Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

ISO 27001 Readiness: Information security practices and implementation challenges in higher education institutions

Esli Joy N. Fernando *

Graduate School, University of La Salette, Inc., Santiago City, Philippines.

Global Journal of Engineering and Technology Advances, 2026, 26(03), 244-256

Publication history: Received on 18 February 2026; revised on 26 March 2026; accepted on 28 March 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.26.3.0072

Abstract

This study was conducted to assess the Information Security practices in Higher Education. The descriptive method was used with a questionnaire as the main tool in gathering data for the study. Statistical tools such as the weighted mean were used in analyzing and interpreting the data gathered. The research was conducted within all nine private higher education institutions located in the Santiago City. The study's findings indicate that respondents perceive their institution as consistently implementing information security practices aligned with ISO/IEC 27001 standards across key domains, including risk assessment, security organization, asset management, human resource security, communications and operations management, access control, system development, incident management, and compliance. Nevertheless, the respondents also identified slight challenges in all nine areas. This suggests that although policies and procedures are in place, their operational maturity and consistency require further development to achieve full alignment with ISO 27001. Addressing these gaps is critical to enhancing the institution's resilience, particularly in the context of evolving cybersecurity threats.

Keywords: Information Security; Higher Education Institutions (HEIS); Digitalization; Cybersecurity; Data Protection and Information Systems Security

1. Introduction

In today's digital age, computers and information systems have revolutionized industries worldwide, including banking, healthcare, retail, and education. The rapid advancement of technology has significantly enhanced efficiency, accessibility, and communication, making digitalization an integral part of modern institutions. Higher education institutions, in particular, rely heavily on digital infrastructure to manage academic records, research data, financial transactions, and administrative operations.

However, as educational institutions embrace digital transformation, they also become prime targets for cyber threats. Cyberattacks, such as data breaches, phishing scams, ransomware, and hacking incidents, pose a significant risk to the confidentiality, integrity, and availability of institutional data. The unauthorized access and exploitation of sensitive information, including student records, faculty research, and financial data, can have severe consequences, leading to financial loss, reputational damage, and disruptions in academic activities.

The growing reliance on cloud computing, online learning platforms, and interconnected systems further amplifies the vulnerability of higher education institutions to cyber threats. Despite implementing security measures, many institutions struggle to keep pace with the evolving nature of cyber risks. Addressing these challenges requires a proactive approach, combining robust information security policies, advanced technological safeguards, and user awareness to strengthen institutional resilience against digital threats.

* Corresponding author: Esli Joy N. Fernando

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution 4.0.

This study aims to examine the information security environment in higher education, highlighting the key challenges posed by digitalization and exploring strategies to mitigate risks. By understanding the current information security situation and identifying best practices, this research seeks to contribute to the development of effective security frameworks that ensure the protection of institutional data and the continuity of academic operations in the face of threats.

Background of the Study

Higher education has undergone a transformative shift with the pervasive integration of digital technologies (Akour and Alenes, 2022). Santiago City, situated at the intersection of education and technology, reflects this dynamic evolution. As academic institutions increasingly rely on digital platforms for communication, collaboration, and information dissemination, the vulnerability of the cyber environment becomes a critical concern. Cyber threats, ranging from data breaches to ransomware attacks, pose significant challenges to the integrity and confidentiality of sensitive information within these educational institutions.

The significance of information security in higher education cannot be overstated, as it not only safeguards institutional data but also upholds the trust and confidence of students, faculty, and stakeholders. Recognizing the need for a comprehensive understanding of the current state of information security practices in higher education institutions, this research focuses in Santiago City. Through assessing the existing information security measures even though institutions are not yet ISO 27001 certified, the study aims to identify potential risks, vulnerabilities, and areas for improvement, contributing to the resilience of the educational system.

In the context of Santiago City, which serves as a microcosm of broader technological trends, this research seeks to bridge the gap between the rapid evolution of cyber threats and the need for robust information security infrastructure in higher education. The insights gained from this study are anticipated to inform strategic decision-making, policy formulation, and the implementation of proactive measures to ensure a safe and secure cyber environment within the higher education institutions of Santiago City. As educational institutions continue to embrace digital innovation, this research endeavors to provide a foundation for sustaining a resilient and secure academic system.

1.1. Research Questions

This research aims to determine the readiness in ISO 27001- information security practices and implementation challenges of higher education institutions. Specifically, it seeks to answers the following:

What are the practices of the higher educational institution on information security based on ISO27001 standards:

- Risk assessment;
- Organizing information security;
- Asset management;
- Human resource security;
- Communications and operations management;
- Access control;
- System development and maintenance;
- Information security incident management;
- Compliance
- What are the challenges encountered of the Higher Education Institution in the implementation of ISO27001 standards?
- What can be recommended to enhance information security resilience in higher education institutions within Santiago City?

1.2. Theoretical Background

1.2.1. Conceptual Framework

- The evaluation will contribute to the creation of a secure digital space conducive to the pursuit of knowledge and academic excellence in Santiago City's higher education institutions.
- The input load consists of practices of the higher educational institution on information security based on ISO27001 standards and challenges encountered of the Higher Education Institution in the implementation of ISO27001 standards.

- The process load contains the information security assessment, stakeholder surveys and interviews, and data collection and analysis.
- The output load consists of the proposed measures for improving information security measures of higher education institutions in the Santiago City.

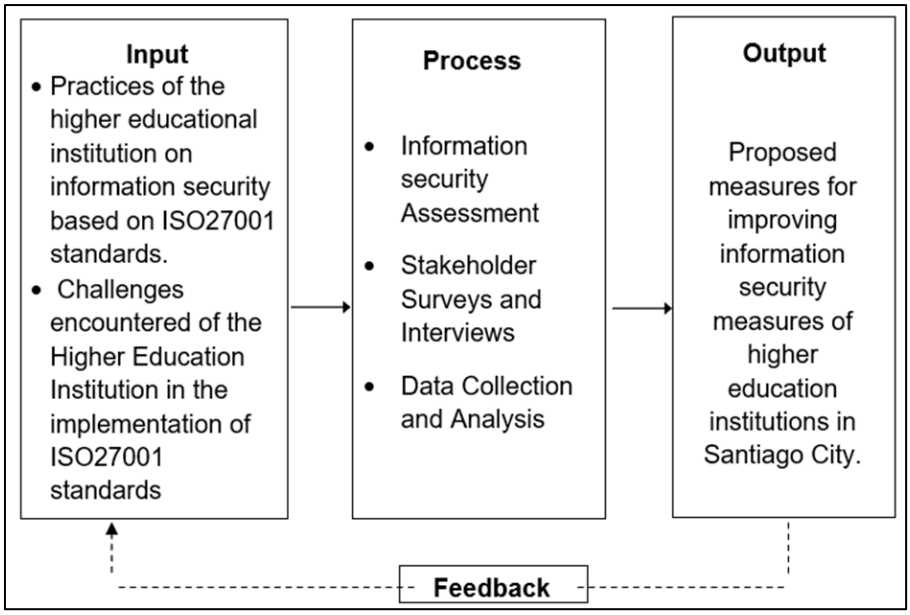

Figure 1 The Schematic Paradigm of the Study

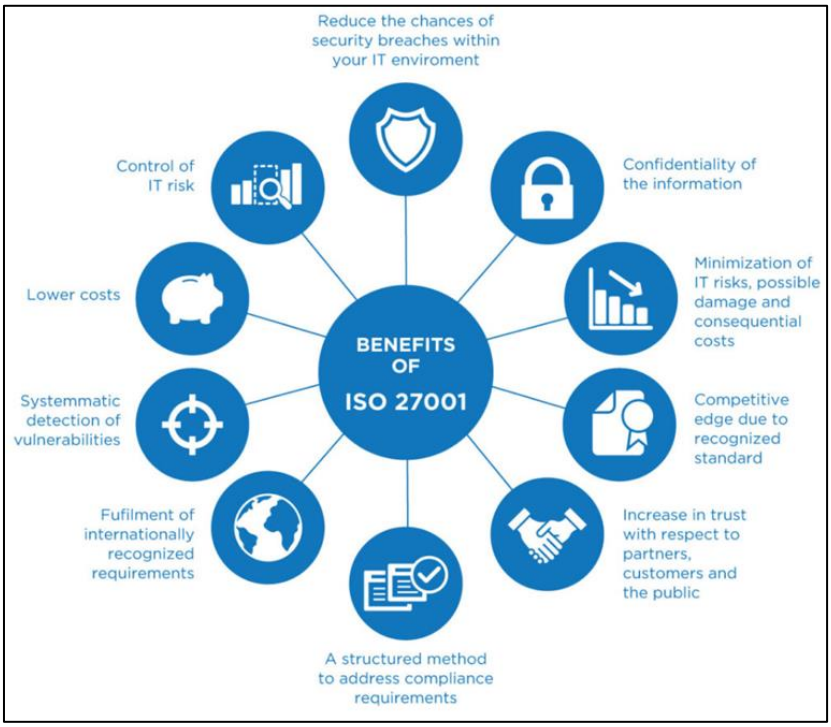

Figure 2 ISO 27001 Framework

Table 1 ISO 27001 Domains

Domain	Variable	Definition
Risk Assessment	Risk Assessment Practices	The systematic process of identifying, analyzing, and evaluating risks to information assets.
Organizing Information Security	Security Governance Structure	The establishment of roles, responsibilities, and organizational structures to manage and coordinate information security activities
Asset Management	Asset Identification and Classification	The process of recognizing, categorizing, and managing information and physical assets
Human Resource Security	Personnel Security Measures	Policies and practices ensuring that employees, contractors, and third parties understand and fulfill their information security responsibilities.
Communications and Operations Management	Operational Security Controls	Implementation of procedures and technologies to safeguard information during processing, storage, and transmission.
Access Control	Access Restriction and Monitoring	Mechanisms that regulate user access to systems and data.
System Development and Maintenance	Secure Development Lifecycle	Integration of security requirements into system design, development, testing, and maintenance.
Information Security Incident Management	Incident Response and Reporting	The structured process for detecting, reporting, analyzing, and responding to information security incidents.
Compliance	Regulatory and Policy Adherence	Ensuring conformity with ISO/IEC 27001 standards, institutional policies, and applicable legal and regulatory requirements.

The framework presented above is anchored on the nine core domains of information security as outlined in ISO/IEC 27001 standards. Each domain is treated as a variable that defines the essential components of an effective Information Security Management System (ISMS) within Higher Education Institutions. Risk assessment emphasizes the systematic identification, analysis, and evaluation of threats to institutional assets, ensuring that mitigation strategies are aligned with organizational objectives. Organizing information security highlights the importance of governance structures, role clarity, and accountability in managing security practices. Asset management focuses on the identification, classification, and protection of both information and physical resources to maintain integrity and availability. Human resource security underscores the role of personnel policies and practices in embedding information security responsibilities across all stages of employment. Communications and operations management ensures that daily processes, including storage, transmission, and operational continuity, are safeguarded through appropriate controls. Access control represents the mechanisms for restricting and monitoring user access to systems and data, ensuring that only authorized individuals can interact with sensitive information. System development and maintenance integrates security requirements into the lifecycle of IT systems, from design to testing and ongoing updates, to prevent vulnerabilities. Information security incident management provides structured processes for detecting, reporting, and responding to breaches, minimizing their impact and preventing recurrence. Finally, compliance ensures adherence to ISO/IEC 27001 standards, institutional policies, and applicable legal and regulatory requirements through monitoring and enforcement. Taken together, these domains form a comprehensive framework that allows institutions to assess both their practices and challenges, positioning ISO 27001 readiness not merely as policy adoption but as the degree to which these domains are operationalized, monitored, and embedded into organizational culture.

2. Literature Review

Bianco and Manahan (2024) stated that in response to the escalating demands of the Information and Communications Technology (ICT) sector, the Philippine Department of ICT announced the National Information security Plan (NCSP) 2022 in May 2017. Amid rising cyber threats targeting the BPO and Offshore Gaming sectors, the NCSP 2022's robust framework is crucial for national economic security. The critical nature of this plan highlights its foundational role in national development, propelled by an increasing dependency on ICT solutions. This study aims to rigorously evaluate the alignment of the NCSP 2022 with the International Telecommunications Union's Global Information security Agenda

(GCA) through a comprehensive benchmarking of its five pillars: legal measures, technical and procedural measures, organizational structure, capacity building, and international cooperation. Using a mixed-methods approach, this study combines quantitative data from an extensive spectrum of scholarly articles, official reports, and industry standards on information security, supplemented by qualitative insights from expert interviews. The findings reveal that while the NCSP 2022 excels in Organizational Structure and Capacity Building, it requires Legal Measures and International Cooperation improvements. Regardless, the assessment yielded an impressive cumulative compliance score of 88.5%, showing a significant adherence to the GCA standards. Despite its robust alignment with global benchmarks, the findings underscore the need for policymakers to prioritize the development of a information security legislative framework, offering professionals more straightforward guidelines for compliance.

Aquino and Noroña (2021) stated that information security devices such as anti-virus, intrusion detection, and prevention system, firewall, network access control, are reactive responses to cyber-attacks because it is based on the known signature. However, security analytics and security information, and event manager are devices, that can gather data about the historical behavior of attacks and correlate it to one another. The significance of this research is to precisely predict if an attack were about to happen, many industries only act if an attack was already happening inside their network or has done significant damages already to the business. This research would significantly help industries, to gain insights on the security events on their network. Artificial Intelligence can instantly predict and suggest if a person can potentially harm based on people's record of good behavior. This can be related to a computer's normal pattern of behavior in the network and once an anomaly happens an unusual behavior can be detected. Hence, the best application of Artificial Intelligence in Cyber Security is to put out a fire before it spread out, preventing data breaches that can cause damages to people's lives and material assets.

According to Pamela et al. (2021) information security constitutes a new field of expertise in the Philippines. There are many international information security laws that have an impact on Philippine businesses. The European Union (EU) Information security Act entered into force on June 27, 2019. The act has these effects: the EU Information security Agency was established; the creation of a information security certification framework. This framework is meant to set the compliance standards for companies that are operating in EU countries. The Association of Southeast Asian Nations (ASEAN) Blueprint for the Political-Security Community 2025 called for the strengthening of cooperation between member states in combating cybercrimes, and developing and improving relevant laws and capabilities to address cybercrime issues and enhance information security. There is an ongoing US–ASEAN Cyber Dialogue which is meant to advance collaboration on this front. Cyber issues are significant for ASEAN countries. The Philippine Government has recognized the importance of instituting mechanisms aimed at providing a conducive environment in ICT.

Rotas and Cahapay (2021) mentioned that amid the current period of massive migration to remote learning, it can be practically assumed in the context of cyber security that giving students threat knowledge will increase their protective behaviors. An emerging stance in behavior theories, however, offer an interesting ground on the dissociation between knowledge and behavior. This article is a preliminary study with the aim to test if threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid the COVID-19 crisis. Gathering data from a sample of students from a teacher education department of a Philippine university, modified questionnaires were used in online surveys. The results revealed that the students are somewhat knowledgeable about the possible threats and they sometimes practice protective behaviors in remote learning. This indicates a practical need to heighten the cyber security of the students. This study further found no significant relationship between threat knowledge and protective behaviors of the students. While this outcome contributes a piece of evidence in the current debate in behavior theories, further validation in other contexts is necessary.

3. Methods

This section shows the data gathering procedure used by the researcher to further show the objective of the study and the methods used in the development of the study.

3.1. Research Design

This study used the descriptive method of research. Descriptive research aims to accurately and systematically describe a population, situation or phenomenon. It can answer questions such as what, where, when and how questions. A descriptive research design may employ a wide variety of research methods to investigate one or more variables. Unlike in experimental research, the researcher does not control or manipulate any of the variables, but instead only observes and measures them.

3.2. Study Site and Participants

The research was conducted within the higher education institutions located in the Santiago City. The Santiago City, with its diverse educational site, serves as an ideal setting to investigate the information security practices within higher education. The selection of this city allows for a nuanced understanding of the dynamics and variations in information security preparedness among educational institutions.

3.3. Population, Sample Size and Sampling Method

The population of interest for this study comprises higher education institutions within the Santiago City. This includes universities, colleges, and other tertiary education institutions operating in the city.

Given the potentially extensive number of higher education institutions in the City of Santiago, a representative sample was selected to balance the need for comprehensive insights with practical research constraints. The respondents were the Director of Management Information System, and Information Technology (IT) technical personnel from each selected institution.

Table 2 Sample Size Distribution of Respondents

Director of Management Information System (MIS)	Information Technology (IT) technical personnel
9	20

3.4. Research Instrument

This study used survey questionnaires to gather quantitative data on the implementation of information security protocols, awareness levels, and challenges faced by faculty and administrators.

The questionnaire is adapted from (Standardized ISO 27001) Torregosa, Jet al. (2021) in their study assessing the conformity level of information security management system of the higher education institutions: Basis for the development of policies and guidelines. Published in Mediterranean Journal of Basic and Applied Sciences (MJBAS).

A Likert scale was used in rating the evaluation where in respondents are asked to express their agreement or disagreement on the relevance with the questions. The scale has the following descriptions:

Table 3 Qualitative Description of the Level of Practice

Scale	Range	Qualitative Description
4	3.25 - 4.00	Always Practiced
3	2.50 – 3.24	Often Practiced
2	1.75 – 2.49	Sometimes Practiced
1	1.00 – 1.74	Never Practiced

Table 4 Qualitative Description of the Level of Challenges

Scale	Range	Qualitative Description
4	3.25 - 4.00	Greatly Challenged
3	2.50 – 3.24	Moderately Challenged
2	1.75 – 2.49	Slightly Challenged
1	1.00 – 1.74	Not Challenged

3.5. Data Gathering Procedures

Firstly, the researcher sought approval to the conduct the study. Secondly, the respondents were informed about the purpose of the study and was invited to participate in the survey. Thirdly, after getting their consent, the researcher distributed the survey. Respondents were given sufficient time to answer the questions.

3.6. Data Analysis

- The data collected were classified, tabulated, and encoded in for analysis. Weighted mean and rank were employed to interpret the data obtained from the survey.
- Weighted Mean was utilized to determine the perception of the respondents on the extent of compliance to the ISO27001.
- Rank was utilized in determining the pressing challenges encountered by the Higher Education Institution in the Implementation of ISO27001 Standards.

3.7. Ethical Considerations

The participants will be given complete information about the nature of the study through a written informed consent form, and the researcher will protect their right to self-determination. The research data, as well as the participants' identities and privacy, will remain highly confidential and their anonymity will be protected.

4. Results and Discussion

This section presents data analysis and interpretation of data gathered from the questionnaire used.

4.1. Part 1. Practices of Higher Education Institution on Information Security Based on ISO27001 Standards

Information security ISO27001 are classified in terms of risk assessment, organizing information security, asset management, human resource security, communications and operations management, access control, system development and maintenance, information security incident management, and compliance.

4.2. Risk Assessment

Table 5 presents show the mean scores of responses on risk assessment practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 5 Risk Assessment

Risk Assessment	M	Interpretation
Designated personnel are responsible for implementing risk management processes.	4.00	Always Practiced
Risk assessments are conducted annually and during significant system changes.	3.80	Always Practiced
HEI's approach to security is based on regular risk assessments.	3.60	Always Practiced
Recognized methods like information security, information security and privacy protection of ISO/IEC 27001 are used in risk evaluations.	3.40	Always Practiced
Management approves risk assessments and ensures mitigation for unacceptable risks.	3.40	Always Practiced
Composite Mean	3.64	Always Practiced

As presented in Table 5, the respondents agreed that the following aspects of information security in terms of risk assessment is always practiced in their institution: designated personnel are responsible for implementing risk management processes (4.00), risk assessments are conducted annually and during significant system changes (3.80), HEI's approach to security is based on regular risk assessments (3.00), recognized methods like information security, information security and privacy protection of ISO/IEC 27001 are used in risk evaluations (3.40) and management approves risk assessments and ensures mitigation for unacceptable risks (3.40). With a composite mean of 3.64, it implies that the Higher Education Institution always practice information security in terms of risk assessment.

4.3. Security Organization in the HEI

Table 6 shows the mean of responses on security organization practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 6 Security Organization in the HEI's

Security Organization in the HEI's	M	Interpretation
Projects follow HEI's manual, integrating information security protocols.	4.00	Always Practiced
Responsibility for research-related data is assigned to appropriate academic leaders.	4.00	Always Practiced
The President, MIS Director, and HR Director each have defined security responsibilities.	3.80	Always Practiced
Information security is regularly reviewed with internal or external audits.	3.80	Always Practiced
Composite Mean	3.90	Always Practiced

As presented in Table 6, the respondents agreed that the practice of information security in terms of security organization are always practiced in their institution. Among the indicators, projects follow the HEI's manual and integrating information security protocols (4.00) and the responsibility for research-related data being assigned to appropriate academic leaders. (4.00) were rated the highest. It is followed by having defined security responsibilities for the President, MIS Director, and HR Director (3.80), as well as the regular review of information security through internal or external audits (3.80). With a composite mean of 3.90, the findings imply that the Higher Education Institution always practices information security in terms of security organization.

4.4. Asset Management

Table 7 shows the mean of responses on asset management practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 7 Asset Management

Asset Management	M	Interpretation
Sensitive documents are clearly labelled and stored securely.	4.00	Always Practiced
Both information and physical assets are classified by confidentiality and criticality.	3.80	Always Practiced
Classification routines and risk analysis protocols are developed and followed.	3.80	Always Practiced
Information remains accessible regardless of system changes.	3.60	Always Practiced
Users handle information in accordance with its assigned classification level.	3.60	Always Practiced
Composite Mean	3.76	Always Practiced

As presented in Table 7, the respondents agreed that the following aspects of information security in terms of asset management are always practiced in their institution: sensitive documents are clearly labeled and stored securely (4.00), both information and physical assets are classified by confidentiality and criticality (3.80), and classification routines and risk analysis protocols are developed and followed (3.80). These were followed by ensuring that information remains accessible regardless of system changes (3.60) and users handle information in accordance with its assigned classification level (3.60). With a composite mean of 3.76, it implies that the Higher Education Institution always practices information security in terms of asset management.

4.5. Human Resource Security

Table 8 shows the mean of responses on human resource security practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 8 Human Resource Security

Human Resource Security	M	Interpretation
Security roles and responsibilities are clearly defined for all employees.	4.00	Always Practiced
Clear routines exist for managing employment changes and asset returns.	4.00	Always Practiced
Background checks and confidentiality agreements are standard practice.	3.80	Always Practiced
Employees are trained on information security policy and procedures.	3.80	Always Practiced
Access rights are updated or terminated based on employment status.	3.80	Always Practiced
Notifications are handled through defined personnel procedures.	3.80	Always Practiced
Misuse or breach of policy may lead to disciplinary actions.	3.60	Always Practiced
Use of IT resources must align with HEI's purpose and policy.	3.40	Always Practiced
IT regulations are included in employment contracts and third-party access agreements.	3.20	Often Practiced
IT regulations are reviewed regularly with staff and new hires.	3.00	Often Practiced
Composite Mean	3.64	Always Practiced

As presented in Table 8, the respondents agreed that several aspects of information security in terms of human resource security are always practiced in their institution. The highest-rated indicators include security roles and responsibilities are clearly defined for all employees (4.00) and clear routines exist for managing employment changes and asset returns (4.00). These are followed by background checks and confidentiality agreements are standard practice (3.80), employees are trained on information security policy and procedures (3.80), access rights are updated or terminated based on employment status (3.8), and notifications are handled through defined personnel procedures (3.80).

Other indicators that are still positively observed but rated slightly lower include misuse or breach of policy may lead to disciplinary actions (3.60) and use of IT resources must align with HEI's purpose and policy (3.40). Meanwhile, the respondents assessed that IT regulations are included in employment contracts and third-party access agreements (3.20) and IT regulations are reviewed regularly with staff and new hires (3.00) are often practiced. With a composite mean of 3.64, the findings imply that the Higher Education Institution generally always practices information security in terms of human resource security.

4.6. Communications and Operations Management

Table 9 shows the mean of responses on communications and operations management practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 9 Communications and Operations Management

Communications and Operations Management	M	Interpretation
IT purchases and installations must be approved by the MIS department.	3.80	Always Practiced
Changes to systems follow documented procedures and risk assessments.	3.80	Always Practiced
Regular backups, anti-virus protections, and emergency plans are maintained.	3.60	Always Practiced
Access and system use are logged and monitored for security incidents.	3.60	Always Practiced
Information exchange and storage follow security guidelines, including encryption.	3.60	Always Practiced
Composite Mean	3.68	Always Practiced

As presented in Table 9, the respondents agreed that the following aspects of information security in terms of communications and operations management are always practiced in their institution: IT purchases and installations must be approved by the MIS department (3.80) and changes to systems follow documented procedures and risk assessments (3.80). These are followed by regular backups, anti-virus protections, and emergency plans are maintained (3.60), access and system use are logged and monitored for security incidents (3.60), and information exchange and storage follow security guidelines, including encryption (3.60). With a composite mean of 3.68, this implies that the

Higher Education Institution always practices information security in terms of communications and operations management.

4.7. Access Control

Table 10 shows the mean of responses on Access Control practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 10 Access Control

Access Control	M	Interpretation
Access control guidelines are regularly updated and enforced.	4.00	Always Practiced
Sensitive data on mobile/portable devices must be encrypted.	4.00	Always Practiced
Access is based on "need to know" principles and role-specific permissions.	3.80	Always Practiced
Remote access requires approved security measures and signed policies.	3.80	Always Practiced
Users must use unique credentials and protect their login information.	3.60	Always Practiced
Composite Mean	3.84	Always Practiced

As presented in Table 10, the respondents agreed that the following aspects of information security in terms of access control are always practiced in their institution: access control guidelines are regularly updated and enforced (4.00) and sensitive data on mobile/portable devices must be encrypted (4.00). These are followed by access is based on "need to know" principles and role-specific permissions (3.80) and remote access requires approved security measures and signed policies (3.80). In addition, users must use unique credentials and protect their login information (3.60) was also assessed as always practiced. With a composite mean of 3.84, it implies that the Higher Education Institution always practices information security in terms of access control.

4.8. System Development and Maintenance

Table 11 shows the mean of responses on system development and maintenance practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 11 System Development and Maintenance

System Development and Maintenance	M	Interpretation
Security requirements are defined for new systems and changes.	3.80	Always Practiced
Encryption guidelines and formal change management are followed.	3.80	Always Practiced
All software is tested and approved before deployment.	3.80	Always Practiced
Risk assessments are done for systems classified as "high."	3.80	Always Practiced
Composite Mean	3.80	Always Practiced

As presented in Table 11, the respondents agreed that all aspects of information security in terms of system development and maintenance are always practiced in their institution. These include security requirements are defined for new systems and changes (3.80), encryption guidelines and formal change management are followed (3.80), all software is tested and approved before deployment (3.80), and risk assessments are done for systems classified as "high" (3.80). With a composite mean of 3.80, the results indicate that the Higher Education Institution always practices information security in terms of system development and maintenance.

4.9. Incident Management

Table 12 shows the mean of responses on incident management practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 12 Incident Management

Incident Management	M	Interpretation
Employees report breaches and incidents immediately.	4.00	Always Practiced
Incident management routines include damage control and prevention.	3.80	Always Practiced
Continuity and contingency plans are tested and maintained.	3.80	Always Practiced
Cost of security incidents is monitored by the MIS Director.	3.80	Always Practiced
Composite Mean	3.85	Always Practiced

As presented in Table 12, the respondents agreed that the following aspects of information security in terms of incident management are always practiced in their institution. The highest-rated indicator was employees report breaches and incidents immediately (4.00). This was followed by incident management routines include damage control and prevention (3.80), continuity and contingency plans are tested and maintained (3.8), and cost of security incidents is monitored by the MIS Director (3.80). With a composite mean of 3.85, the findings indicate that the Higher Education Institution always practices information security in terms of incident management.

1.9 Compliance

Table 13 shows the mean of responses on compliance practices of Higher Education Institution on Information Security based on ISO27001 Standards.

Table 13 Compliance

Compliance	M	Interpretation
All stakeholders comply with information security policies and IT regulations.	3.60	Always Practiced
Evidence from incidents may be handed to authorities when needed.	3.60	Always Practiced
Security audits are conducted with minimal disruption to HEI operations.	3.60	Always Practiced
Composite Mean	3.60	Always Practiced

As presented in Table 13, the respondents agreed that compliance with information security are always practiced in their institution. These include all stakeholders comply with information security policies and IT regulations (3.60), evidence from incidents may be handed to authorities when needed (3.60), and security audits are conducted with minimal disruption to HEI operations (3.60). With a composite mean of 3.60, this implies that the Higher Education Institution always practice information security in terms of compliance.

4.9.1. Part II. Challenges Encountered by the Higher Education Institution in the Implementation of ISO27001 Standards

Table 14 shows the mean of responses on challenges encountered by the Higher Education Institution in the Implementation of ISO27001 Standards.

Table 14 Challenges Encountered by the Higher Education Institution in the Implementation of ISO27001 Standards

Challenges	M	Interpretation
Risk Assessment Our institution lacks a systematic and consistent process for conducting risk assessments.	2.00	Slightly Challenged
Security Organization There is inadequate definition and assignment of roles for information security.	2.00	Slightly Challenged
Asset Management Assets (information and physical) are not properly identified, classified, or managed.	2.00	Slightly Challenged
Human Resource Security	2.20	Slightly Challenged

Information security roles and responsibilities are not clearly communicated to employees.		
Communications and Operations Management Backup, recovery, and operational controls are not sufficiently implemented.	2.20	Slightly Challenged
Access Control Access to systems and data is not adequately restricted or monitored.	2.40	Slightly Challenged
System Development and Maintenance Security is not effectively integrated during the development or updating of systems.	2.00	Slightly Challenged
Incident Management There is no clear procedure for reporting and managing information security incidents.	2.00	Slightly Challenged
Compliance Compliance with ISO/IEC 27001 policies and legal requirements is not regularly monitored or enforced.	2.00	Slightly Challenged
Composite Mean	2.09	Slightly Challenged

As presented in Table 14, the respondents indicated that the Higher Education Institution experiences several challenges in the implementation of ISO/IEC 27001 standards, all of which were assessed as slightly challenging. These include the institution lacks a systematic and consistent process for conducting risk assessments (2.00), there is inadequate definition and assignment of roles for information security (2.00), assets (information and physical) are not properly identified, classified, or managed (2.00), security is not effectively integrated during the development or updating of systems (2.00), there is no clear procedure for reporting and managing information security incidents (2.00), and compliance with ISO/IEC 27001 policies and legal requirements is not regularly monitored or enforced (2.00).

Other indicators that the respondents also identified as slightly challenging include information security roles and responsibilities are not clearly communicated to employees (2.20), backup, recovery, and operational controls are not sufficiently implemented (2.20), and access to systems and data is not adequately restricted or monitored (2.40). With a composite mean of 2.09, the results indicate that the Higher Education Institution experiences slight challenges in implementing the ISO/IEC 27001 standards.

Recommendation to Enhance Information Security Resilience in Higher Education Institutions within Santiago City.

- Risk Assessment. Put in place a simple, repeatable risk assessment routine so risks stop being “someone’s worry” and become a manageable part of how we plan IT and projects.
- Organizing Information Security. Clarify who does what for security — give people clear roles so questions like “who’s in charge?” stop slowing things down.
- Asset Management. Make a basic asset registry — know what you have and how critical it is — so nothing important slips through the cracks.
- Human Resource Security. Ensure staff know their security responsibilities from day one and when roles change — this protects both people and data.
- Communications and Operations Management. Strengthen backups, recovery plans and day-to-day operational controls so interruptions don’t become crises.
- Access Control. Make sure only the right people can get to sensitive systems and that we know when access changes.
- System Development and Maintenance. Include security into every new system and update — not as an afterthought, but as part of the build checklist.
- Incident Management. Create a simple, well-known way for staff to report incidents and a clear small team to act fast.
- Compliance. Make compliance part of routine operations — small, regular checks beat one big audit that surprises everyone.

5. Conclusion

The study's findings indicate that respondents perceive their institution as consistently implementing information security practices aligned with ISO/IEC 27001 standards across key domains, including risk assessment, security organization, asset management, human resource security, communications and operations management, access control, system development, incident management, and compliance. Nevertheless, the respondents also identified minor challenges in all nine areas. This suggests that although policies and procedures are in place, their operational maturity and consistency require further development to achieve full alignment with ISO 27001. Bridging these gaps is critical to enhancing the institution's resilience, particularly in the context of evolving information security threats.

Compliance with ethical standards

Acknowledgement

The researcher would like to express her gratitude to Ramonsito B. Adducul, DIT, the researcher's adviser, who guided her and shared his knowledge, recommendations and expertise in the study and to her respondents, for their patience in answering the questionnaire.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Akour, M., and Alenezi, M. (2022). Higher education future in the era of digital transformation. Education Sciences, 12(11), 784.

[2] Aquino, M. F. M., and Noroña, M. I. (2021, March). Enhancing cyber security in the Philippine academe: A risk-based it project assessment approach. In Proceedings of the international conference on industrial engineering and operations management (pp. 5166-5179).

[3] Bibangco, M. H., and Manahan, E. (2024). Assessing the Philippine National Cybersecurity Plan 2022 for SMEs: Challenges and Opportunities. Philippine Journal of Science, Engineering, and Technology, 1(1), 1-9.

[4] Pamela, A., Fabe, H., and Zarcilla-Genecela, E. (2021). The Philippines' Cybersecurity Strategy: Strengthening partnerships to enhance cybersecurity capability. In Routledge Companion to Global Cyber-Security Strategy (pp. 315-324). Routledge.

[5] Rotas, E., and Cahapay, M. (2021). Does threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid COVID-19 crisis?. Journal of Pedagogical Sociology and Psychology, 3(1), 45-53.

[6] Torregosa, J. T., Orong, M. Y., Ricalde, G. T., Amin, W. D., Lonzon, H. A., and Alcontin, R. B. (2021). Assessing the conformity level of information security management system of the higher education institutions: Basis for the development of policies and guidelines. Mediterranean Journal of Basic and Applied Sciences (MJBAS).