International Journal of Safety and Security Engineering
Vol. 16, No. 3, March, 2026, pp. 655-667
Journal homepage: http://iieta.org/journals/ijsse

Strategies for Information Security in Medical Appointment Management Systems

Misael Lazo Amado, Laberiano Andrade-Arenas*

Faculty of Sciences and Engineering, Universidad de Ciencias y Humanidades, Lima 15304, Perú

Corresponding Author Email: landrade@uch.edu.pe

https://doi.org/10.18280/ijsse.160316

Received: 14 February 2026
Revised: 20 March 2026
Accepted: 25 March 2026
Available online: 31 March 2026

Keywords:
continuous improvement, information security, ISO27001, medical appointment, risks

ABSTRACT

Medical appointment management systems are essential tools for improving efficiency, coordination, and service quality in healthcare organizations. These platforms handle highly sensitive information, including personal and clinical data, making them vulnerable to internal misuse, human error, and external cyber threats. Inadequate security controls may compromise the confidentiality, integrity, and availability of information, potentially disrupting operations and undermining patient trust. This study aims to design and implement structured information security strategies for such systems based on the ISO/IEC 27001 standard. It adopts the Information Security Management System (ISMS) framework, focusing on systematic risk identification, qualitative and quantitative risk assessment, and risk treatment through Annex A controls. Additionally, it incorporates contingency planning, business continuity, secure backup policies, encryption, access control, and continuous improvement supported by the Plan-Do-Check-Act (PDCA) cycle. The results show a substantial reduction in identified risks, with most reaching acceptable levels, while some residual risks require continuous monitoring. A quantitative evaluation revealed improvements between 15% and 40%, with an average increase of 22.7%. Key indicators include 98% backup success, 100% encryption coverage, full access compliance, and 99.95% system availability, demonstrating enhanced security and operational resilience.

1. INTRODUCTION

In the digital era, online medical appointment systems have become essential tools to facilitate healthcare, offering patients and professionals an efficient, accessible, and fast platform for managing their consultations. However, the management of medical information involves a high degree of sensitivity, as it includes personal and clinical data that require strict protection measures to prevent unauthorized access, loss, or improper manipulation. Therefore, the implementation of information security in these systems is crucial to ensure the confidentiality, integrity, and availability of data, protect patient privacy, and comply with current legal regulations [1-3]. This process involves adopting recognized regulatory frameworks such as ISO/IEC 27001, applying robust technologies, and fostering an organizational culture committed to security [4], which helps mitigate risks and strengthen trust in digital health services [5].

The absence of a well-structured security system can lead to multiple negative consequences, ranging from identity theft [6], exposure of confidential information, and misuse of data, to non-compliance with legal regulations such as personal data protection laws in the healthcare sector. In addition, the loss of user trust and the deterioration of institutional reputation can have irreversible effects [7-9]. This risk increases particularly in environments with low cybersecurity awareness, lack of internal policies, and absence of technical controls [10].

One of the most serious risks arising from the lack of security in medical appointment systems is identity theft. When a platform lacks strong protection mechanisms such as encryption, multi-factor authentication (MFA), or access controls, it becomes vulnerable to data breaches [11]. Attackers can obtain personal information such as full names, identification numbers, addresses, phone numbers, emails, health insurance numbers, and even details about diagnoses or treatments. With this data, criminals can impersonate patients to access other healthcare services [12-14], request controlled medications, conduct financial fraud, or illegally open bank accounts and lines of credit [15]. Similarly, the impersonation of medical personnel can facilitate more complex fraudulent activities, such as issuing false prescriptions or gaining access to internal institutional systems [16]. Furthermore, such incidents not only affect direct victims but also compromise the credibility of the healthcare system, increase operational costs due to internal investigations, and impact regulatory compliance in data protection [17-20]. For these reasons, identity theft prevention should be considered a priority in the implementation of any information security strategy in healthcare environments.

Trust is a fundamental element in the relationship between patients and healthcare providers, especially when managing sensitive information through digital platforms such as medical appointment systems [21]. A security incident, such as a data breach or unauthorized access, can severely undermine this trust, generating fear and resistance toward the use of digital technologies for health management [22-25].

When patients perceive that their personal data are not adequately protected, they may choose to avoid online systems, preferring traditional methods that, although less efficient, provide a greater sense of control and security [26]. This distrust not only limits the adoption of technological innovations that could improve medical care and patient experience, but also impacts the reputation of healthcare providers [27], reducing user loyalty and satisfaction. In the long term, loss of trust may result in lower engagement levels, reduced availability of data for clinical analysis, and a decline in the overall quality of digital healthcare services.

Despite the growing adoption of information security frameworks such as ISO/IEC 27001 in healthcare environments, existing studies mainly focus on general implementations or theoretical approaches, without specifically addressing the requirements and operational challenges of online medical appointment systems. In particular, there is limited integration between risk assessment, control implementation, system architecture, and their validation in real-world operational contexts tailored to these platforms.

Furthermore, many approaches do not explicitly evaluate how security controls mitigate critical risks such as identity theft, unauthorized access, or service disruption, nor how these controls influence user trust in digital health services.

In this context, this study aims to fill this gap by proposing and implementing an Information Security Management System (ISMS) specifically adapted to a medical appointment system. The novelty of this research lies in the integration of a structured risk management process, the application of ISO/IEC 27001-based controls, the incorporation of system architecture design, and the evaluation of their effectiveness in mitigating risks within a real operational environment.

This approach not only strengthens data protection but also provides a practical and replicable model for other digital healthcare systems.

2. LITERATURE REVIEW

This section reviews the literature, addressing the theoretical foundations that underpin this article. It also analyzes the background of previous research, with the aim of demonstrating how various authors show that the application of information security is effective in protecting data and improving digital systems.

2.1 Background

Secure information management in medical appointment systems is essential to protect sensitive patient data and ensure trust in digital health services. In this context, the existing literature can be grouped into three main approaches: (i) implementations based on standards such as ISO/IEC 27001, (ii) technical security controls, and (iii) organizational practices and human factors.

First, several studies analyze the implementation of ISMSs based on ISO/IEC 27001. These works highlight benefits such as improved risk management, regulatory compliance, and strengthened organizational reputation [28, 29]. Additionally, recent research shows that the adoption of ISO 27001:2022 significantly enhances the cybersecurity posture of organizations across different sectors [30]. However, other studies indicate that many organizations remain at intermediate levels of ISMS maturity, suggesting challenges in achieving full implementation and the need to apply continuous improvement approaches such as the PDCA cycle [31]. Overall, these studies agree on the importance of the standard, but differ in terms of implementation level and evaluation in real-world contexts.

Second, another group of studies focuses on technical security controls, such as data encryption, authentication mechanisms, and access control. These studies consistently emphasize that such controls are essential to ensure the confidentiality, integrity, and availability of medical information [32, 33]. However, they also highlight that, despite their recognized importance, the practical implementation of these mechanisms in healthcare environments remains challenging, particularly in specific systems such as medical appointment platforms, where the integration of multiple technologies may introduce additional vulnerabilities.

Third, several studies highlight the importance of organizational and human factors in information security. It has been shown that continuous staff training, security culture, and user behavior directly influence the effectiveness of security policies [34, 35]. Furthermore, user perception of security has been identified as a key factor influencing trust and adoption of digital health systems [36]. Nevertheless, a gap persists between the recognized importance of information security and the actual implementation of formal controls within organizations [37].

Overall, the reviewed studies can be clearly grouped into three main categories: (i) ISO/IEC 27001-based management implementations, (ii) technical security control approaches, and (iii) organizational and human-centered practices. ISO-based studies primarily focus on governance, compliance, and risk management frameworks, while technical approaches emphasize mechanisms such as encryption, authentication, and access control. On the other hand, organizational studies highlight the role of user behavior, training, and security culture in ensuring effective protection.

Despite these contributions, most existing works address these aspects in isolation, lacking a comprehensive integration of management standards, technical controls, and human factors within a single operational system. Furthermore, limited research evaluates these elements in real-world implementations, particularly in specific platforms such as medical appointment systems.

This gap highlights the need for an integrated and practically validated approach, which is addressed in this study.

2.2 Theoretical bases

2.2.1 Information security

Information security is the set of principles, policies, and controls designed to protect data from unauthorized access, improper alteration, or accidental loss. Its main purpose is to ensure confidentiality, integrity, and availability of information, which are fundamental pillars in any organizational environment. Nowadays, with digital systems managing large volumes of data, its application has become essential [38]. This discipline encompasses both technical measures, such as encryption and access controls, and administrative strategies, such as internal regulations and staff training. It also includes the identification and management of risks that may affect information assets. Information security

is not limited to the technological sphere but also involves processes and people. Its proper implementation reduces vulnerabilities and prevents security incidents. It also contributes to compliance with legal regulations related to data protection. In the healthcare sector, for example, it is key to safeguarding sensitive patient information [39-42]. In short, it is a strategic element in ensuring trustworthiness and continuity of digital services.

2.2.2 Risk management

Risk management is a systematic process aimed at identifying, analyzing, and controlling events that may affect the achievement of an organization's objectives [43]. Its main purpose is to reduce the probability of threats occurring and minimize the impact of possible negative consequences [44]. This approach allows organizations to anticipate adverse situations rather than reacting only after they have already occurred. Risk management involves assessing vulnerabilities, estimating exposure levels, and prioritizing preventive actions. It also requires the design of strategies for mitigating, transferring, accepting, or eliminating risk, depending on its nature and level of criticality [45]. It is not limited to the financial sphere, but also applies to areas such as technology, health, information security, and business management. A key component is decision-making based on objective analysis and reliable data. In addition, it fosters an organizational culture focused on prevention and continuous improvement. Its proper implementation contributes to institutional stability, sustainability, and resilience [46]. In short, risk management is a strategic tool for protecting resources and ensuring the achievement of organizational goals.

2.2.3 Continuous improvement

In summary, the literature reviewed shows that the implementation of ISMSs, especially under the ISO 27001 standards and their updates, constitutes a fundamental pillar to protect sensitive information in digital medical environments [47]. Critical elements such as ongoing training, effective access controls and encryption are recurrently highlighted as factors that strengthen security and trust in these systems [48]. However, challenges persist in the comprehensive adoption of these regulatory frameworks and their alignment with the specific needs of each organization, underscoring the need to continue investigating adaptive and effective implementation strategies. In this way, strengthening the security of medical appointment systems not only ensures regulatory compliance [49-51], but also protects patient privacy and improves the quality of digital health service.

3. METHOD

This section describes the methodology adopted to implement information security within a medical appointment management system, in alignment with the ISO/IEC 27001 standard. It outlines the structured approach followed to identify, assess, and mitigate technological risks, as well as to establish appropriate security controls. The methodology integrates risk management, policy development, control implementation, and continuous improvement processes to ensure the confidentiality, integrity, and availability of information. Through this framework, the organization strengthens its ISMS and enhances the protection of sensitive medical data.

3.1 ISO27001

Information security encompasses various management strategies that are analyzed through the ISO 27000 series. This series provides the technical requirements needed to mitigate the risks of security breaches [52]. In particular, ISO 27001 enables the assessment of security risks that may threaten organizations, helping them to meet their functional and strategic objectives. Companies apply this standard to organize, implement, develop, monitor, review and manage information security, ensuring data integrity, confidentiality and availability. A key approach of ISO 27001 is the PDCA cycle, which facilitates the continuous improvement of information security management processes. This systematic approach not only accelerates management processes but also ensures that security measures are effective and adaptable to the changing needs of the organization [53], as shown in Figure 1.

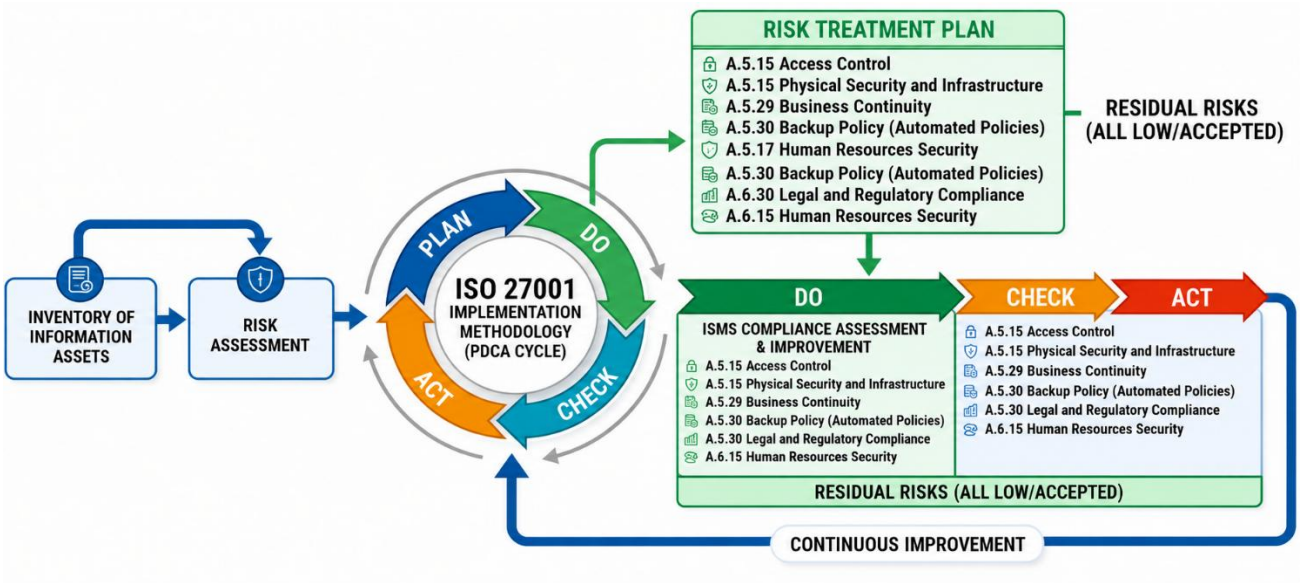

Figure 1. ISO 27001

3.2 Inventory of information assets

The inventory of information assets is an essential step in the implementation of an ISMS, as it allows to identify, classify and adequately protect all the elements that contain or process critical information for the organization. This inventory categorizes assets such as data, software, hardware, networks, backup media, auxiliary equipment, facilities and personnel, with specific examples for each type. Its importance lies in the fact that it facilitates the identification of risks, allows specific security controls to be assigned according to the criticality of each asset and guarantees traceability and control over the information, thus ensuring its confidentiality [54], integrity and availability.

Table 1 presents a structured inventory of information assets within the organization, identifying for each one its code, name, type, responsible party, location, and primary use. This includes digital assets such as the patient database and automatic backups, software assets such as the web-based appointment scheduling application, critical hardware such as computers, routers, switches, and the UPS system, as well as documentation and user credentials. This classification allows for the assignment of clear responsibilities, knowledge of where assets are located, and understanding of their operational function, facilitating risk management and the application of appropriate security controls according to their criticality.

Table 1. Inventory of information assets

Asset ID	Asset Name	Asset Type	Owner	Location	Primary Use
A001	Patient Database	Information / Digital	System Administrator	Central Server	Management of patient histories and appointments
A002	Appointment Web Application	Software	Development Area	Cloud / External Hosting	Scheduling and appointment management
A003	Reception Computers	Hardware	Technical Support	Front Desk	Patient registration and system access
A004	Security Policies Manual	Documentation	CISO	Shared Folder	Security compliance guidance
A005	Automatic Backups	Information / Digital	Backup Manager	Cloud + External Drive	Information recovery
A006	Router and Switches	Hardware	Network Department	Communications Room	System connectivity
A007	User Credentials	Confidential Information	Help Desk / Security Team	Access Control System	Access control
A008	Power Backup System (UPS)	Hardware	Infrastructure Department	Server Room	System continuity during power outages

3.3 Medical appointment system architecture

The proposed medical appointment management system is based on a layered architecture designed to ensure scalability, security, and reliability. The system is structured into five main layers: user interface, API Gateway/backend, security layer, database layer, and external services, as shown in Figure 2.

The user interface layer consists of a web application developed using modern frameworks such as React or Angular, providing an intuitive and accessible interface for patients, doctors, and administrative staff. This layer is responsible for handling user interactions and forwarding requests to the backend through secure communication channels.

The API Gateway/backend layer represents the core of the system and is responsible for processing business logic and managing system operations. It integrates key security mechanisms such as MFA and role-based access control (RBAC), ensuring that only authorized users can access specific functionalities. In addition, a security middleware component is implemented to validate incoming requests, manage sessions, and detect anomalous behaviors.

The security layer includes protection mechanisms such as firewalls, intrusion detection and prevention systems (IDS/IPS), and centralized logging and monitoring tools. These components enable real-time threat detection and support incident response processes in accordance with ISO/IEC 27001 requirements.

The database layer stores sensitive patient information in encrypted form, ensuring data confidentiality and protection against unauthorized access. It also incorporates backup mechanisms and audit logs to guarantee data integrity, availability, and traceability.

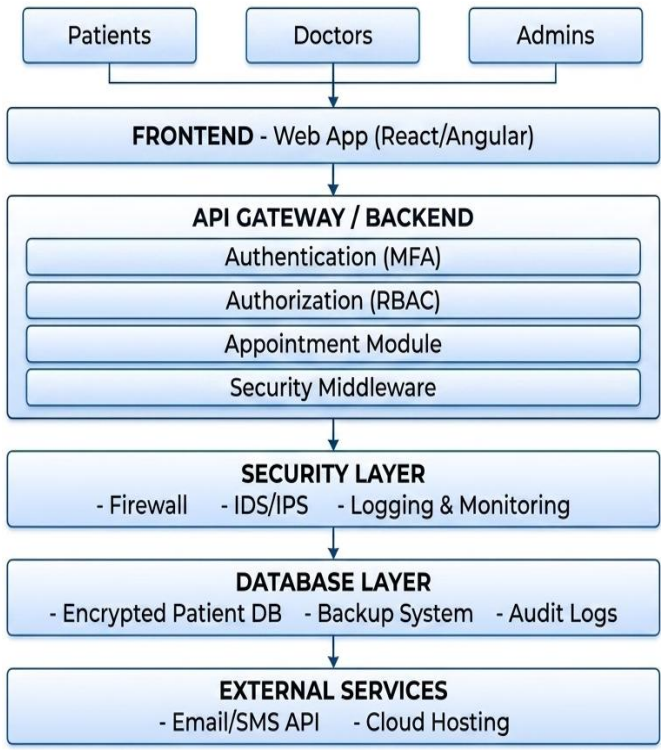

Figure 2. System architecture

Finally, the system integrates external services such as cloud hosting infrastructure and email/SMS APIs, which support system scalability, availability, and communication with users.

Overall, this layered architecture enables the effective implementation of ISO/IEC 27001 security controls across all system components, ensuring a robust, secure, and resilient medical appointment management system, as shown in Figure 2.

Additionally, secure communication between layers is enforced through TLS 1.3 encryption, and sensitive data at rest is protected using AES-256 encryption, ensuring compliance with modern security standards.

3.4 System modules

To facilitate the understanding of the internal structure of the proposed system, it is organized into several functional modules. Each module is responsible for specific tasks and contributes to both the functionality and security of the system. The main modules and their respective functions are summarized in Table 2.

Table 2. System modules description

Module	Description	Security Function
Authentication Module	Manages user login and identity verification	Multi-Factor Authentication (MFA)
Authorization Module	Controls access based on user roles	Role-Based Access Control (RBAC)
Appointment Module	Handles appointment scheduling and management	Access validation
Security Middleware	Filters and validates incoming requests	Threat detection and prevention
Logging and Monitoring	Records system activities	Auditing and incident detection
Database Module	Stores and retrieves patient data	Data encryption and integrity protection

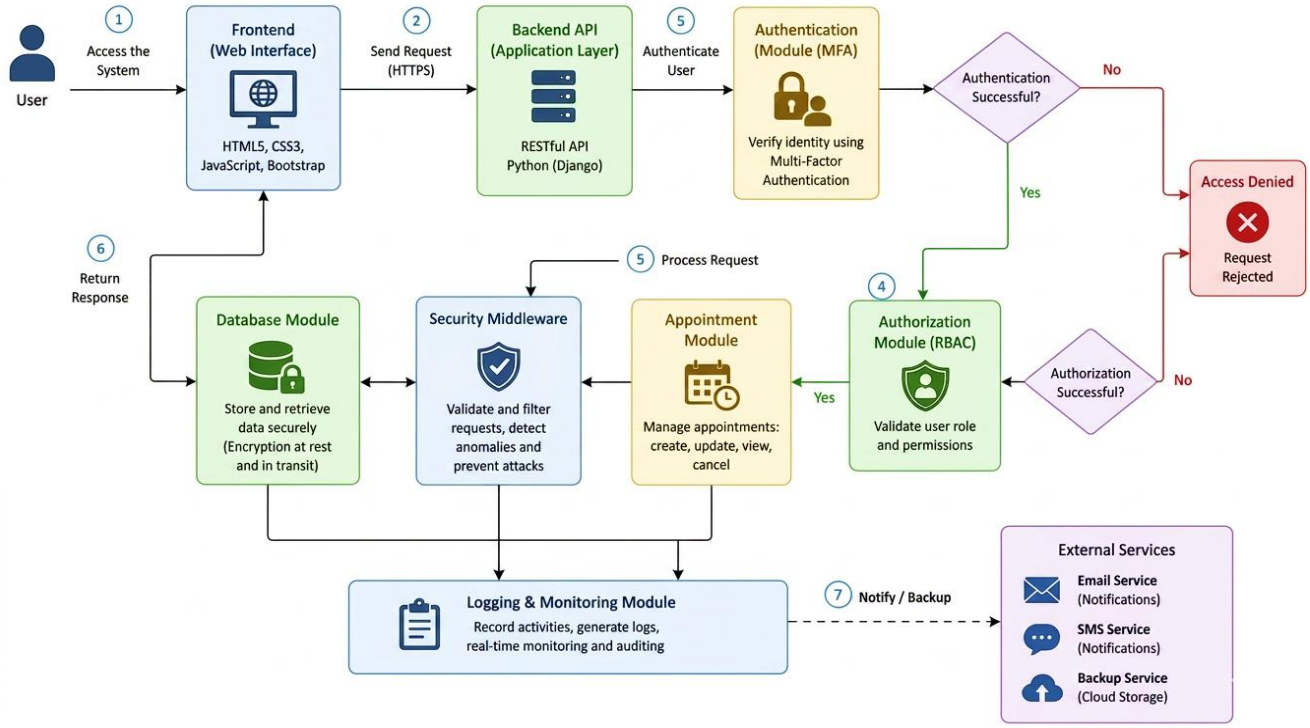

Figure 3. System interaction flow

As shown in Table 2, each module performs a specific function to ensure the secure and efficient operation of the system. The integration of authentication, authorization, and monitoring mechanisms strengthens the system's ability to prevent unauthorized access and detect potential threats. To provide a detailed understanding of how the system operates during execution, the interaction flow between its components is illustrated in Figure 3. The process begins when a user accesses the system through the web interface. The request is securely transmitted via HTTPS to the backend API, where it is initially processed by the authentication module. This module verifies the user's identity using a MFA mechanism.

3.5 Attack scenarios and mitigation measures

To strengthen the technical perspective of the proposed system, several potential cybersecurity attack scenarios were analyzed. These scenarios were selected based on common threats affecting healthcare information systems and their potential impact on confidentiality, integrity, and availability. For each identified threat, corresponding mitigation strategies were defined and implemented within the system architecture. The analyzed attack scenarios and their respective countermeasures are summarized in Table 3.

As shown in Table 3, the implementation of layered security mechanisms significantly reduces both the likelihood and impact of these attacks. In particular, the use of MFA and RBAC strengthens protection against unauthorized access, while secure coding practices mitigate injection attacks. Furthermore, backup and recovery strategies enhance system resilience against data loss incidents such as ransomware.

Table 3. Attack scenarios and mitigation strategies

Attack Scenario	Description	Impact	Mitigation Strategy
Unauthorized Access	Use of stolen credentials to access the system	Exposure of patient data	Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), account lockout mechanisms
SQL Injection	Malicious input used to manipulate database queries	Data leakage or corruption	Input validation, prepared statements, parameterized queries
Ransomware Attack	Malware encrypts system data	System unavailability	Regular backups, network segmentation, disaster recovery plans

3.6 System interaction flow

If authentication is successful, the request proceeds to the authorization module, which evaluates user permissions based on RBAC. If this stage fails, access to the system is denied. Once authorized, the request is forwarded to the appointment module, where the corresponding operation is executed, such as creating, updating, or retrieving appointment data. Before reaching the core functionality, the request passes through a security middleware layer, which performs validation, filters malicious inputs, and detects potential threats. Subsequently, the system interacts with the database module to securely store or retrieve information. All relevant activities are recorded by the logging and monitoring module, enabling traceability and supporting audit processes. Finally, the system may interact with external services, such as email or SMS APIs, to send notifications to users. The processed response is then returned to the user through the interface. As shown in Figure 3, this structured interaction flow ensures secure, controlled, and efficient processing of user requests, while maintaining system integrity and data protection.

3.7 Residual risk

Residual risk is defined as the level of risk that persists after the implementation of controls or mitigation measures, and represents the actual exposure that an organization still faces. Unlike initial risk, residual risk considers the effectiveness of the controls implemented, allowing a more accurate assessment of the security environment. Mathematically, it is expressed by the formula (1) where (RR) is the residual risk, (Ri) is the initial risk calculated as I×P (impact per probability), and (Ec) is the overall effectiveness of the implemented controls, in a range from 0 to 1. This formula provides a quantitative basis for risk management decision making.

$$RR=Ri\times(1-Ec) \quad (1)$$

This extended formulation enhances the traditional risk model by incorporating the effectiveness of implemented controls, providing a more realistic and less simplistic representation of the risk environment. By considering mitigation capacity, the model allows a more accurate estimation of residual risk and supports better decision-making in information security management.

3.8 Risk evaluation criteria

To ensure consistency and reduce subjectivity in risk assessment, standardized scales were defined for assigning impact (I) and probability (P) values, aligned with ISO/IEC 27001 best practices. These scales are established on a range from 1 to 5, where each level represents a specific degree of severity or likelihood. The assignment of these values is based on a combination of predefined criteria, expert judgment, and, where available, historical security incident data from similar systems. Table 4 presents the impact evaluation scale, considering factors such as the effect on confidentiality, integrity, availability of information, regulatory compliance, and service continuity. This structured definition of scales ensures consistency, repeatability, and reduces subjectivity in the risk evaluation process.

Similarly, Table 5 presents the probability scale, which evaluates the likelihood of occurrence of a threat based on the system's operational context.

Table 4. Impact evaluation scale

Value	Impact Level	Description
1	Very Low	Minimal impact without affecting operations or data confidentiality
2	Low	Minor impact with limited effect, quickly recoverable
3	Moderate	Significant impact with partial service disruption
4	High	Severe impact affecting critical processes and compromising sensitive data
5	Very High	Critical impact involving data loss, legal non-compliance, and severe reputational damage

Table 5. Probability scale

Value	Probability Level	Description
1	Very Low	Highly unlikely event, with no known prior occurrences.
2	Low	Unlikely event, occurring sporadically.
3	Moderate	Possible event; has occurred occasionally.
4	High	Likely event; occurs with some frequency.
5	Very High	Very frequent event or almost certain to occur.

3.9 Risk level classification

Based on the values of impact (I) and probability (P), the initial risk level (Ri) is calculated by multiplying both factors (Ri = I × P). This result allows risks to be classified into different levels, facilitating their prioritization and supporting decision-making in the implementation of security controls.

Table 6 presents the risk level classification, establishing ranges that help identify the criticality of each risk and define appropriate treatment actions.

Table 6. Risk level classification

Range (Ri = I × P)	Risk Level	Impact Description	Recommended Action
1 - 5	Low	Minimal risk with limited impact	Accept and monitor
6 - 10	Moderate	Manageable risk with moderate impact	Implement additional controls
11 - 15	High	Significant risk affecting key processes	Prioritized mitigation
16 - 25	Critical	Severe risk with high organizational impact	Immediate action and strict controls

3.10 Example of risk evaluation and calculation

To enhance the understanding of the risk assessment process, a practical example is presented using an asset from the medical appointment system.

First, the selected asset is the patient database (A001), which contains highly sensitive personal and clinical information. Subsequently, a relevant threat is identified, such as unauthorized access to the system.

For the risk evaluation, two criteria are used: impact (I) and probability (P), both measured on a standardized scale from 1 to 5, where 1 represents a very low level and 5 represents a very high level.

Impact (I): A value of 5 is assigned, as the exposure of medical data would severely compromise patient privacy, legal compliance, and the organization's reputation.

Probability (P): A value of 4 is assigned, considering that attacks are likely to occur in the absence of robust security controls. The initial risk is calculated as follows: $Ri = I \times P = 5 \times 4 = 20$.

To reduce this risk, the following security controls are implemented: database encryption, MFA, and RBAC.

These controls are aligned with the best practices defined in ISO/IEC 27001 and aim to reduce both the probability and impact of the identified threat.

The effectiveness of the implemented controls (Ec) is estimated at 0.7 (70%), based on expert evaluation and expected control performance according to ISO/IEC 27001 guidelines, based on their level of implementation and expected mitigation capability. The residual risk is calculated as follows: $RR = Ri \times (1 - Ec) = 20 \times (1 - 0.7) = 6$.

This result indicates that the risk is reduced from a High level (20) to a Moderate level (6), demonstrating that the implemented controls significantly improve the system's security posture. However, continuous monitoring and periodic reassessment are still required to ensure sustained risk control.

4. RESULTS

This section presents the main results obtained during the development of the study, focusing on the design of a contingency plan derived from the identified technological risks. The plan was structured based on a prior risk assessment that evaluated vulnerabilities and their potential impact on operations. It is aligned with the requirements of the ISO/IEC 27001 standard and supports the implementation of an ISMS. The risk treatment plan is used to define and implement actions to reduce the risks identified in an organization, seeking to reduce their impact or probability of occurrence to acceptable levels; it allows prioritizing measures, assigning responsibilities and ensuring compliance with standards such as ISO 27001.

4.1 Risk assessment

The Risk Identification and Analysis Matrix evaluates the main technological risks by linking each identified threat to its corresponding vulnerability. Each risk is coded (e.g., AME001) and assessed based on its probability of occurrence (P) and impact (I), using a standardized scale from 1 to 5, as defined in the methodology. The resulting risk value is calculated using the expression ($R = P \times I$), which enables the classification of risks into different levels according to their severity. Based on this evaluation, risk levels are categorized as Medium, High, or Critical, following predefined classification ranges. Critical risks ($R \geq 16$) require immediate attention due to their potential to significantly affect system operations, compromise sensitive data, or lead to regulatory non-compliance. High risks (R = 11-15) represent significant threats that must be prioritized for mitigation, while Medium risks (R = 6-10), although less severe, still require appropriate control measures to prevent escalation.

Table 7 presents the systematic assessment of 26 technological risks identified within the organization, establishing a clear relationship between each risk and its associated vulnerability. The results indicate that a significant proportion of the risks are classified as Critical and High, reflecting a considerable level of exposure prior to the implementation of security controls. These risks include hardware failures, power outages, unauthorized access, regulatory non-compliance, malware threats, unencrypted data transmission, and the absence of a business continuity plan.

This distribution highlights the need for a structured and proactive approach to risk management, as promoted by ISO/IEC 27001, in order to reduce potential impacts on operational continuity, data protection, and organizational reliability. Although a smaller number of risks fall within the Medium category, they still represent relevant operational concerns and must be addressed through appropriate preventive and corrective controls. Overall, this matrix serves as a strategic tool for prioritizing mitigation actions and guiding the implementation of an effective ISMS.

4.2 Risk treatment plan

Table 8 details the implementation of the risk treatment plan, showing that each identified threat was addressed through specific corrective and preventive actions aligned with the controls established in ISO/IEC 27001. It specifies the type of treatment applied (mitigation), the description of the action plan, the associated regulatory control, the responsible area, and the residual risk assessment.

The results indicate that, following the implementation of technical, organizational, and administrative measures, most risks were reduced to low and acceptable residual levels, achieving a closed status. This demonstrates a systematic and effective risk management approach aimed at strengthening information security and ensuring the continuous improvement of the ISMS.

However, a limited number of risks remain at a moderate level due to their inherent nature and dependence on external factors, such as infrastructure reliability and the evolving landscape of cyber threats. These risks are considered

acceptable within the organization's risk tolerance but require continuous monitoring and periodic reassessment to ensure their impact remains under control over time.

Furthermore, the results reflect a controlled implementation scenario, in which security measures were applied under defined conditions and aligned with ISO/IEC 27001 requirements. Therefore, while all identified risks were addressed, not all can be completely eliminated, reinforcing the importance of continuous improvement within the ISMS.

Table 7. Risk assessment

ID RISK	Risk	Vulnerability	(P)	(V)	(R)	(NR)
AME001	Lack of software license	Lack of inventory and management	4	4	16	Critical
AME002	Hardware failures	Obsolete or poorly maintained equipment	5	4	20	Critical
AME003	Power outage	No energy backup	5	5	25	Critical
AME004	Unauthorized access	Authentication/authorization failure	4	4	20	Critical
AME005	Internet connection failure	Single provider with no backup	3	4	12	High
AME006	DNS hijacking	Unsecured or unmonitored DNS	5	5	16	High
AME007	Lack of backups	Lack of policies and testing	4	4	16	High
AME008	Untrained staff	Lack of training	3	4	12	High
AME009	Accidental data alteration	Misconfigured permissions	3	4	12	High
AME010	Uncontrolled physical access	Unmonitored facilities	3	5	15	High
AME011	Duplicate or overlapping appointments	Lack of logical validations	4	3	12	High
AME012	Outdated software	Inadequate patching	5	3	15	High
AME013	Weak passwords	Poor password policy	4	4	16	Critical
AME014	Lack of incident reporting	Informal or nonexistent processes	5	4	20	Critical
AME015	Non-compliance with LOPD/GDPR	Processing without legal basis	5	5	25	Critical
AME016	Single provider dependency	No backup or clear contract	5	5	25	Critical
AME017	Uncontrolled BYOD use	No policies or control	4	4	16	Critical
AME018	Malware or ransomware	No active protection or alerts	4	4	16	Critical
AME019	Uncertified medical software	Unvalidated or pirated software	4	5	20	Critical
AME020	Outdated policies	Lack of periodic review	3	4	12	Medium
AME021	Unencrypted data transmission	No encryption in transit	4	5	20	High
AME022	Loss of mobile devices	No encryption or remote control	4	4	16	High
AME023	Poor permission management	Poorly defined roles	5	4	20	High
AME024	Log failures	Not centralized or reviewed	3	4	12	High
AME025	Uncontrolled printed documents	Visible or poorly stored papers	4	3	12	High
AME026	No continuity plan (BCP/DRP)	Plan does not exist or is untested	4	4	16	Critical

Table 8. Risk treatment plan

ID RISK	Treatment	Description of Action Plan	Controls	Responsible	Residual	Acceptable	Status
AME001	Mitigate	Perform a complete software inventory and ensure license renewal and control.	A.5.31	Legal / IT	LOW	YES	CLOSED
AME002	Mitigate	Establish a preventive maintenance plan and replacement of critical equipment.	A.5.17	Infrastructure	MEDIUM	YES	CLOSED
AME003	Mitigate	Install and test UPS and generators; conduct periodic drills.	A.5.17	Infrastructure	LOW	YES	CLOSED
AME004	Mitigate	Implement multi-factor authentication, define roles, and monitor access.	A.5.15	IT Security	LOW	YES	CLOSED
AME005	Mitigate	Contract alternative providers and configure load balancing.	A.5.28	Network	LOW	YES	CLOSED
AME006	Mitigate	Implement DNSSEC, monitor DNS records, and alert on changes.	A.5.23	Network	MEDIUM	YES	CLOSED
AME007	Mitigate	Define backup policy, automate backups, and conduct regular restoration tests.	A.5.30	Backup / IT	LOW	YES	CLOSED
AME008	Mitigate	Design an annual training program and assess staff knowledge.	A.6.3	HR / CISO	LOW	YES	CLOSED
AME009	Mitigate	Implement change control system and review changes before applying.	A.5.12	DBA / Dev	LOW	YES	CLOSED
AME010	Mitigate	Install cameras, access controls, and visitor logs.	A.5.18	Physical Security	LOW	YES	CLOSED
AME011	Mitigate	Review and improve system logic to avoid overlapping appointments.	A.5.14	QA / Dev	LOW	YES	CLOSED
AME012	Mitigate	Implement automatic update policy and monitor patches.	A.5.14	Systems	LOW	YES	CLOSED
AME013	Mitigate	Establish password policy and enforce mandatory 2FA.	A.5.15	IT Security	LOW	YES	CLOSED
AME014	Mitigate	Create formal procedures and	A.5.24	CISO / Help Desk	LOW	YES	CLOSED

		platforms for incident reporting and tracking.					
AME015	Mitigate	Conduct compliance audits and update privacy policies.	A.5.31	Data Protection	LOW	YES	CLOSED
AME016	Mitigate	Negotiate SLA contracts and define alternative providers.	A.5.19	Procurement / IT	LOW	YES	CLOSED
AME017	Mitigate	Define and enforce BYOD policy with MDM tools.	A.5.22	IT Security	LOW	YES	CLOSED
AME018	Mitigate	Implement antivirus solutions and train staff on phishing.	A.5.20	IT Security	MEDIUM	YES	CLOSED
AME019	Mitigate	Validate and approve software with official certification.	A.5.31	Technology	LOW	YES	CLOSED
AME020	Mitigate	Establish annual calendar for policy review and updates.	A.5.1	CISO / ISMS Committee	LOW	YES	CLOSED
AME021	Mitigate	Implement automatic encryption on emails and files.	A.5.25	IT Security	MEDIUM	YES	CLOSED
AME022	Mitigate	Configure MDM policies for encryption and remote wipe.	A.5.22	IT Mobility	LOW	YES	CLOSED
AME023	Mitigate	Conduct semiannual audits and adjust permissions as needed.	A.5.15	User Administration	LOW	YES	CLOSED
AME024	Mitigate	Centralize logs and define monitoring and alerting procedures.	A.5.12	IT Audit	LOW	YES	CLOSED
AME025	Mitigate	Establish document handling and secure destruction policies.	A.5.10	Archive / Legal	LOW	YES	CLOSED
AME026	Mitigate	Develop a continuity plan and conduct drills regularly.	A.5.29	Business Continuity	LOW	YES	CLOSED

4.3 Information Security Management System compliance assessment and improvement summary

The ISMS Compliance Assessment and Improvement Summary is a process that allows verification of the extent to which the ISMS complies with established policies, objectives, and controls. It consists of measuring key indicators, comparing the initial situation with the results after the implementation of improvements, and analyzing the level of progress achieved. Its purpose is to identify gaps, strengthen information security, and ensure continuous improvement of the system.

Table 9 presents the assessment of ISMS compliance using quantifiable indicators associated with each security policy, comparing the initial situation ("Before") with the results after the implementation of improvements ("After"). The results show consistent and significant progress across all evaluated indicators. A quantitative analysis reveals that the implementation of the ISMS led to improvements ranging from 15% to 40%, with an average increase of approximately 22.7% across all indicators. The most notable improvements were observed in risk management processes and physical security controls, both increasing from 60% to full compliance (100%), representing a 40% improvement. Similarly, database encryption and access control reached full compliance levels, strengthening the protection of sensitive information. In addition, critical operational indicators such as backup success rate improved from 80% to 98%, while system availability increased to 99.95%, exceeding the defined target. User-related metrics, such as patient satisfaction, also showed a significant increase from 75% to 92%, indicating a positive perception of system reliability. Overall, these results demonstrate that the implementation of the ISMS not only improved compliance with security policies but also significantly enhanced the system's operational performance and security posture. This quantitative evidence supports the effectiveness of the proposed approach and reinforces its applicability in real-world healthcare environments.

4.4 Comparative analysis using an approach that does not rely on the Information Security Management System

To strengthen the evaluation of the proposed approach, a comparison was conducted between the implemented ISMS based on ISO/IEC 27001 and a baseline scenario without a structured information security framework. In the baseline scenario, risk management is performed informally, without clearly defined policies, standardized controls, or continuous monitoring mechanisms. As a result, risk identification is incomplete, control implementation is inconsistent, and incident response is primarily reactive. In contrast, the proposed ISMS introduces a structured approach that includes formal risk assessment, security controls, continuous monitoring, and ongoing improvement. This enables proactive risk management and compliance with internationally recognized standards. Table 10 presents a comparative analysis between the non-ISMS approach and the proposed ISMS-based model. As shown in the table, structured ISMS implementation improves risk management practices, enhances control effectiveness, and strengthens compliance with security standards.

The comparison highlights the advantages of the ISMS-based approach over the unstructured model. In particular, standardized controls and continuous monitoring enhance the organization's ability to identify, assess, and mitigate risks. Furthermore, the transition from a reactive to a proactive security model improves incident prevention and strengthens regulatory compliance, especially in environments requiring strict protection of sensitive data, such as healthcare systems.

In this context, adopting an ISMS aligned with ISO/IEC 27001 not only reduces risk levels but also improves overall security posture, operational resilience, and trust in digital services. Finally, while the ISMS approach enhances security conditions, its effectiveness depends on proper implementation, continuous monitoring, and periodic updates, reinforcing the principle of continuous improvement inherent to the standard.

Table 9. Evaluation and improvement of Information Security Management System (ISMS) compliance

Policy / Objective	Indicator	Formula	Target	Before	After
Backup and recovery systems	Backup success rate	(Successful backups / Total scheduled backups) × 100	>= 95%	80%	98%
Risk Management	% of system tests performed	(Tests carried out / Total planned tests) × 100	100%	60%	100%
Database creation	Patient satisfaction with database	(Sum of satisfaction scores / Number of respondents)	>= 90% satisfaction	75%	92%
Database security	% of encrypted patient records	(Encrypted records / Total patient records) × 100	100%	70%	100%
General access security policies	Access compliance rate	(Authorized users with correct access / Total users) × 100	100%	85%	100%
Disaster recovery plans	System uptime (%)	(System active time / Total planned time) × 100	>= 99.9%	98%	99.95%
Physical and environmental safety	% of physical security controls implemented	(Implemented controls / Total required controls) × 100	100%	60%	100%
Policies on use of software licenses	% of licenses up to date	(Renewed licenses / Total licenses) × 100	100%	80%	100%

Table 10. Comparison between non-ISMS approach and ISMS-based approach

Aspect	Non-ISMS Approach	Proposed ISMS Approach
Risk Management	Informal and reactive	Structured and proactive
Security Controls	Undefined or inconsistent	Defined and standardized
Monitoring	Limited or absent	Continuous monitoring
Compliance	Low or not guaranteed	Aligned with standards
Risk Level	Medium-High	Low (after treatment)
Incident Response	Reactive	Preventive and controlled

Note: ISMS = Information Security Management System

5. DISCUSSIONS

The results obtained confirm that the implementation of an ISMS based on ISO/IEC 27001 enables a transformation of security from a reactive approach to a structured, systematic, and proactive one. This shift not only involves the adoption of technical controls, but also the integration of organizational processes focused on continuous risk management. In this regard, the findings are consistent with previous studies that highlight the importance of mechanisms such as encryption, access control, and continuous training as fundamental pillars for protecting information in healthcare environments [29]. Beyond the improvement of specific indicators, these results demonstrate that the coordinated application of controls strengthens security governance and reduces exposure to critical threats. From a risk management perspective, the adoption of a structured approach made it possible to identify, assess, and treat risks systematically, which aligns with the findings [31, 34], where the strategic value of ISO 27001 in organizational decision-making is emphasized. In this context, risk reduction should not be interpreted as its complete elimination, but rather as its control within acceptable levels, in accordance with ISO/IEC 27001 best practices. Furthermore, the application of the continuous improvement cycle (PDCA) demonstrates that information security is a dynamic and evolving process. Continuous improvement allows controls to adapt to technological changes and emerging threats, which is essential to ensure the operational resilience of digital healthcare systems [30]. From an organizational perspective, the results also indicate that the success of ISMS implementation largely depends on institutional commitment and the development of a strong security culture. This is consistent with studies [32, 37], which emphasize that the effective adoption of security standards requires not only technological infrastructure but also strategic alignment and active staff participation. On the other hand, it is observed that strengthening security positively influences the perception of system reliability, which is consistent with the study [35], where it is established that information protection directly impacts user trust in digital healthcare services. This aspect is particularly relevant in contexts where the management of sensitive data requires high levels of credibility and transparency. However, this study presents several limitations that should be considered. First, the ISMS implementation was carried out in a specific environment, which limits the generalizability of the results to other organizations with different technological and operational characteristics. Second, the risk assessment was based on internally defined criteria, which introduces a certain degree of subjectivity, although structured guidelines aligned with ISO/IEC 27001 were applied. Additionally, the measurement of indicators was conducted in the immediate post-implementation phase, without a longitudinal analysis to assess the sustainability of controls over time in the face of evolving threats. Likewise, the study did not include a formal external audit, meaning that the results reflect technical and methodological implementation rather than official certification of the standard. Finally, although improvements in user perception were identified, no inferential statistical models were applied to establish causal relationships between ISMS implementation and user satisfaction. Furthermore, the evaluation of the proposed system was conducted over a relatively short observation period. While the results demonstrate improvements in security and risk management, the long-term stability and sustainability of these improvements cannot yet be fully confirmed. Future work will focus on conducting longitudinal evaluations to assess the performance of the implemented controls over extended periods, considering evolving threat scenarios and system scalability. Additionally, continuous monitoring and periodic reassessment will be essential to ensure that the security posture remains effective over time. This will enable a more robust validation of the proposed ISMS model and strengthen its applicability in dynamic healthcare environments.

6. CONCLUSION

This study presented a structured and technically grounded approach to improving information security management in healthcare systems through the integration of ISO/IEC 27001 principles, risk-based analysis, and a modular system design. The proposed model was successfully applied to a medical appointment system, enabling the systematic identification, assessment, and mitigation of security risks within a real operational environment. The results demonstrate significant improvements in both security performance and system reliability. A quantitative evaluation showed an average improvement of approximately 22.7% across key indicators, with several controls reaching full compliance after implementation. These results are supported by a descriptive statistical analysis of pre- and post-implementation indicators, providing objective validation of the observed improvements. These findings confirm that the proposed model effectively enhances risk management processes and strengthens the protection of sensitive healthcare data. From an engineering perspective, the modular architecture and structured implementation facilitate scalability, interoperability, and adaptation to similar healthcare contexts, particularly in small and medium-sized organizations with limited resources. This positions the proposed model as a practical and replicable solution for real-world ISMS deployment. However, several challenges remain, including integration with legacy systems, user adoption, and the need for continuous monitoring to address evolving cybersecurity threats. Additionally, the study is limited by its short-term evaluation context, which may not fully capture long-term system behavior and stability. Future work will focus on extending the model through long-term validation, the incorporation of automated monitoring mechanisms, and the integration of more advanced risk evaluation techniques to further improve accuracy and robustness. Overall, this study contributes not only a validated implementation framework but also a practical reference model that bridges the gap between theoretical ISMS guidelines and real-world healthcare system requirements.

ACKNOWLEDGMENTS

This work was sponsored by the University of Sciences and Humanities and its Research Directorate. We extend our sincere appreciation for their unconditional support, which was essential to the development of this study. Their commitment to academic research has been a driving force throughout this project. We are deeply grateful for their continued encouragement and trust.

REFERENCES

[1] Li, P., Zhang, L. (2025). Application of big data technology in enterprise information security management. Scientific Reports, 15(1): 1022. https://doi.org/10.1038/s41598-025-85403-6

[2] Salam, M., Abu Bakar, K.A., Mohd Aman, A.H. (2025). Building cyber-resilient universities: A tailored maturity model for strengthening cybersecurity in higher education. International Journal of Advanced Computer Science & Applications, 16(5): 95. https://doi.org/10.14569/IJACSA.2025.0160510

[3] Collante, L.H., Escobar, Y., Acosta, F., Pranolo, A., Prasetya, A. (2023). Preparation of the information security management system implementation based on the NTC-ISO-IEC 27001: 2013 Standard at the IUB university institution. In 2023 IEEE Colombian Caribbean Conference (C3), Barranquilla, Colombia, pp. 1-6. https://doi.org/10.1109/C358072.2023.10436270

[4] Ryanto, K., Tundjungsari, V. (2024). Standardization of information security management in the banking sector using the iso 27001: 2022 framework. Journal La Multiapp, 5(4): 361-379. https://doi.org/10.37899/journallamultiapp.v5i4.1399

[5] Suhartono, B., Asbari, M. (2024). Meningkatkan keamanan informasi melalui sustainable IT capabilities: Studi tentang integrasi information security management dalam organisasi. Journal of Information Systems and Management (JISMA), 3(1): 132-140. https://doi.org/10.4444/jisma.v3i1.1120

[6] Rajagopal, M., Ramkumar, S. (2023). Adopting artificial intelligence in ITIL for information security management—way forward in industry 4.0. In Artificial Intelligence and Cyber Security in Industry 4.0, Singapore: Springer Nature Singapore, pp. 113-132. https://doi.org/10.1007/978-981-99-2115-7_5

[7] Aldulaimi, S. H., Abdeldayem, M., Abu-AlSondos, I. A., Almazaydeh, L., Alnajjar, I.A., Mushtaha, A.S. (2024). Robust information security for strengthening HR in organizations. In 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, pp. 1-5. https://doi.org/10.1109/ICCR61006.2024.10533019

[8] Yoo, C.W., Hur, I., Goo, J. (2023). Workgroup collective efficacy to information security management: manifestation of its antecedents and empirical examination. Information Systems Frontiers, 25(6): 2475-2491. https://doi.org/10.1007/s10796-022-10367-1

[9] Patra, D., Rajagopalan, N. (2025). Integration of emerging technologies in cybersecurity for healthcare: A systematic review. Computers & Security, 161: 104763. https://doi.org/10.1016/j.cose.2025.104763

[10] Virk, A., Alasmari, S., Patel, D., Allison, K. (2025). Digital health policy and cybersecurity regulations regarding artificial intelligence implementation in healthcare. Cureus, 17(3): e80676. https://doi.org/10.7759/cureus.80676

[11] Narayan, S.M., Kohli, N., Martin, M.M. (2025). Addressing contemporary threats in anonymised healthcare data using privacy engineering. NPJ Digital Medicine, 8: 145. https://doi.org/10.1038/s41746-025-01520-6

[12] Fišter, K., Belani, H. (2026). Cybersecurity preparedness and resilience in health care: A narrative review. International Journal of Health Governance, 31(1): 38-49. https://doi.org/10.1108/IJHG-07-2025-0108

[13] Chuma, K.G. (2025). Legacy electronic health record systems as a source of cybersecurity risks in public healthcare facilities. Global Security: Health, Science and Policy, 10(1): 2532556. https://doi.org/10.1080/23779497.2025.2532556

[14] Pool, J., Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A. (2025). Towards a model for understanding failures in health data protection: A mixed-methods study. Behaviour & Information Technology, 45(7): 1381-1406.

https://doi.org/10.1080/0144929X.2025.2551568
[15] Ghahramani, F., Yazdanmehr, A., Chen, D., Wang, J. (2022). Continuous improvement of information security management: An organisational learning perspective. European Journal of Information Systems, 32(6): 1011-1032. https://doi.org/10.1080/0960085X.2022.2096491
[16] Fauzi, R., Sembiring, J. (2023). Information security risk assessment of smart systems: Risk landscape, challenges, and prospective methods. International Conference on ICT for Smart Society, Bandung, Indonesia, pp. 1-6. https://doi.org/10.1109/ICISS59129.2023.10291306
[17] Shiau, W. L., Wang, X., Zheng, F. (2023). Trends and core knowledge in information security: A citation and co-citation analysis. Information & Management, 60(3): 103774. https://doi.org/10.1016/j.im.2023.103774
[18] Li, X. (2023). Research on network information security service model based on user requirements under artificial intelligence technology. In 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA), Shenyang, China, pp. 1568-1572. https://doi.org/10.1109/ICPECA56706.2023.10075946
[19] Abdiraman, A., Goranin, N., Balevicius, S., Nurusheva, A., Tumasonienė, I. (2023). Application of multicriteria methods for improvement of information security metrics. Sustainability, 15(10): 8114. https://doi.org/10.3390/su15108114
[20] Qureshi, R., Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. Applied Sciences, 16(3): 1511. https://doi.org/10.3390/app16031511
[21] Carboni, C., Brightwell, C., Halpern, O., Freyer, O., Gilbert, S. (2025). Reconciling security and care in digital medicine. npj Digital Medicine, 8(1): 261. https://doi.org/10.1038/s41746-025-01685-0
[22] Galety, M.G., Tan, K.T., Kshirsagar, P.R., Polamuri, S.R. (2025). Medical data security and effective organization using integrated Blockchain principles in AI-based healthcare 6.0 infrastructures. Discover Computing, 28(1): 162. https://doi.org/10.1007/s10791-025-09588-0
[23] Taloba, A.I., Rayan, A. (2025). A privacy preserving medical data management framework using blockchain enabled encrypted role based access control. Scientific Reports, 15: 43864. https://doi.org/10.1038/s41598-025-30916-3
[24] Badri, S., Ullah Jan, S., Alghazzawi, D., Aldhaheri, S., Pitropakis, N. (2023). Blockchain-enabled healthcare architecture for information security in the Internet of Medical Things. Computer Systems Science and Engineering, 46(3): 3667-3684. https://doi.org/10.32604/csse.2023.037531
[25] Zyoud, B., Lebai Lutfi, S. (2024). The role of information security culture in zero trust adoption: Insights from UAE organizations. IEEE Access, 12: 72420-72444. https://doi.org/10.1109/ACCESS.2024.3402341
[26] Wang, C., Jiang, W., Yu, Y., Jing, H., Qin, Y., Li, J. (2023). Research on information security of network accounting based on Apriori and AOI algorithms. In 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, pp. 715-719. https://doi.org/10.1109/CSNT57126.2023.10134691
[27] Suprun, A.F., Gar'kushev, A.Y., Lipis, A.V., Karpova, I.L., Shalkovskaya, A.A. (2024). Assessment of the competence of an intelligent information security management system. Automatic Control and Computer Sciences, 58(8): 1429-1435. https://doi.org/10.3103/S0146411624701220
[28] Jevelin, J., Faza, A. (2023). Evaluation the information security management system: A path towards ISO 27001 certification. Journal of Information Systems and Informatics, 5(4): 1240-1256. https://doi.org/10.51519/journalisi.v5i4.572
[29] Shojaei, P., Vlahu-Gjorgievska, E., Chow, Y.W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. Computers, 13(2): 41. https://doi.org/10.3390/computers13020041
[30] Lusmitasari, L., Agustina, T. S. (2025). Information security management systems using ISO 27001:2013 in the industrial revolution 4.0. Transekonomika, 5(2): 363-369. https://doi.org/10.55047/transekonomika.v5i2.866
[31] Kamil, Y., Lund, S., Islam, M.S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden. Information Systems and e-Business Management, 21(3): 699-722. https://doi.org/10.1007/s10257-023-00646-y
[32] Hsu, H.H., Shih, J.R. (2023). ISO 27001 information security survey of medical service organizations. Engineering Proceedings, 55(1): 19. https://doi.org/10.3390/engproc2023055019
[33] Ahouanmenou, S., Van Looy, A., Poels, G. (2023). Information security and privacy in hospitals: A literature mapping and review of research gaps. Informatics for Health and Social Care, 48(1): 30-46. https://doi.org/10.1080/17538157.2022.2049274
[34] 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. https://doi.org/10.1109/CyMaEn57228.2023.10051114
[35] Fernández-Alemán, J.L., Carrión Señor, I., Oliver Lozoya, P.Á., Toval, A. (2023). Security, confidentiality, privacy and patient safety in hospital information systems. International Journal of Medical Informatics, 175: 105066. https://doi.org/10.1016/j.ijmedinf.2023.105066
[36] Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3): 541-562. https://doi.org/10.1016/j.jbi.2012.12.003
[37] Sari, P.K., Handayani, P.W., Hidayanto, A.N., Yazid, S., Aji, R.F. (2022). Information security behavior in health information systems: A review of research trends and antecedent factors. Healthcare, 10(12): 2531. https://doi.org/10.3390/healthcare10122531
[38] Rodríguez-Correa, P.A., Valencia-Arias, A., Martínez Rojas, E., Oré León, A., Mellin Rubio, R.H., Vásquez Coronado, M.H., Jiménez García, J.A. (2025). Information security education: A thematic trend analysis. F1000Research, 14: 5. https://doi.org/10.12688/f1000research.159828.2
[39] Dos Santos, R.F. (2025). Applying zero trust to

Kubernetes clusters. ARIS2 Journal, 5(1): 57-71. https://doi.org/10.56394/aris2.v5i1.58
[40] Gonçalves, E. (2025). Comprehensive analysis for cybersecurity and interoperability in portuguese healthcare systems under NIS2. ARIS2-Advanced Research on Information Systems Security, 5(1): 38-56. https://doi.org/10.56394/aris2.v5i1.59
[41] Elatoubi, M., Tan, X. (2025). Assessing domain specific LLMs for CWEs detections. ARIS2-Advanced Research on Information Systems Security, 5(1): 72-85. https://doi.org/10.56394/aris2.v5i1.53
[42] Lestari, P.S., Tambunan, F.Z., Nasution, A.W., Manurung, M.A., Ropika, Purnama Panjaitan, C.L., Sinaga, D.S. (2025). Implementation of ISO 27001 in improving user trust in the industrial sector. Jurnal Pengabdian Masyarakat dan Riset Pendidikan, 4(1): 1152-1167. https://doi.org/10.31004/jerkin.v4i1.1565
[43] Pilamunga, X.M., Berrones, R.C. (2025). Políticas de seguridad de la información según la norma iso 27001 para el municipio de Guaranda, Bolívar, Ecuador. 593 Digital Publisher CEIT, 10(3): 340-351. https://doi.org/10.33386/593dp.2025.3.3134
[44] Quispe, G.O., Zuloaga, C.K., Castañeda, P.S. (2025). Mitigating information leakage in tech-sector SMEs: Implementing ISO 27001: 2022 for comprehensive security. International Conference on Information Management, 2540: 273-285. https://doi.org/10.1007/978-3-031-99353-4_24
[45] Podrecca, M., Sartor, M., Nassimbeni, G. (2025). Decertification from international management standards: A systematic review and research agenda. The TQM Journal, 37(9): 51-80. https://doi.org/10.1108/TQM-01-2025-0023
[46] Malekolkalami, M., Jabbari, L., Mantegh, H. (2024). Evaluating the status of information security management in academic libraries. Information Security Journal: A Global Perspective, 33(5): 579-592. https://doi.org/10.1080/19393555.2024.2347255
[47] Mera-Amores, F., Roa, H.N. (2024). Enhancing information security management in SMEs through ISO 27001 compliance. Lecture Notes in Networks and Systems, 920: 1-12. https://doi.org/10.1007/978-3-031-53963-3_14
[48] Folorunso, A. (2024). Information security management systems on patient information protection in healthcare. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4955632
[49] Al Hosan, S. (2025). Securing the Flow: A DAMA-ISO 27001 cybersecurity framework for oil & gas data pipelines. In SPE EOR Conference at Oil and Gas West Asia, Muscat, Oman, p. D021S018R006. https://doi.org/10.2118/224951-MS
[50] Haghighat, A., Kalantari, M., Kolahdoozi, M. (2025). Providing a framework to support the analysis and implementation of information security management systems based on the ISO/IEC 27001 ISMS standard in several subsidiary companies of the ministry of roads and urban development. Management Strategies and Engineering Sciences, 7(4): 23-32. https://doi.org/10.61838/msesj.7.4.3
[51] Setyoso, F.A., Mulyana, R., Nugraha, R.A. (2024). Utilizing ISO 27001: 2022 in information security design for SME digital transformation. Ranah Research, 6(6): 2544-2553. https://doi.org/10.38035/rrj.v6i6.1121
[52] Bibi, S., Azam, F., Anwar, M.W. (2024). Implementing ISO 27001 security measures in educational ERP systems. In 2024 14th International Conference on Software Technology and Engineering (ICSTE), Macau, China, pp. 35-39. https://doi.org/10.1109/ICSTE63875.2024.00014
[53] Chavez, S., Anahue, J., Ticona, W. (2024). Implementation of an ISMS based on ISO/IEC 27001: 2022 to improve information security. In 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, pp. 184-189. https://doi.org/10.1109/Confluence60223.2024.10463392
[54] Kreutz, H., Jahankhani, H. (2024). Impact of artificial intelligence on enterprise information security management in the context of ISO 27001 and 27002: A tertiary systematic review and comparative analysis. Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation, pp. 1-34. https://doi.org/10.1007/978-3-031-52272-7_1