	0.00013775	8.03901E-07
B23	6.5	0.000412	0.009375	5.09E-09	5.43E-07	0.00041552	6.27181E-06
B24	6.25	0.000206	0.008906	1.27E-09	1.43E-07	0.00020689	1.65169E-06
B25	3.5	2.38E-07	0.002813	1.71E-15	6.06E-13	0.00000024	6.99948E-12
B26	9	0.025028	0.0175	1.88E-05	0.001073	0.03465566	0.01239347
B27	4	9.54E-07	0.00375	2.73E-14	7.28E-12	0.00000095	7.66316E-06
B28	5.75	6.1E-05	0.007969	1.12E-10	1.4E-08	0.00006112	0.014736842
B29	11.25	0.421875	0.026719	0.005339	0.166552	2.22532557	0.07484388
B30	4	9.54E-07	0.00375	2.73E-14	7.28E-12	0.00000095	3.27143E-12
B31	3	5.96E-08	0.001875	1.07E-16	5.68E-14	0.00000006	2.55244E-14
B32	5.5	6.1E-05	0.006563	1.12E-10	1.7E-08	0.00006113	0.000278096
B33	3.25	1.19E-07	0.002344	4.26E-16	1.82E-13	0.00000012	2.97726E-09
B34	5.25	3.05E-05	0.006094	2.79E-11	4.58E-09	0.00003054	0.000149967

نتیجه	WSM	WPM	Q1	Q2	Landa	Score	Normal Score
B35	5	1.53E-05	0.005625	6.98E-12	1.24E-09	0.00001526	8.12582E-05
B36	3.5	2.38E-07	0.002813	1.71E-15	6.06E-13	0.00000024	3.97117E-08
B37	8.5	0.012514	0.015625	4.7E-06	0.000301	0.01506535	0.019979622
B38	8	0.003708	0.014688	4.12E-07	2.81E-05	0.00393243	0.001865207
							14

بدین ترتیب وزن لایه‌های اهداف کنترلی و معیارهای ارزیابی محاسبه و نرمال‌سازی شده‌اند.

٤-٤. تعیین اهداف اصلی امنیتی برای هر توصیه (کنترل) استاندارد

در گام بعدی به‌منظور تعیین هدف اصلی امنیت مربوط به توصیه (کنترل) های استاندارد، پنج هدف اصلی مندرج در جدول ۸ که در ادبیات پژوهش بیشتر مورد تأکید و تکرار بودند، انتخاب شدند.

جدول ۸. اهداف امنیتی

ردیف	هدف امنیتی	پژوهشگر	تعریف
۱	در دسترس بودن	Stonirner (2001), Hout (2007), Whitman (2011), Cimpa (2013), Chang & Lee (2013), Alghananeem & Altaee (2014), Binner (2018),Khafidh and Ruki (2024), Tarek et al. (2024)	اطمینان از این‌که اطلاعات به‌طور صحیح و در زمان موردنیاز، در دسترس افرادی که مجاز هستند قرار گیرد.
۲	صحت	Stonirner (2001), ISO/IEC 27001(2005), Chang & Lee (2013)	از دو منظر موردبررسی قرار می‌گیرد: صحت داده و صحت سیستم. صحت داده به معنی این است که داده‌ها در حین ذخیره، انتقال و پردازش به‌طور غیرمجاز تغییر داده نشوند و صحت سیستم به معنی عدم دست‌کاری در حین انجام‌وظیفه هست.
۳	محرمانگی	Stonirner (2001), Conklin (2004), Hout (2007), Whitman(2011),	به معنی حفاظت اطلاعات در مقابل دسترسی‌های غیرمجاز

ردیف	هدف امنیتی	پژوهشگر	تعریف
		Al-Tai (2012), Cimpa (2013), Chang & Lee (2013), Alghananeem & Altaee (2014), Binner (2018), Khafidh and Ruki(2024), Tarek et al. (2024)	است.
۴	مسئولیت‌پذیری/ عدم انکار	Griffin (1993), Stonirner(2001), F.Tipton & Krause (2005), Al-Qahtani & Alghathbar (2009), Alghananeem & Altaee(2014), مدیری و همکاران (۱۳۸۷)	نیازی است که اعمال یک موجودی (سازمان یا سیستم) به‌طور انحصاری فقط توسط همان موجودی دنبال شود.
۵	قابلیت ممیزی	Conklin (2004), F.Tipton & Krause(2005), Alghananeem & Altaee(2014), Binner(2018)	قابلیت ره‌گیری هر نوع عملیات برای هر عامل استفاده‌کننده در هر سطحی است.

در این مرحله با توجه به تعریف ارائه شده برای اهداف اصلی، هدف اصلی امنیت برای هر توصیه (کنترل) مشخص‌شده و طی مصاحبه حضوری به تائید خبرگان رسیده است.

٤-٥. تعیین امتیاز

نتیجه نهایی سیستم بیان‌کننده وضعیت امنیت اطلاعات سازمان است. سیستم طراحی‌شده شامل سه خروجی است که در ادامه هر سه مورد، شرح داده شده است.

الف. محاسبه امتیاز امنیت اطلاعات سازمان بر مبنای استاندارد ایزو ۲۷۰۰۱:

امتیاز امنیت سازمان از مجموع امتیازات قوانین منطبق بر رابطه ۱، به دست می‌آید.

رابطه ۱ $\text{Ponit} = \sum_{i=1}^{n} X_i$

Point: امتیاز امنیت سازمان بر اساس استاندارد

X_i: امتیاز هر سؤال از چک‌لیست که با استفاده از قوانین محاسبه می‌شود.

امتیاز امنیت به سه دسته طبقه‌بندی می‌شوند. امتیاز نمره از ۰ تا ۴۵ به‌عنوان امتیاز کم، از ۴۶ تا ۹۰ امتیاز متوسط و از ۹۱ ب تا ۱۳۷ امتیاز بالا محسوب می‌شود.

ب: محاسبه میزان تحقق اهداف اصلی امنیت در سازمان:

درصد تحقق هر یک از اهداف امنیت اطلاعات نیز بر اساس رابطه ۲ محاسبه می‌شود:

رابطه ۲ $\text{GoalRealization} = \frac{\sum G_i}{N}$

G_i: امتیاز هر سؤال بر اساس قرارگیری در گروه یک هدف اصلی مشخص.

N: مجموع امتیاز هر هدف اصلی در کل چک‌لیست

ج. محاسبه امتیاز امنیت اطلاعات سازمان بر مبنای استاندارد ایزو ۲۷۰۰۱ و با احتساب ضرایب وزن اهداف کنترلی و معیارهای ارزیابی:

امتیاز امنیت اطلاعات سازمان با احتساب ضرایب وزن اهداف کنترلی و وزن معیارهای ارزیابی از رابطه ۳ به دست می‌آید:

رابطه ۳ $\text{Ponit} = \sum(\text{The Average Score For Each Criterion}) * \text{CW} * \text{GW}$

Point: امتیاز امنیت سازمان بر اساس استاندارد با احتساب ضرایب

The Avrage Score for Each Criteria: میانگین امتیاز هر معیار

CW: وزن هر معیار ارزیابی

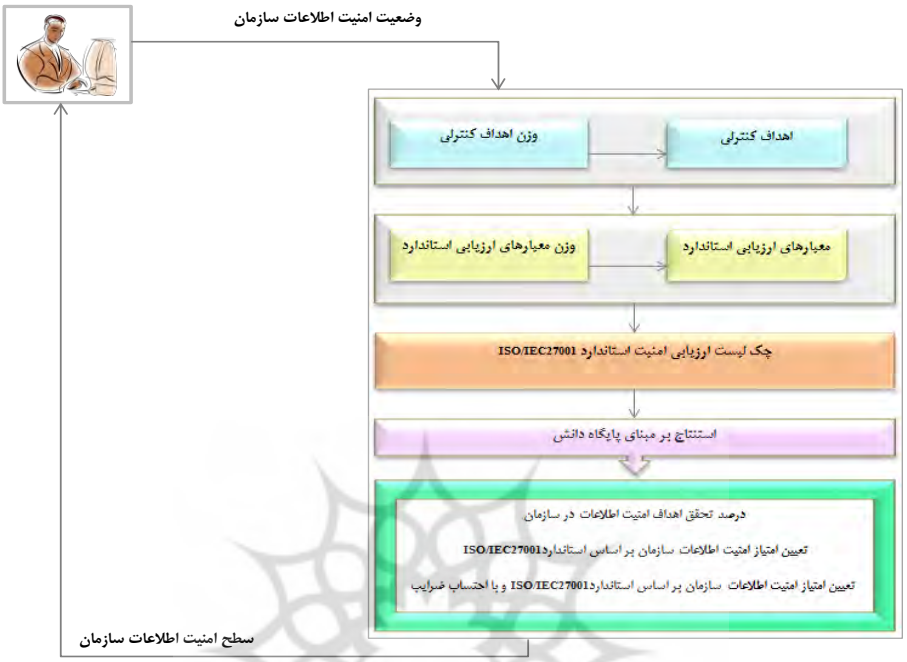
GW: وزن هدف کنترلی

این امتیاز مقداری بین صفر تا یک دارد. امتیاز بین ۰ تا ۰,۳۳ به‌عنوان امتیاز کم، امتیاز بین ۰,۳۴ تا ۰,۶۶: به معنی امتیاز متوسط و امتیاز بین ۰,۶۷ تا ۱: به معنی امتیاز بالا محسوب می‌شود.

۵. پیاده‌سازی سیستم خبره

در این مرحله با استفاده از اطلاعات گردآوری‌شده در مراحل قبلی سیستم خبره‌ی ارزیابی امنیت اطلاعات طراحی و پیاده‌سازی شده است. جهت پیاده‌سازی رابط کاری از زبان ویژوال‌بیسیک و جهت پیاده‌سازی الگوریتم استنتاج از نرم‌افزار اکسل ۲۰۱۶ استفاده شد. رابط کاربری سیستم به‌طور کاملاً منطبق با استاندارد ایزو ۲۷۰۰۱ طراحی شد. طی تعامل با کاربر وضعیت امنیت اطلاعات سازمان به‌دست‌آمده و در فایل اکسل ذخیره می‌شود. پس از اتمام پاسخگویی، استنتاج بر مبنای قواعد طراحی‌شده با ساختار اگر-آنگاه آغاز می‌شود. ساختار سیستم به‌صورت چندلایه‌ای طراحی شده است که معماری آن در شکل ۲ نشان داده شده است.

شکل ۲. معماری سیستم خبره



در لایه رابط کاربری به ازای هر هدف کنترلی یک فرم طراحی‌شده که سؤالات هر فرم با توجه به معیارهای ارزیابی دسته‌بندی‌شده و به ازای هر کنترل یک سؤال منظور شده است و اطلاعات موردنیاز در زمینه وضعیت فعلی امنیت اطلاعات سازمان در قالب تعامل با کاربر دریافت می‌شود. این اطلاعات در فایل اکسل ذخیره می‌شود.

همان‌طور که در معماری سیستم (شکل ۲) نشان داده شده است، دو لایه وزن دهی در طراحی سیستم قرار دارد. لایه اول مربوط به وزن دهی اهداف کنترلی استاندارد ایزو ۲۷۰۰۱ بوده (شامل ۱۴ هدف) و لایه دوم به وزن دهی معیارهای سنجش این اهداف (شامل ۳۸ معیار) می‌پردازد. لایه سوم لایه کنترل‌های امنیتی است که امتیازهای مربوط به آن با لحاظ کردن وزن دو لایه به دست می‌آید. در لایه استنتاج، سیستم طبق قوانین نوشته‌شده با رویکرد زنجیره پیشرو استنتاج می‌کند. در این پژوهش به ازای تمام توصیه‌های استاندارد، قانون تدوین‌شده و توسط خبره تائید شده است.

در لایه خروجی علاوه بر امتیاز امنیت اطلاعات سازمان منطبق با استاندارد، امتیاز امنیت اطلاعات سازمان با در نظر گرفتن وزن اهداف کنترلی استاندارد و وزن معیارهای ارزیابی استاندارد محاسبه‌شده و نتیجه در سه سطح به کاربر نشان داده می‌شود. سطح نخست که با رنگ قرمز مشخص می‌شود به معنی وضعیت بحرانی برای امنیت اطلاعات سازمان محسوب شده، سطح دوم که به رنگ زرد است وضعیت متوسطی برای امنیت اطلاعات سازمان محسوب می‌شود و رنگ سبز به معنی سطح بالای امنیتی در سازمان تلقی می‌شود. همچنین امتیاز سازمان در میزان تحقق هریک از اهداف اصلی امنیت شامل، صحت، محرمانگی، در دسترس بودن، مسئولیت‌پذیری و قابلیت ممیزی نیز محاسبه‌شده و به کاربر نشان داده می‌شود.

۵-۱. اعتبارسنجی سیستم

در این بخش به‌منظور اعتبارسنجی سیستم طراحی‌شده و بررسی صحت عملکرد آن، آزمایش سیستم در دو سازمان ایرانی واقع در تهران، با سطوح مختلف، اجرا شده است. اختلاف سطح دو سازمان در تعداد کارکنان، دامنه خدمات و اجرای استاندارد ایزو ۲۷۰۰۱ است.

- سازمان اول، با کد A با محدوده خدمات بین‌المللی، با تعداد کارمندان حدود ۵۰۰ الی ۱۰۰۰ کارمند، یک سازمان بزرگ است و استاندارد ایزو ISO/IEC 27001 را اجرا کرده است و در زمینه ارائه راهکارهای نوین بانکی فعالیت می‌کند.
- دومین سازمان با کد B، یک سازمان بزرگ طبقه‌بندی نمی‌شود. نه بیش‌ازحد بزرگ و نه بیش‌ازحد کوچک است. کارکنان آن بین ۵۰ تا ۱۰۰ نفر بوده و خدمات آن به‌صورت محلی است و همین‌طور سیستم مدیریت امنیت اطلاعات را کاملاً منطبق با استاندارد ایزو ISO/IEC 27001 اجرا نکرده است. این سازمان در زمینه مشاوره راهکارهای پرداخت به‌صورت همکار با شرکت A فعالیت می‌کند.

اعداد حاصل در جدول ۹ برای شرکت A و B اعدادی هستند که توسط سیستم خبره طراحی‌شده محاسبه‌شده و این امتیازات با اعمال ضرایب نیز در این جداول نشان داده شده

است. در ردیف‌های انتهایی جدول پس از جمع امتیازات محاسبه‌شده توسط سیستم خبره، امتیاز محاسبه‌شده توسط خبره انسانی نیز ذکر شده است تا بتوان اختلاف مجموع امتیازات را راحت‌تر مشاهده نمود. امتیازات محاسبه‌شده توسط سیستم بر اساس میانگین اطلاعات واردشده توسط ۳ نفر از متخصصان امنیت اطلاعات در سازمان که تجربه ممیزی ایزو ۲۷۰۰۱ را داشته‌اند انجام گرفته است و محاسبه نتیجه توسط سیستم خبره محاسبه‌شده است. همچنین، امتیاز محاسبه‌شده توسط خبره انسانی، آخرین نتیجه ممیزی توسط ممیز رسمی ISMS می‌باشد که به جهت کمک به پیشبرد اهداف پژوهش در اختیار پژوهشگر قرار گرفته است.

همان‌طور که در جدول ۹ مشاهده می‌شود از ارزیابی ۱۳۷ موردی که در شرکت A انجام‌گرفته، در بیش از ۱۰۰ مورد آن نتیجه ارزیابی سیستم خبره با خبره انسانی مطابقت دارد. میزان دقت سیستم خبره طراحی‌شده در ارزیابی شرکت A برابر با ۹۴٪ می‌باشد. از ارزیابی ۱۳۷ موردی که در شرکت B انجام‌گرفته، در بیش از ۱۰۰ مورد آن نتیجه ارزیابی سیستم خبره با خبره انسانی مطابقت دارد. میزان دقت سیستم خبره طراحی‌شده در ارزیابی شرکت B برابر با ۹۷٪ می‌باشد.

جدول ۹. مقایسه نتیجه خبره انسانی و سیستم خبره

هدف کنترلی	سازمان A		سازمان B	
	امتیاز استاندارد	امتیاز با اعمال ضرایب	امتیاز استاندارد	امتیاز با اعمال ضرایب
خط‌مشی امنیت اطلاعات	۵	۰,۰۹۷۸	۳	۰,۰۵۸۷
ساختار امنیت اطلاعات	۶	۰,۰۷۵۲	۸	۰,۰۷۵۲
امنیت منابع انسانی	۱۱	۰,۰۵۷۳	۶	۰,۰۵۶۸
مدیریت دارایی‌ها	۱۰	۰,۰۶۴۹	۱۲	۰,۰۴۸۵
کنترل دسترسی	۱۵	۰,۰۶۸۶	۱۱	۰,۰۴۶۳
رمزگذاری	۲	۰,۰۶۱۲	۰	۰
امنیت فیزیکی و محیطی	۱۲	۰,۰۷۳۵	۱۰	۰,۰۴۹۲
امنیت عملیات	۱۹	۰,۰۷۸۹	۷	۰,۰۶۲۷

هدف کنترلی	سازمان A		سازمان B	
	امتیاز استاندارد	امتیاز با اعمال ضرایب	امتیاز استاندارد	امتیاز با اعمال ضرایب
امنیت ارتباطات	۷	۰,۰۸۱۵	۰	۰
نگهداری سیستم	۸	۰,۰۵۰۸	۳	۰,۰۲۵۴
روابط تأمین‌کنندگان	۴	۰,۰۴۱۶	۰	۰
مدیریت رخدادها	۶	۰,۰۶۲۷	۰	۰
مدیریت تداوم	۴	۰,۰۵۸۴	۰	۰
انطباق	۷	۰,۰۷۱۲	۳	۰,۰۴۲۳
نتیجه سیستم خبره	۱۱۶	۰,۹۴۳۶	۶۳	۰,۴۶۵
نتیجه خبره انسانی	۱۰۹	_	۶۰	-
اختلاف	۷	_	۳	_
میزان دقت	٪۹۴	_	٪۹۷	_

٦. بحث و پیشنهادات کاربردی

تاکنون سیستم‌های هوشمند (خبره) بسیاری در حوزه ارزیابی امنیت اطلاعات توسعه داده شده‌اند. سیستم‌های موجود عموماً به ارزیابی ریسک و تعیین سطح خطر پرداخته‌اند. در تمام سیستم‌های موجود اهمیت اهداف و معیارهای ارزیابی امنیت یکسان در نظر گرفته‌شده است، درصورتی‌که در واقعیت میزان اهمیت اهداف و معیارهای ارزیابی باهم متفاوت می‌باشد. بدین منظور پژوهش حاضر در راستای خلق نوآوری، با ترکیب دو ایده مطرح‌شده سعی در طراحی و پیاده‌سازی سیستم خبره جهت ارزیابی امنیت اطلاعات سازمان داشته است. در استاندارد ISO/IEC 27001، میزان اهمیت اهداف و معیارهای کنترل امنیت اطلاعات در مقایسه باهم یکسان در نظر گرفته‌شده درصورتی‌که طبق نظر خبرگان اهمیت این اهداف و معیارها یکسان نبوده و برخی از تأثیر بالاتری در برقراری امنیت نسبت به بقیه برخوردار هستند و در صورت عدم اجرای صحیح، امنیت سازمان را با مخاطرات جدی‌تری روبرو می‌کنند. وزن دادن به اهداف و معیارهای ارزیابی اهداف کنترلی منجر به توجه بیشتر به هدف موردنظر در برقراری امنیت شده و همین موضوع از بروز چالش‌های پر

ریسک امنیتی جلوگیری خواهد کرد.

در پژوهش حاضر اهداف کنترلی و معیارهای ارزیابی امنیت اطلاعات از استاندارد ایزو ۲۷۰۰۱ استخراج‌شده است و چک‌لیست مورداستفاده به‌صورت کاملاً منطبق با استاندارد می‌باشد و سیستم امتیاز امنیت اطلاعات سازمان بر اساس استاندارد را محاسبه کرده است. علاوه بر آن سیستم ارائه شده در مقایسه با پژوهش‌های پیشین دارای جنبه‌های نوآورانه ویژه می‌باشد. رتبه‌بندی اهداف و معیارهای کنترلی استاندارد طبق نظر خبرگان صورت پذیرفته و امتیاز امنیت اطلاعات با احتساب وزن اهداف کنترلی و معیارهای ارزیابی نیز محاسبه‌شده است. همچنین در ادامه اهداف اصلی امنیت اطلاعات به ازای هر توصیه (کنترل) طبق نظر خبرگان مشخص‌شده و سیستم طراحی‌شده میزان تحقق هدف اصلی امنیت در سازمان را نیز مورد ارزیابی قرار داده است.

شایان‌ذکر است که روش تخصیص امتیاز به هر کنترل بر اساس مصاحبه با ممیزان امنیت در ایران به کار گرفته شده است و ساختار استاندارد ایزو ۲۷۰۰۱ روش مشخصی برای امتیازدهی مشخص نکرده است که این مسئله در ایجاد قوانین و کارایی سیستم خبره تأثیرگذار می‌باشد.

پژوهش انجام‌گرفته هیچ‌گونه قصدی جهت تغییر دسته‌بندی اهداف اصلی استاندارد نداشته و در جهت بهبود امنیت سازمان باهدف مشخص کردن اهداف پراهمیت‌تر از منظر خبرگان حوزه امنیت، ساختار ضریب‌دار سلسله مراتبی را پیشنهاد کرده و بر اساس اطلاعات جمع‌آوری‌شده طی چندین مرحله مصاحبه، برای اهداف استاندارد وزن و ضریب تعیین شده است.

پیشنهاد می‌شود سیستم طراحی‌شده در سازمان‌ها و صنایع مختلف برای ارزیابی‌های درون‌سازمانی وضعیت امنیت اطلاعات به کار گرفته شود. سپس می‌بایست نتایج ارزیابی مورد تحلیل قرار گیرد تا در صورت نیاز، سازمان در جهت بهبود وضعیت امنیت اطلاعات خود در نقاط پراهمیت‌تر اقدامات اصلاحی انجام دهد. از سیستم طراحی‌شده می‌توان در شرکت‌هایی که پروانه صدور گواهی ایزو ۲۷۰۰۱ را کسب نموده‌اند و ممیزی را به شکل

سنتی انجام می‌دهند برای افزایش کارایی و کاهش زمان و هزینه استفاده نمود. با توجه به رتبه‌بندی اهداف کنترلی و معیارهای ارزیابی استاندارد، سازمان‌ها می‌توانند با توجه به اولویت‌های موجود خود در رابطه با اهداف کنترلی امنیت به تقویت و بهبود امنیت بپردازند. همچنین با تعیین اهداف اصلی امنیت اطلاعات به ازای هر توصیه استاندارد، سازمان می‌تواند با اقدامات اصلاحی و تقویتی در جهت رسیدن به اهداف اصلی امنیت گام بردارد. سیستم موردنظر می‌تواند در فواصل کوتاه و دوره‌ای جهت بهبود امنیت اطلاعات در سازمان مورداستفاده قرار بگیرد و با توجه به نتیجه ارزیابی طبق اولویت اهداف کنترلی و معیارهای ارزیابی برای اقدامات اصلاحی برنامه‌ریزی نموده و نتیجه ارزیابی پس از اصلاح با نتیجه قبلی مقایسه شود.

٦. جمع‌بندی

در این پژوهش یک سیستم خبره جهت ارزیابی امنیت اطلاعات طراحی شده است. این سیستم به محاسبه امتیاز امنیت اطلاعات با ساختار ضریب دار و مبتنی بر استاندارد ایزو ۲۷۰۰۱ می‌پردازد، بنابراین پیشنهاد می‌شود در مطالعات آتی سیستم خبره ضریب دار با ترکیب سایر استانداردهای امنیتی طراحی شود.

در پژوهش حاضر وزن لایه اهداف کنترلی و معیارهای ارزیابی بر مبنای نظر خبرگان محاسبه و اعمال شده است، پیشنهاد می‌شود سیستمی طراحی شود تا بتواند مقادیر وزن را به‌صورت منعطف و بر اساس نظر سازمان تحت ارزیابی در نظر بگیرد.

ساختار استاندارد به دلایل مختلفی چون مواجهه با تهدیدات جدید ممکن است دچار تغییراتی شود و نسخه جدیدی ارائه شود. در صورت تغییر نسخه استاندارد لازم است تا سیستم بازطراحی شود، اما به نظر می‌رسد نیاز به تغییر در ساختار سیستم وجود ندارد بلکه با اعمال تغییرات جدید و یا اضافه نمودن تعدادی از قواعد می‌توان این کار را انجام داد. در صورت تغییر کلی در ساختار سیستم می‌توان با به دست آوردن مجدد وزن اهداف کنترلی و معیارها سیستم را تغییر داد.

از دیگر موضوعاتی که می‌توان در تحقیقات آتی به آن پرداخت، مقایسه نتایج قبل و

بعد از اجرای این سیستم در سازمان خواهد بود که مزایای ارزیابی امنیت اطلاعات با استفاده از سیستم خبره را بیش‌ازپیش پررنگ خواهد نمود.

در پژوهش حاضر خروجی سیستم، وضعیت امنیت اطلاعات در سازمان را مشخص می‌کند، پیشنهاد می‌شود در تحقیقات آتی سیستمی طراحی شود که بتواند برای بهبود وضعیت امنیت اطلاعات در سازمان راهکارهای مختلفی عرضه کند.

تعارض منافع

تعارض منافع وجود ندارد.

ORCID

Melika Armandi **https://orcid.org/0009-0006-8619-8805**
Mina Ranjbar **https://orcid.org/0000-0002-5642-4190**
Zahra Taheri **https://orcid.org/0009-0003-1843-6726**

منابع

۱. آذر، عادل و مؤمنی، منصور. (۱۳۸۴). *آمار و کاربرد آن در مدیریت*. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها.

۲. آزادبیگی، نورالله. (۱۳۹۸). ارائه راهکارهای بومی و عملیاتی جهت رفع آسیب‌پذیری و تهدیدات امنیتی شبکه‌های کامپیوتری سازمانی در چارچوب استانداردهای ISO/IEC 27K (پایان‌نامه کارشناسی‌ارشد رشته کامپیوتر، گرایش نرم‌افزار). مؤسسه آموزش عالی اشراق بجنورد.

۳. آفتابی، نوید. (۱۳۹۷). یک مدل مدیریت امنیت اطلاعات برای کاهش ریسک‌های احتمالی در سازمان‌های مبتنی بر فناوری اطلاعات (پایان‌نامه کارشناسی‌ارشد گرایش سیستم‌های اقتصادی و اجتماعی). دانشکده مهندسی صنایع، دانشگاه شریف.

۴. اخوان، فاطمه، موسوی، سید عبداله امین و سرآبادانی، ابوالقاسم. (۱۴۰۲). عوامل کلیدی موفقیت در پیاده‌سازی حاکمیت امنیت اطلاعات (مطالعهٔ موردی: شرکت نفت مناطق مرکزی ایران). *مطالعات راهبردی در صنعت نفت و انرژی*، *۱۴* (۵۶)، ۱۳۲-۱۱۳.

۵. جعفرنژاد، سهیلا و تقوا، محمدرضا. (۱۳۹۸). نقش پیاده‌سازی چارچوب‌های مدیریت خدمات و امنیت (ITIL و ISMS) در تداوم خدمات فناوری اطلاعات. *نشریه علمی مطالعات مدیریت کسب و کار هوشمند*، *۷* (۳۰)، ۳۳-۵۴.

۶. شاه‌بهرامی، اسدالله، رفیع‌زاده کاسانی، رامین و پوریوسفی‌درگاه، حسین. (۱۳۹۷). شناسایی و اولویت‌بندی پارامترهای تأثیرگذار بر سیستم مدیریت امنیت اطلاعات (مطالعه موردی: شعب تأمین اجتماعی استان گیلان). *فصلنامه علمی-پژوهشی فناوری اطلاعات و ارتباطات ایران*، *۱۰* (۳۵ و ۳۶)، ۵۷-۷۴.

۷. شیخ‌ابومسعودی، روح‌اله، کوهی‌حبیبی، سحر، عطایی، مریم و اسماعیلی، نازیلا. (۱۳۹۴). ارزیابی سیستم‌های مدیریت اطلاعات دانشگاه علوم پزشکی با استفاده از استاندارد ISO/IEC 27001. *مدیریت اطلاعات سلامت*، *۱۲* (۳)، ۳۰۶-۳۱۶.

۸. فرهادی، کامران. (۱۳۹۶). *آموزش جامع پیاده‌سازی و سرممیزی سیستم مدیریت امنیت اطلاعات*. تهران: آکادمی باتیس.

۹. میدانی، زهرا، عصاری، محمدامین، موسوی، سید غلامعباس و عطایی اندزق، علی. (۱۳۹۶). ارزیابی امنیت سیستم‌های اطلاعات بیمارستانی. *مدیریت اطلاعات سلامت*، ۵ (۱۴)، ۱۸۷-۱۹۳.

References

10. Aileen, A., & Fianty, M. I. (2024). Capability level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Journal of Information Security, 8*(1), 91-103.
11. Atymtayeva, L. B., Bortsova, G. K., Inoue, A., & Kozhakhmet, K. T. (2012). Methodology and ontology of expert system for information security audit. In *The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligent Systems* (pp. 238-243). IEEE.
12. Bartoš, J., Walek, B., Klimeš, C., & Farana, R. (2014). Fuzzy tool for conducting information security risk analysis. In *Proceedings of the 2014 15th International Carpathian Control Conference (ICCC)* (pp. 28-33).
13. Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report, 11*, 26–31.
14. Chang, L.-Y., & Lee, Z.-J. (2013). Applying fuzzy expert system to information security risk assessment: A case study on an attendance system. In *2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY)* (pp. 346-351).
15. Clinch, J. (2009). ITIL V3 and information security. *Best Management Practice*.
16. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76-105.
17. Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security, 63*, 1-13.
18. Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*. https://doi.org/10.1177/01655515231160026
19. Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science, 48*(2), 213-222.

20. Ganji, D., Kalloniatis, C., Mouratidis, H., & Malekshahi Gheytassi, S. (2019). Approaches to develop and implement ISO/IEC 27001 standard-information security management systems: A systematic literature review. *International Journal on Advances in Software, 12*(3).
21. Hentea, M. (2007). Intelligent system for information security management: Architecture and design issues. *Informing Science: International Journal of an Emerging Transdiscipline, 4*(1), 29-43.
22. Herath, T. C., Herath, H. S. B., & Cullum, D. (2023). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers, 25*(2), 681-721.
23. ISO/IEC 27000. (2013). Information technology, security techniques. Information security management systems. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
24. Kamal, M., Muhamad, M., Sudianto, Y., Fauzan, M. A., Anggito, Y., Yasin, W., & Hermawan, H. (2024). Information technology security audit at the YDSF national zakat institution using the ISO 27001 framework. *Jurnal Sisfokom (Sistem Informasi dan Komputer), 13*(1).
25. Kanatov, M., Atymtayeva, L. B., & Yagaliyeva, B. (2014). Expert systems for information security management and audit: Implementation phase issues. In *2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS)* (pp. 896-900).
26. Khafidh Sunny Al Fajri, & Harwahyu, R. (2024). Information security management system assessment model by integrating ISO 27002 and 27004. *Institut Riset dan Publikasi Indonesia (IRPI)*. P-ISSN: 2797-2313.
27. Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a risk analysis strategy framework for impact assessment in information security management systems: A case study in IT consulting industry. *Sustainability, 14*(3), 1269.
28. Kozhakhmet, K. T., Bortsova, G., Inoue, A., & Atymtayeva, L. B. (2012). Expert system for security audit using fuzzy logic. In *Midwest Artificial Intelligence and Cognitive Science Conference* (p. 146).
29. Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., & Bazylevych, V. (2016). Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. *Восточно-Европейский журнал передовых технологий, 65*(4), 32-45.

30. Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., & Singh, V. (2010). A survey of payment card industry data security standards. *IEEE Communication Surveys & Tutorials, 12*(3), 287-303.
31. Mera-Amores, F., & Roa, H. N. (2024). Enhancing information security management in small and medium enterprises (SMEs) through ISO 27001 compliance. In *Future of Information and Communication Conference* (pp. 197-207). Cham: Springer Nature Switzerland.
32. Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security, 109*, 102383.
33. Muhammad Azam, M. S., Ali Khan, M., & Yang, S. (2022). A decision-making approach for the evaluation of information security management under complex intuitionistic fuzzy set environment. *Journal of Mathematics, 2022*, Article ID 9704466. https://doi.org/10.1155/2022/9704466
34. Olzak, T. (2013). Insider threats: Implementing the right controls. TechRepublic.
35. Piech, H., & Grodzki, G. (2017). Audit expert system of communication security assessment. *Procedia Computer Science, 112*, 147-156.
36. Proenca, D., & Borbinha, J. (2018). Information security management systems: A maturity model based on ISO/IEC 27001. In *Business Information Systems: 21st International Conference, BIS 2018, Berlin, Germany, July 18-20, Proceedings 21* (pp. 102-114).
37. Raghavendra Rao Althar, D. S., Samanta, D., Purushotham, S., Singh Senga, S., & Hewage, C. (2023). Design and development of artificial intelligence knowledge processing system for optimizing security of software system. *SN Computer Science, 4*, 331.
38. Riswaya, A. R., Sasongko, A., Maulana, A., Mardira Indonesia, S., & Langlangbuana Bandung, U. (2020). Evaluasi tata kelola keamanan teknologi informasi menggunakan indeks kami untuk persiapan standar SNI ISO/IEC 27001 (Studi Kasus: STMIK Mardira Indonesia). *Jurnal Computech & Bisnis, 14*(1), 10–18.
39. Rkaur, G., Rani, P., & Garg, S. (2016). Various issues in expert system for information management and audit. *International Journal of Advanced Research in Computer Science, 79*(3), 245-261.
40. Saha, P., Mahanti, A., Chakraborty, B. B., & Navlani, A. (2013). Development of ontology-based framework for information security standards. In *Proceedings of the 9th International Conference on Autonomic and Autonomous Systems* (pp. 83-89).
41. Sendi, A. S., Jabbarifar, M., Shajari, M., & Dagenais, M. (2010). FEMRA: Fuzzy expert model for risk assessment. In *2010 Fifth*

International Conference on Internet Monitoring and Protection (pp. 48-53).

42. Sihwi, S. W., Andriyanto, F., & Anggrainingsih, R. (2016). An expert system for risk assessment of information system security based on ISO 27002. In *2016 IEEE International Conference on Knowledge Engineering and Applications (ICKEA)* (pp. 56-61).
43. Singhal, D., Tripathy, S., & Kumar Jena, S. (2018). DEMATEL approach for analyzing the critical factors in remanufacturing process. *Materials Today: Proceedings, 5*(9), 18568-18573.
44. Sun, H., & Bai, S. H. (2022). Enterprise information security management using Internet of Things combined with artificial intelligence technology. *Computational Intelligence and Neuroscience, 2022*, Article ID 7138515. https://doi.org/10.1155/2022/7138515
45. Suorsa, M., & Helo, P. (2024). Information security failures identified and measured: ISO/IEC 27001: 2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal: A Global Perspective*, 1-22.
46. Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences, IJECSIJENS, 11*(5), 23-29.
47. Tarek Ali, M., Al-Khalidia, M., & Al-Zaidib, R. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2024.2329985
48. Tripathi, K. P. (2011). A review on knowledge-based expert system: Concept and architecture. *IJCA Special Issue on Artificial Intelligence Techniques-Novel Approaches & Practical Applications, 4*, 19-23.
49. Wallhoff, J. (2004). Combining ITIL with COBIT and ISO/IEC 17799: 2000. *Scillani Information AB.*
50. Holbert, R. L., Lee, J., Esralew, S., Walther, W. O., Hmielowski, J. D., & Landreville, K. D. (2013). Affinity for political humor: An assessment of internal factor structure, reliability, and validity. *Humor, 26*(4), 551-572.
51. Deepak, S., Sushant, T., & Sarat, K. (2018). DEMATEL approach for analyzing the critical factor in remanufacturing process. *Materials Today: Proceedings, 5*, 18568–18573.
52. Sfaei, H., & Homayounzadeh, F. (2017). A hybrid approach using fuzzy multi-criteria techniques to evaluate the performance of in-service training courses (Case study: Mazandaran and Golestan Regional

Electricity Company). *Journal of Applied Research on Industrial Engineering, 4*(1), 39–49.

53. Zavadskas, E. K., Turskis, Z., Antucheviciene, J., & Zakarevicius, A. (2012). Optimization of weighted aggregated sum product assessment. *Electronics and Electrical Engineering, 122*(6), 3-6.

استناد به این مقاله: ارمندئی، ملیکا.، رنجبرفرد، مینا.، طاهری، زهرا. (۱۴۰۳). سیستم خبره ضریب‌دار سلسله مراتبی جهت ارزیابی امنیت اطلاعات سازمان مبتنی بر استاندارد بین‌المللی ایزو ۲۷۰۰۱، *مطالعات مدیریت کسب وکار هوشمند*، ۱۳(۵۰)، ۴۹-۹۷. DOI: 10.22054/ims.2024.76541.2401