TADWIN : Jurnal Ilmu Perpustakaan dan Informasi
Available online at:
https://jurnal.radenfatah.ac.id/index.php/tadwin
https://jurnal.radenfatah.ac.id/index.php
Copyright ©2020, ISSN: 27232409 print/online 2774-8936
Vol. 6 No. 1, June 2025, pages: 141-153
https://doi.org/10.19109/tadwin.v6i1.29814

Evaluation of Information Security Management Based on ISO/IEC 27001 at Universitas Nasional Library (UNAS)

Afifah Nur Fadilah[1*], Dwi Fajar Saputra [2], Ibnu Fyras Maulana[3], Muhammad Jordan A. N[4], Dzaki Rizky Jumayyil[5], Sarah Aurelia T. M[6], Saffana Mufiddah Adhayanti[7], Saffana Mufiddah Adhayanti[8]

[12345678]Sains Informasi, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia
*Email orrespondence: dwifajar@upnvj.ac.id

Information

Submited: 27-05-2025
Revised: 26-06-2025
Accepted: 28-06-2025

How to cite: Evaluation of Information Security Management Based on ISO/IEC 27001 at the UNAS Library. (2025). *TADWIN: Jurnal Ilmu Perpustakaan Dan Informasi, 6* (1), 131-144. https://doi.org/10.19109/tadwin.v6i1.29814

DOI: 10.19109/tadwin.v6i1.29814

First Publication Right:
Tadwin: Jurnal Ilmu Perpustakaan dan Informasi Program Studi Ilmu Perpustakaan, Fakultas Adab dan Humaniora, UIN Raden Fatah Palembang, Indonesia

ABSTRACT

As the utilization of digital systems continues to grow, libraries must strengthen their information management systems to protect against threats such as cyberattacks and data breaches. This study employed a descriptive qualitative approach using interviews, observation, and documentation. The findings indicate that several ISO/IEC 27001 based controls have been implemented, including firewalls, encryption, and regular audits. However, security gaps remain, such as weak credentials, the absence of multi-factor authentication, and limited real-time monitoring and data backup. Major risks include malware, network attacks, and system failures. Although the National University (UNAS) Cyber Library has developed a Disaster Recovery Plan (DRP), improvements in formal documentation and user digital literacy are still needed. These findings serve as a strategic evaluation basis for enhancing the effectiveness of information security governance in academic library environments.

Keywords: *Information Security; ISO/IEC 27001;Library*

1. INTRODUCTION

The rapid advancement of information technology has made information security a critical concern for all institutions, including universities (Cheng & Wang, 2022). Currently, information is a vital asset that must be safeguarded (Farid et al., 2023), with information security referring to the protection of confidentiality, integrity, and availability of data (Rahmat, 2019). Without adequate protection, systems are vulnerable to various threats, ranging from data breaches to cyberattacks that can not only disrupt operations but also affect the institution's reputation (Aslan et al., 2023). University libraries are one of the units that now also rely on information systems to support daily operations (Spring et al., 2022). Digital transformation is driving libraries to act as technology-based information centers (Ikenwe & Udem, 2022), library services are no longer limited to providing physical collections (Ruthven et al.,

Tadwin: Jurnal Ilmu Perpustakaan dan Informasi,
Volume 6 No.1, 2025, Pages. 141-153
DOI: https://doi.org/10.19109/tadwin.v6i1.29814

2023), but also as digital information centers with a crucial role in managing library assets, such as book collections, archives, user identities, and other sensitive data (Onunka et al., 2023).

Information security challenges now stem not only from technical issues but also from weak governance or insufficient internal regulations (Dunn Cavelty & Smeets, 2023). Information security also requires risk management structures, disaster recovery planning, and active involvement of all stakeholders, including service users (AL-Dosari & Fetais, 2023). Therefore, information systems and management are important aspects that must be considered and managed not only to ensure efficient operations (Mehmood, 2021) but also to guarantee the security of stored data (Taherdoost, 2023). To ensure this, the implementation of structured information security management standards is required (Folorunso et al., 2024). One of the most widely used standards is SNI ISO/IEC 27001, which provides a systematic framework for implementing and maintaining an information security management system (ISMS) (Jevelin & Faza, 2023).

Several studies have examined the implementation of ISO/IEC 27001 in the library field. One of them is a study conducted by Bahrudin & Firmansyah (2018), which discusses the implementation of ISO/IEC 27001 in libraries. The results showed that the implementation of this standard can help libraries strengthen information security controls, but they also identified challenges such as insufficient human resources (HR), inadequate infrastructure, and a lack of technical training, which are the main obstacles in the implementation process. Meanwhile, Fattah Ys et al. (2024) conducted research on the National Library of Indonesia, which also noted that the presence of ISO 27001 provides a more structured framework for the National Library. Fattah et al. also highlighted the weakness in information asset documentation, the continued vulnerability to hacker attacks due to insufficient monitoring in information management, and the fact that not all servers have been restored to backup servers.

Both studies provide insights into the benefits and challenges of implementing ISO/IEC 27001 in information security management within library environments. Given the importance of strengthening information security in library environments, this article was written to evaluate the extent to which SNI ISO/IEC 27001 has been implemented in information security management at the National University (UNAS) library. Additionally, this article contributes by providing strategic recommendations to improve the effectiveness of information security management relevant to the actual conditions of the institution. Using a qualitative approach through interviews and observations, this article aims to provide a realistic picture of the level of readiness, obstacles, and opportunities for improving information security.

2. LITERATURE REVIEW

1. ISO/IEC 27001 and Information Security Management System (ISMS)

   ISO/IEC 27001 is an international standard that provides a comprehensive framework for data security management. To protect the confidentiality, integrity, and availability of data, organizations must implement an Information Security Management System (ISMS) in accordance with this standard (International Organization for Standardization, 2013). To protect digital collections, user data, and increasingly digitally integrated information service systems, ISMS is essential for libraries (International Organization for Standardization, 2013). ISO/IEC 27001 enables organizations to systematically identify threats, establish relevant security controls, and conduct regular audits and monitoring of policies. As part of a comprehensive security strategy, this standard covers technical protection in addition to internal policies, operational procedures, and staff instructions. This creates a secure and reliable information environment for all library users.

2. Information Security Governance in Educational Institutions

According to Posthumus & von Solms (2004), management is responsible for regulating and monitoring policies, roles, and processes related to information protection. This task is called information security governance (Posthumus & von Solms, 2004). It includes standard operating procedures (SOPs), routine training, and access control mechanisms in libraries. Galih (2020) states that several factors that can disrupt library system security include firewall failures, inconsistent internal policies, and a lack of staff instructions. As a result, to support the effective implementation of SMKI, governance needs to be strengthened (Galih, 2020).

3. ISO/IEC 27001-Based Library-Related Research

The COBIT (Control Objectives for Information and Related Technologies) framework and ISO/IEC 27001 are two important approaches in supporting information technology governance in organizations, including in library environments. COBIT, developed by ISACA, provides comprehensive guidance for aligning IT strategies with business objectives through risk management, operational monitoring, and security performance evaluation (ISACA, 2019). Meanwhile, ISO/IEC 27001 is an international standard for Information Security Management Systems (ISMS) that focuses on protecting the confidentiality, integrity, and availability of data (CIA triad). This standard uses a risk management approach and the PDCA (Plan-Do-Check-Act) cycle to manage information security comprehensively (International Organization for Standardization, 2013). The integration of both can strengthen the implementation of information security while clarifying the governance structure, roles and responsibilities, and audit and performance measurement systems on a regular basis. In the context of libraries, this synergy enables information systems to be managed strategically and sustainably, in line with the values of transparency and accountability of the institution.

4. Designing a Disaster Recovery Plan (DRP) in Information Institutions

Digital literacy is a key component in the successful implementation of information security, especially in a digital era fraught with risks. This literacy encompasses not only the technical ability to use devices, but also knowledge about cyber threats, data usage ethics, and how to filter data safely. According to San Nicolas-Rocca & Burkhard (2019), digital literacy must be an important component of an organization's security strategy. Digital literacy in libraries means educating employees and users about digital dangers such as account security, data protection, and how to avoid phishing (San Nicolas-Rocca & Burkhard, 2019). According to UNAS Library research, even though security systems have been implemented, people still lack understanding about data security. Therefore, to support a sustainable and comprehensive information security system, regular training, policy socialization, and user training must be promoted.

5. The Role of Digital Literacy and User Education

Studies on the implementation of ISO/IEC 27001 in libraries have shown a significant improvement in data security. According to Bahrudin & Firmansyah (2018), this standard helps strengthen system controls and reduce the risk of data breaches. However, there are challenges such as insufficient technical training and inadequate documentation (Bahrudin & Firmansyah, 2018). Additionally, Fattah Ys et al. (2024) conducted research at the National Library of Indonesia and found that, although most controls have been designed, they are still lacking in terms of asset-based risk assessment and incident handling (Fattah Ys et al., 2024). These results are consistent with the situation at the UNAS Library, where security systems have been implemented with data backup,

firewalls, and system logs, but DRP documentation and incident monitoring are still lacking. This indicates that the implementation of a systematic and managerial approach is crucial for the implementation of ISO 27001.

Perbandingan Manajemen Kelola Sebelum dan Sesudah Implementasi ISO/IEC 27001 di Perpustakaan UNAS

Comparison of Management Before and After the Implementation of ISO/IEC 27001 at the UNAS Library

As a review of two programs in the same research object, this study compares the information security conditions of the National University Library (UNAS) before and after the implementation of the ISO/IEC 27001 standard. This comparison is conducted to assess the effectiveness of changes in policies, infrastructure, and resource readiness implemented alongside the adoption of this international standard. Prior to implementing ISO/IEC 27001, the information security system at the UNAS Library did not have a standardized framework. There were no official regulations regarding password strength, data backup processes were carried out manually and unscheduled, and there was no real-time traffic monitoring system.

In addition, risk documentation and post-incident recovery procedures were not formally regulated, resulting in a high potential for disruption to library services. After the implementation of the standard, a significant transformation took place. The UNAS Library began using a Web Application Firewall (WAF) to protect the system from command injection and XSS attacks, implemented SSL/TLS data encryption, and developed a Disaster Recovery Plan (DRP) framework, although it is still in the advanced documentation stage. Security audits have also been conducted regularly, and the monitoring system has begun to function to detect anomalies in real-time. Although its implementation is still gradual, the system has shown an increase in its capabilities in mitigating information security risks.

The following is a comparison of the information security system before and after the implementation of ISO/IEC 27001:

Table 1. Comparison of Literature Reviews

No	Aspect	Before ISO/IEC 27001	After the Implementation of ISO/IEC 27001
1.	Password Policy	No standard yet	Strong password policy established
2.	Backup System	Manual, unscheduled	Weekly, with backup servers prepared
3.	System Monitoring	Not available	Real-time monitoring with software
4.	Disaster Recovery Plan (DRP))	Not yet available	Organized in a structured plan
5.	Data Protection	No encryption	Use SSL/TLS for data protection
6.	Staff Training	Not yet implemented	Started gradually

An internal comparison at the UNAS Library shows that although not yet fully ideal, the implementation of ISO/IEC 27001 has provided significant direction for improvement in information security management. Analysis of these two system conditions also provides valuable lessons regarding the importance of policy, infrastructure, and human resource readiness in building a robust system.

Tadwin: Jurnal Ilmu Perpustakaan dan Informasi,
Volume 6 No.1, 2025, Pages. 141-153
DOI: https://doi.org/10.19109/tadwin.v6i1.29814

3. RESEARCH METHOD

In this study, the researcher used a descriptive qualitative approach that allowed for more in-depth information to be obtained regarding the implementation and evaluation of ISO/IEC 27001-based information security at the UNAS library. Creswell explains in his book entitled Research Design that qualitative research is an approach to exploring and understanding the meaning given by individuals or groups to a social or human problem involving data collection methods such as interviews, observations, and document analysis, which are then analyzed inductively to form certain themes or patterns (Creswell & Creswell, 2017).

The techniques used in this study to obtain in-depth data to answer the research questions are:

1. Interview

   According to Yusuf (2016), an interview is a process of interaction between an interviewer and an interviewee through direct communication (Yusuf, 2016). Interviews are one of the most commonly used tools in qualitative research. In this study, the interviews conducted by the researcher were structured interviews, where we as researchers created a set of questions, read the questions in order, and recorded the results of the interviews. The interviews were conducted on Thursday, June 19, 2025, at the UNAS Library Digital Library. The selection of informants was entrusted to the UNAS Library, but the researcher's criteria were individuals aligned with the research focus. In this case, the researcher interviewed two librarians from the UNAS Library, Y and R, both of whom were assisted by responses from the UNAS Library and Information Science Department based on questions we had previously submitted.

2. Documentation

   Documentation is a methodology used for data acquisition to facilitate the examination of historical records. Documents related to individuals or collectives, as well as events or incidents in a social context, are highly beneficial for qualitative investigations (Yusuf, 2016). In this study, the researcher used documentation techniques to collect secondary data from journals, archives, and books to support this research.

In this study, the data analysis technique used follows the model proposed by Miles, Huberman, & Saldaña (2014), which divides data analysis into three main activities: data reduction, data display, and drawing conclusions or verification (Miles, Huberman, & Saldaña, 2014).

1. Data Reduction

   Data reduction is conceptualized as a methodological process of selecting and focusing on simplifying, abstracting, and transforming "raw" data derived from field observations. The data reduction process begins concurrently with the initiation of data collection, encompassing activities such as summarization, coding, thematic exploration, and memo composition, among other tasks. The purpose of data reduction is to eliminate extraneous data or information, after which the remaining data undergoes verification.

2. Data presentation

   Data presentation is an explanation of synthesized information that enables the derivation of conclusions and the implementation of actions. Qualitative data representation is articulated in the form of narrative text, with the aim of combining information in a coherent and understandable manner.

3. Drawing conclusions or verification

Conclusions represent a synthesis of research results that articulate final statements based on previous descriptions or determinations obtained through inductive or deductive reasoning methodologies. The conclusions drawn must be related to the research topic, research objectives, and research findings that have been interpreted and discussed. As a result, conclusions in qualitative research can indeed address the problem formulation proposed at the outset; however, they may equally fail to do so, as it has been indicated previously that problems and problem formulations in qualitative research are still tentative and evolving as researchers engage in fieldwork or begin their investigations.

4. RESULTS AND DISCUSSION

This study evaluates how the National University Library (UNAS) implements information security management principles based on the ISO/IEC 27001 framework. The findings are categorized into four main aspects, namely:

Information Security Policies and Procedures

The National University Library (UNAS) has implemented information security policies and procedures that refer to the principles of ISO/IEC 27001. These policies are aimed at maintaining the integrity, confidentiality, and availability of information in the management of digital and physical archives. Some of the main procedures implemented include data encryption, role-based authorization, and real-time system monitoring. The UNAS Library also mandates the use of SSL/TLS to ensure data encryption during transmission, as well as storage encryption to protect sensitive digital archives. To limit access, Role-Based Access Control (RBAC) is implemented to ensure that only users with specific permissions can access or manage data. From a physical security perspective, the UNAS Library strictly controls access to the archive room and limits access to authorized personnel only. The room is equipped with security systems such as CCTV, special locks, and temperature and humidity controls to maintain the condition of physical documents.

Security policies also include routine weekly data backups and the use of early detection systems such as firewalls and Intrusion Detection Systems (IDS) capable of detecting unauthorized access attempts. In the event of a security incident, the UNAS Library has an incident response procedure that begins with incident detection, isolation of the affected system, and system recovery. All incidents are documented for evaluation to prevent similar occurrences. Internal audits are conducted monthly to assess compliance with policies and the effectiveness of implemented controls. Additionally, to support policy implementation, the UNAS Library uses ISMS tools that enable systematic monitoring and reporting of all information security processes.

Organizational Structure and Human Resources Roles

In the implementation of ISO/IEC 27001-based information security management, the organizational structure at the National University (UNAS) Library plays a crucial role in ensuring the effectiveness of security policy implementation. This structure not only outlines responsibility distribution but also supports cross-departmental collaboration to address complex and dynamic information security challenges. The UNAS library has an information systems team consisting of professionals in the fields of IT and information security. This team is responsible for planning, implementing, and monitoring information security controls. They also lead the internal audit process, risk mitigation, and response to security incidents. The main roles of the human resources involved include:

1. System Administrator: Responsible for managing servers, digital archive storage systems, firewalls, and encryption systems. They ensure the stability and security of daily operational systems.
2. Incident Response Team: Actively involved in handling security breaches, from detection, isolation, investigation, to recovery and reporting.
3. Archive Management Officer: Responsible for maintaining the security of physical and digital archives, including ensuring that backup procedures are carried out according to schedule and access protocols are strictly followed.
4. Physical Security and Facility Staff: Ensures surveillance of non-digital archive storage rooms with key systems, access control, and CCTV monitoring.
5. Service Users (end-users): Provided with basic training on account usage policies, safe file upload procedures, and the importance of maintaining personal credential security.

However, interviews revealed that the main challenge still faced is the limited number of personnel specifically assigned to information security management. This requires high work efficiency and collaboration between work units. Therefore, the UNAS Library implements a periodic training strategy to improve staff capacity in understanding and implementing established information security policies. Strengthening the role of human resources is an important foundation in maintaining the integrity of the information security system in the library environment, in line with the principles of people, process, and technology in the ISO/IEC 27001 framework.

Information Security Awareness and Literacy

One important aspect of information security governance at the UNAS Library is user awareness and literacy regarding information security risks and procedures. Based on interviews with the information system management team, it was found that low user awareness is one of the main risk factors in digital archive management. Users often upload files without first verifying their security and use weak credentials, such as easily guessed username and password combinations. This shows that weaknesses do not only originate from technical systems, but also from human factors within the information ecosystem.

The UNAS Library itself has made several efforts to build a culture of security through internal education. For example, strengthening policies on the use of strong passwords and encouraging the use of two-factor authentication (2FA) have been implemented, although not yet comprehensively. However, limitations in formal training and routine socialization have resulted in uneven levels of digital literacy among all members of the academic community. San Nicolas-Rocca & Burkhard (2019) emphasize that information security literacy must be part of comprehensive digital literacy, including understanding cyber risks, ethical practices in the use of information systems, and skills in securing personal and institutional data. In the context of libraries, this literacy is particularly important because users interact directly with digital systems, including accessing electronic collections, storing research data, and managing user accounts.

To address this issue, the UNAS Library is advised to develop a sustainable digital literacy program, for example through online training, educational infographics on the user portal, and periodic outreach on good security practices. This step will not only improve compliance with the ISO/IEC 27001 standard but also create a culture of resilience against cyber threats on campus. This increased awareness will also support the technical effectiveness of the information security systems that have been implemented, such as firewalls, encryption, and real-time monitoring systems. Without risk-aware user

Tadwin: Jurnal Ilmu Perpustakaan dan Informasi,
Volume 6 No.1, 2025, Pages. 141-153
DOI: https://doi.org/10.19109/tadwin.v6i1.29814

behavior, even the most advanced technology remains vulnerable to security breaches due to individual negligence.

Risk Assessment of Information Systems

According to Nugroho & Legowo (2022), risk assessment is a systematic procedure that aims to identify, measure, and prioritize risks in aspects that can be audited in a company (Nugroho & Legowo, 2022). Risk assessment is the initial stage in the development of a Disaster Recovery Plan (DRP) that aims to identify, assess, and evaluate the level of vulnerability and impact of various threats to information assets, in accordance with the ISO 27001 methodology framework that has been widely applied in information security management (Clarissa & Wang, 2023). The information assets at the National University Library (UNAS) include digital archives, user accounts, network systems, and physical collections integrated into the library's information service system.

Risk assessment focuses on cyber threats such as files containing malware, weak credential usage, external attacks on web applications, and physical disruptions to archive rooms. This information was obtained through direct interviews with the information system management team. As part of the risk management process aligned with ISO/IEC 27001, the UNAS Library conducted a risk mapping of key information assets. The purpose was not only for technical identification but also as a basis for developing mitigation policies based on the impact and probability of risks to information service operations. The results are presented in the following table.

Tabel 2. Risk Assessment

No	Threats	Threats	Vulnerabilities	Critical Assets	Consequences	Risk Level
1	Malware files	Files uploaded by users contain viruses/malware.	No automatic filtering during uploads; users do not perform verification	Digital archiving system, servers, network	System disruption, data corruption, risk of malware spread	High
2	Weak credentials	Users use simple usernames/passwords.	No comprehensive strong password enforcement policy	User accounts, user information system	User accounts, user information systems	High
3	Cyber attacks	SQL injection and XSS attempts from external parties.	Limited manual monitoring, WAF not updated	Library web application	Service disruption, compromise of sensitive data	High
4		Power outages or server downtime.	No rapid recovery or automatic failover	Servers, network, data backup	Operational disruption, temporary loss of data access	Moderate
5	System/server failures	Unauthorized access to storage space, risk of disaster.	Limited physical surveillance, access does not use digital logs	Physical archives, server room, non-digital	Damage to collections, loss of archives, operational shutdown	Low-Moderate

				collection s		

The results of the risk assessment indicate that most threats are at a high risk level, highlighting the importance of policy intervention and strengthening managerial procedures. Without integrating risk assessment results into the organization's decision-making structure, security efforts will be reactive and unsustainable. Most risks fall into the high category and need to be addressed in a structured manner. The mitigation measures implemented by UNAS are appropriate, but need to be strengthened through formal DRP documentation, user education, and disaster recovery simulations. Going forward, the integration of log systems, AI-based monitoring, and the strengthening of user policies will be key to creating a library ecosystem that is secure, responsive, and sustainable in the face of disruptions and cyber threats.

Disaster Recovery Plan (DRP) Design

The Disaster Recovery Plan (DRP) is a key element in proactive information security management. In business strategy, a DRP is a plan designed to ensure the operational continuity of an organization's systems and information technology after a disaster or event that threatens the integrity, availability, and security of IT systems (Nur Fa'izi, 2024). A DRP is intended to keep systems operational despite disruptions and to protect information systems from disasters (Wibowo, n.d.).

The findings indicate compliance with the SNI ISO/IEC 27001 standard. The UNAS Library has developed strategic steps in response to operational disruption scenarios that may arise due to technical or non-technical incidents. The following table summarizes the DRP elements designed to ensure the continuity of information services.

Tabel 3. Disaster Recovery Plan

No	Disruption	Obstacles	Recovery Process
1.	System failure or server downtime	a. The server malfunctioned and went down, making it inaccessible to users. b. There was no active backup server. c. Backups were not performed in real time, but only once a week.	a. Activate weekly backup server b. Prepare backup server for faster recovery
2.	Files infected with viruses or malware	a. Users uploaded files without scanning them. b. Not all files were automatically detected by the antivirus.	a. Install automatic scanning system b. Virus removal and restoration from backup
3.	User accounts hacked by illegal access	a. Many users used weak passwords. b. Not all accounts used two-factor authentication. (2FA)	a. Implement strong password policy and 2FA b.b. Reset affected accounts and conduct security audit.
4.	Cyber attacks (SQL injection, XSS, etc.)	a. System protection is not fully equipped with a Web Application Firewall (WAF) b. The system is vulnerable to command injection	a. Activate firewall and Web Application Firewall (WAF) b. Monitoring activities and patching security vulnerabilities

5.	Limited personnel during incidents	a. The number of IT staff is insufficient to respond quickly b. Incident handling requires extra coordination	a. Forming an incident response team b. Incident handling SOPs must be followed appropriately
6.	Physical threats to non-digital archives	a. Room humidity is unstable b. Access to the archive room is not restricted	a. Adjusting the temperature and humidity of the archive room b. Restricting access and installing CCTV
7.	System failure due to human error	a. System misconfiguration b. Accidental deletion of archives by operators	a. Regular training for staff is necessary b. Auditing configurations and recovery backups

The Disaster Recovery Plan (DRP) presented in the table has not been fully documented in the form of formal policies, and periodic simulations have not been conducted to test the readiness of the management team. This indicates that disaster recovery management at UNAS still needs to be strengthened through written SOPs, clear role definitions, and periodic staff training to anticipate potential incidents.

Risk Assessment and Follow-Up Analysis

Based on the results of the evaluation of the implementation of information security management at the National University Library (UNAS), it was found that the institutional approach to risk management and information protection is still in its early stages. Although technical controls such as firewalls, encryption, and the development of a Disaster Recovery Plan (DRP) have been implemented, not all of these efforts have been formalized within a comprehensive policy framework and organizational structure. Therefore, several strategic follow-up actions are needed to strengthen the effectiveness of information security management:

1. Formalization of Information Security Management Policy Documents and SOPs
   It is necessary to develop comprehensive information security policies that cover asset classification, access rights management, system change control, and incident response procedures. All of these policies must be documented, approved by management, and implemented through measurable SOPs so that governance is consistent and standardized.
2. Establishment of an Information Security Organizational Structure
   Currently, there is no formal unit that is fully responsible for overseeing information security. Therefore, the formation of an Information Security Team or Information Security Governance Unit is crucial to ensure the continuity of ISO/IEC 27001 implementation. This team will play a role in coordinating audits, managing risks, educating staff, and reviewing policies on a regular basis.
3. Integration of Risk Assessment into the Strategic Planning Process
   The results of risk assessments have not been optimally used as a basis for strategic decision-making and security resource allocation. An institutional risk register needs to be developed and integrated into the annual planning process and supervised by the university's risk management unit.
4. Strengthening the DRP Function as an Operational Risk Management Policy
   The DRP needs to be regularly updated and tested through incident simulations and the active involvement of all stakeholders. The DRP should not only be a technical response but also part

of the planning for the continuity of information services and the protection of the institution's reputation.

5. Improving Information Security Literacy and Organizational Culture
   The lack of awareness among users and staff regarding security practices is a major challenge. Therefore, continuous training, awareness campaigns, and the integration of information security into human resource development programs must be a permanent agenda in institutional governance.
6. Continuous Institutional Monitoring and Evaluation
   A mechanism for periodic evaluation of security policy implementation, control effectiveness, and unit compliance with ISO/IEC 27001 standards must be established. This evaluation serves as the basis for the continual improvement process as mandated by ISO/IEC 27001:2013.

4. CONCLUSION

Based on the results of an evaluation study on the implementation of information security governance at the National University Library (UNAS), it was found that the institution has taken a number of important initiatives in implementing ISO/IEC 27001-based controls. These include the use of firewalls, encryption systems, system monitoring, and the development of a Disaster Recovery Plan (DRP). However, field findings also indicate that most of these controls are still at the technical stage and are not yet supported by a comprehensive institutional governance structure.

Information security policies are not yet fully documented, there is no formal information security management unit, and the results of risk assessments have not been integrated into the strategic planning process. The DRP that has been developed still requires formal legalization and periodic simulations. On the other hand, the low level of information security literacy among staff and users adds to the challenge of building an adaptive and sustainable security culture. Thus, it can be concluded that the successful implementation of ISO/IEC 27001 depends not only on the adoption of technical controls but also on management's capacity to develop policies, organizational structures, and collective awareness in protecting information assets. Strengthening institutional governance is key to enabling the UNAS Library to realize an effective, sustainable, and resilient information security system in the face of evolving risks.

REFERENCES

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, *12*(17), 3629. DOI 10.3390/electronics12173629

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. DOI 10.3390/electronics12061333

Bahrudin, M., & Firmansyah, F. (2018). Manajemen keamanan informasi di perpustakaan menggunakan Framework SNI ISO/IEC 27001. *Media Pustakawan*, *25*(1), 43-50. DOI 10.37014/medpus.v25i1.191

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192. DOI 10.3390/ info13040192

Clarissa, S., & Wang, G. (2023). *Assessing Information Security Management Using ISO 27001:2013 | Jurnal Indonesia Sosial Teknologi*. DOI 10.59141/jist.v4i9.739

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications. https://books.google.co.id/books?hl=en&lr=&id=335ZDwAAQBAJ

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, *30*(7), 1330-1352. DOI 10.1080/13501763.2023.2173274

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*, 01655515231160026. DOI 10.1177/01655515231160026

Fattah Ys, Moh. A., Parga Zen, B., & Wasitarini, D. E. (2024). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. *Cyber Security Dan Forensik Digital*, *6*(2), 76-82. DOI 10.14421/csecurity.2023.6.2.4190

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, *24*(1), 2582-2595. DOI 10.30574/wjarr.2024.24.1.3169

Galih, A. P. (2020). Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan IPusnas. *AL Maktabah*, *5*(1), 10. DOI 10.29300/mkt.v5i1.3086

Ikenwe, I. J., & Udem, O. K. (2022). Innovative digital transformation for dynamic information service sustainability in university libraries in Nigeria. DOI 10.12775/FT.2022.004

International Organization for Standardization. (2013). *ISO/IEC 27001:2013(en), Information technology—Security techniques—Information security management systems—Requirements*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISACA. (2019). *COBIT | Control Objectives for Information Technologies*, ISACA. https://www.isaca.org/resources/cobit

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. DOI 10.51519/journalisi.v5i4.572

Mehmood, T. (2021). Does information technology competencies and fleet management practices lead to effective service delivery? Empirical evidence from e-commerce industry. *International Journal of Technology Innovation and Management (IJTIM)*, *1*(2), 14-41. DOI 10.54489/ijtim.v1i2.26

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). Arizona State University. https://books.google.co.id/books?id=p0wXBAAAQBAJ

Nugroho, A. R., & Legowo, N. (2022). Risk Assessment at it Company by Focusing on Information Security Area Using Iso 27001:2022. *Syntax Literate; Jurnal Ilmiah Indonesia*, *7*(12), 20307–20324. https://jurnal.syntaxliterate.co.id/index.php/syntax-literate/article/view/15349

Nur Fa'izi, M. B. (2024, October 17). *Strategi Pentingnya Disaster Recovery Plan dalam IT Bisnis*. https://cyberhub.id/pengetahuan-dasar/disaster-recovery-plan

Onunka, O., Onunka, T., Fawole, A. A., Adeleke, I. J., & Daraojimba, C. (2023). Library and information services in the digital age: Opportunities and challenges. *Acta Informatica Malaysia*, *7*(1), 113-121. DOI 10.26480/aim.02.2023.113.121

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23* (8), 638-646. DOI 10.1016/j.cose.2004.10.006

Rahmat, D. (2019). Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar Sni Iso/Iec 27001: 2013. *COMPUTING | Jurnal Informatika*, *6* (2), 37-41. DOI 10.55222/computing.v6i2.203

Ruthven, I., Robinson, E., & McMenemy, D. (2023). The value of digital and physical library services in UK public libraries and why they are not interchangeable. *Journal of Librarianship and Information Science*, *55*(4), 1143-1154. DOI 10.1177/09610006221127027

San Nicolas-Rocca, T., & Burkhard, R. J. (2019). Information Security in Libraries. *Information Technology and Libraries*, *38*(2), 58–71. DOI 10.6017/ital.v38i2.10973

Spring, M., Faulconbridge, J., & Sarwar, A. (2022). How information technology automates and augments processes: Insights from Artificial-Intelligence-based systems in professional service operations. *Journal of Operations Management*, *68*(6-7), 592-618. DOI 10.1002/joom.1215

Taherdoost, H. (2023). An overview of trends in information systems: Emerging technologies that transform the information technology industry. *Taherdoost, H. (2023). An overview of trends in information systems: emerging technologies that transform the information technology industry. Cloud Computing and Data Science*, 1-16. DOI 10.37256/ccds.4120231653

Wibowo, A. M. (n.d.). *Business Continuity Plan & Disaster Recovery Plan*.

Yusuf, A. M. (2016). *Metode penelitian kuantitatif, kualitatif & penelitian gabungan*. Prenada Media. https://books.google.co.id/books?id=RnA-DwAAQBAJ