International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 40-53 www.ijaem.net ISSN: 2395-5252

Development of Information Security Framework in the Office of the University Registrar of the University of Southeastern Philippines (USEP)

Lady Vee S. Agunod
Student
University of Southeastern Philippines

Date of Submission: 01-08-2024 Date of Acceptance: 08-08-2024

ABSTRACT
This study aimed to evaluate the dimensions of information security management within the Registrar's Office of the University of Southeastern Philippines. To achieve this, primary data were collected through a survey questionnaire. A purposive sampling method was employed, targeting 150 participants, including faculty members, registrar officers, and staff from various campuses of the University of Southeastern Philippines—namely, Tagum-Mabini, Mintal, Malabog Extension, and the main Obrero Campus.
The items were categorized into three dimensions: institutional commitment towards information security, assessment on good governance in information security performance, and established procedure and transparent policy communication. These dimensions describe the different contributory dimensions in ISM of the registrar's office of USeP.

I. BACKGROUND OF THE STUDY

Information security in educational institutions is meant to ensure continuity and minimize potential business damage by limiting the impact of security incidents (Padyab, 2021). The annual review by the National Cyber Security Centre (NCSC) revealed that there has been a record number of information security incidents between September 2019 and August 2020. According to the US Center for Strategic and International Studies, the annual damage from crimes related to the theft of school computer information exceeds $ 440 billion worldwide. In addition, researchers and IT security companies report that there has been a 45% increase in information security attacks directed to school credentials worldwide, and the educational sector tops the list for cybercriminals compared to other industries (Search Inform, 2019).

More than 50% of educational institutions have faced some sort of data security incident, especially regarding enrollment security. Student data security stands as a paramount concern, reflecting the need to protect individuals' privacy and uphold the integrity of academic processes. Information systems play a pivotal role in this context as the guardians of invaluable data repositories. This comprehensive guide aims to shed light on the significance of data security and provide insights into how information systems play a pivotal role in an educational setting (Shanganlall, 2023).

In Region XI, every year, the University of Southeastern Philippines creates a Student Record Information System (SRIS) for admission, enrollment evaluation, and graduation of the students. The archival management process at the University of Southeastern Philippines is challenging for several reasons. With the rapid advancement of technology, the transition from physical records to electronic formats has introduced new challenges in archival management. While electronic records offer numerous benefits, they also present complexities, especially since some documents within the university have yet to be digitized. According to Zuazola (2023), incomplete digitization can complicate retrieving records in disasters such as fires, earthquakes, or flash floods.

Additionally, there is insufficient data security, a lack of dedicated program providers, and no systematic approach to data management. The existing infrastructure is inadequate, with limited storage capacity that has struggled to accommodate records dating back to 1978. To compound these issues, there is no allotted budget for enhancing the registrar's system, which impedes efforts to improve data management and security. Without robust protection measures, comprehensive policies, and necessary financial resources, there is an increased risk of data breaches, which could significantly affect data privacy and institutional security (Zuazola, 2023).

Thus, the problems identified include challenges in archival management due to incomplete digitization and reliance on electronic records, vulnerability to natural disasters affecting record retrieval, insufficient database security measures, lack of proper data retention policies, and concerns regarding data privacy in case of breaches. Addressing these issues would require implementing robust archival and disaster recovery strategies, enhancing database security, establishing clear data retention policies, and strengthening measures to protect data privacy. The researcher is encouraged to conduct this study to determine the Information Security Management (ISM) model of the registrar's office of USeP. This offers key recommendations to serve as the foundation for future policy directives.

Statement of the Problem

The study was conducted to determine the information security management model of the registrar's office of USeP. Specifically, this paper sought to answer the following questions:

1. What are the dimensions of Information Security Management (ISM) of the Registrar's Office of USeP?
2. What Information Security framework could be developed?

II. REVIEW OF LITERATURE AND THEORETICAL FRAMEWORK

Information Security Management. Information security management, or ISM, is the process of managing risks associated with the use of information technology. It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets. The end goal of this process is to treat risks by an organization's overall risk tolerance. Businesses shouldn't expect to eliminate all risks; rather, they should seek to identify and achieve an acceptable risk level for their organization (Rapid7, 2022).

Information security risk management and cybersecurity risk management are derivatives of that too. Both of these risk areas are growing in importance to organizations so the purpose of this article is to help demystify it to a practical and actionable level. In particular, we'll share how to do risk management for the ISO 27001 standard and achieving compliance for the risk-focused part of the General Data Protection Regulation. Information security risk management (ISRM) is the process of identifying, evaluating, and treating risks around the organization's valuable information. It addresses uncertainties around those assets to ensure the desired business outcomes are achieved (Darby, 2019).

However, cybersecurity and information security are commonly considered to be the same thing, but they are not. Without having a deeply theoretical or academic debate, cybersecurity is more typically about the protection of information held electronically. That means it's a subset of a broader information security posture, which looks at the protection of information from all angles. Information security also means physical security ((Enisa, 2023). The use of social media is prevalent in both the general society and on college campuses. The increasing popularity of the use of social media sites has brought to the forefront a new set of problems and issues facing the 21st century. Today's college generation is facing an emerging risk to reputational harm or financial loss much more so than prior generations since social media is their main form of communication (Bhatnagar, 2020).

Institutional Commitment Towards Information Security. The focus, methods, and effectiveness of security awareness training have undergone significant changes over the years. Back in 2004, most programs were driven by the need for compliance — simply meeting regulatory requirements. Today, that focus has shifted to seeing cybersecurity awareness training as a means to manage and mitigate organizational risk. Around 2014, security awareness training began shifting toward continuous education and improvement, in which a program includes ongoing cycles of assessments and training. The latest developments have been just-in-time and in-context training, which adds the ability to launch training in response to an end user exhibiting poor cybersecurity behavior, such as unsafe web browsing (Profpoint, 2023).

In addition, Security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches. Effective security awareness training helps employees understand proper cyber hygiene, the security risks associated with their actions and to identify cyberattacks they may encounter via email and the web. Research suggests that human error is involved in more than 90% of security breaches. Security awareness training helps to minimize risk thus preventing the loss money or brand reputation. An effective awareness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world such as tailgating or improper document disposal (Mimecast, 2023).

Assessment and Good Governance in Information Security Performance. These results align with Winkler's (2017) article, which states that the Information Security Governance Principles of the Australian Institute of Company Directors (AICD) place a strong emphasis on adopting a proactive and risk-based approach to enhancing governance in Information Security System (ISM). This comprehensive guide underscores the critical role of leadership and board-level engagement in shaping the strategic direction of information security governance. It highlights the importance of establishing well-defined policies, procedures, and frameworks to ensure compliance with relevant regulations and industry standards. Furthermore, the guide stresses conducting regular risk assessments, developing robust incident response plans, and continuously monitoring and reviewing cybersecurity controls.

Security behavior change is a crucial aspect of implementing and maintaining an effective Information Security Management System (ISMS) in any organization. However, changing the habits, attitudes, and practices of employees, managers, and stakeholders is not an easy task. It requires a clear understanding of the common barriers and enablers that influence security behavior, as well as the strategies and tools that can help overcome or leverage them (Linkedin, 2023).

Established Procedure and Transparent Policy Communication. In view of this context, employees' Information Security Awareness (ISA) exerts a significant impact on information security behaviours and employees' security policy compliance Previous studies have argued that a lack of employees' ISA through Information Security Policies (ISP) and procedures was the major cause of mishandling of sensitive information. Further, ISA has become a top priority both in research and practice mainly because humans are found to be one of the weakest links in attempts to secure systems and networks. It has been reported that 88% of UK data breaches were caused by human errors, not by cyberattacks. the most common error was sending sensitive data to the wrong recipient which mostly happened through email or via post or fax and other issues included the loss or theft of paperwork, forgetting to redact data or storing data in an insecure location, such as a public cloud server (Khando, 2021).

In today's interconnected world, international trade relies heavily on digital systems and data exchange. International standards and conformity assessment can help ensure the security and integrity of these digital transactions. Technical barriers to trade (TBT) can emerge when countries or organizations have varying cyber security practices, which hinder the smooth flow of goods and services. To address this issue, international standards provide a common framework for cyber security. Two of the best-known and most trusted cyber security standards are ISO/IEC 27001 for IT and IEC 62443 for the operational technology (OT) found in cyber-physical systems. Both standards contribute to removing TBT in several ways (International Electrotechnical Commission, 2023).

Rivera, Di Gangi, Worrell, Thompson, and Johnston (2015) stated that "academics must consider how they prepare current and future college students to deal with the personal risks involved in using social media. News coverage has made everyone aware of some of the dangers of revealing personal information through social media, but most news stories sacrifice measured and helpful coverage in the interest of sensational headlines. As a result, it is fair to assume that most social media users have a distorted view of the personal risk associated with using social media". This creates a compelling reason for gaining a deeper understanding of students' attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media sites. Moallem (2018) established the importance of awareness to cybersecurity threats and cited prior studies that found the issue is not with awareness but action.

Theory Base

This study is anchored to the Defense-In-depth theory of the U.S. National Security Agency (NSA) (2012). Defense in depth is a strategy that leverages multiple security measures to protect an organization's assets. The thinking is that if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way. Defense in depth addresses the security vulnerabilities inherent not only with hardware and software but also with people, as negligence or human error often cause a security breach. Defense-in-depth is an information assurance strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited. It originates from a military strategy by the same name, which seeks to delay the advance of an attack, rather than defeating it with one strong line of defense.

This approach involves the registrar of a school, such as USeP, handling sensitive data, including academic records, personal information, and student records. Defense in Depth guarantees that this data is fully protected by utilizing numerous security layers. The institution's employees, students, and administration may all suffer significantly if the registrar's sensitive information were to be compromised. By lessening the chance that an attack will be successful and lowering the consequences if security measures are compromised, Defense in Depth helps to reduce these risks. The adoption of Defense in Depth can strengthen USEP's registrar's defenses against both external and internal threats. This method guarantees that operational continuity and sensitive data protection are maintained even during a security layer failure. To put it simply, basing the creation of an information security framework for USEP's registrant on the Defense in Depth theory guarantees a strong, flexible, and legal method of protecting confidential data in an ever-changing learning environment.

III. METHODOLOGY

Research Design. This study used a quantitative, non-experimental survey method. Non-experimental research is the type of research that lacks an independent variable. Instead, the researcher observes and analyzes the phenomenon's context to obtain information. On-experimental research happens during the study when the researcher cannot control, manipulate, or alter the subjects but relies on interpretation or observations to conclude. This means the method must not rely on correlations, surveys, or case studies and cannot demonstrate an actual cause-and-effect relationship (Wiese, 2015).

Sources of Data. The study used primary data, which were taken from the respondents of the University of Southeastern Philippines, all campuses, through a quantitative survey questionnaire. The responses of the survey questionnaire were used in determining the dimensions of ISM of the registrar’s office of USeP.

Data Gathering Instrument. The research data was gathered using a survey questionnaire. A questionnaire was used to explain the variables under the study. In making questions, the researcher ensured that the respondents answered it quickly and truthfully. Furthermore, the research instrument was a self-made survey questionnaire to gather the needed data on ISM of Registrar’s Office of USeP. The questionnaire is a checklist using a Likert-type questionnaire.

Sampling Technique. This study employed purposive random sampling technique. In this study, only 150 respondents were selected from all USeP campuses. Thomas (2020) states that a simple random sample is a randomly selected population subset. Each population member has an equal chance of being selected in this sampling method. This method is the most straightforward since it only involves a single random selection and requires little advance knowledge about the population. Because it uses randomization, any research performed on this sample should have high internal and external validity and be at a lower risk for research biases like sampling biases and selection.

Statistical Treatment

Data Reduction Analysis: This method was used to identify the dimensions of Information Security Management (ISM) within the Registrar’s Office at the University of Southeastern Philippines (USeP).Principal Component Analysis (PCA) was used as the data reduction technique in this study to obtain factors that summarize, to the greatest extent possible, the information available in the dataset. This was also used to condense a large dataset with many variables into a more manageable size.

KMO. Kaiser-Meyer-Olkin Measures of Sampling Adequacy (KMO) were used to indicate the proportion of variance in the variables that underlying factors might cause.

Barlett’s Test of Sphericity. Bartlett’s test of sphericity was used to test the hypothesis that the correlation matrix is an identity matrix, indicating that the variables are unrelated and unsuitable for structure detention.

IV. RESULTS AND DISCUSSION

Factor Analysis. This section presents the results of KMO and Bartlett's Test and Principal Component Analysis. The derivation of the number of factor structures and rotated matrix of the model is also presented using Varimax with Kaiser Normalization.

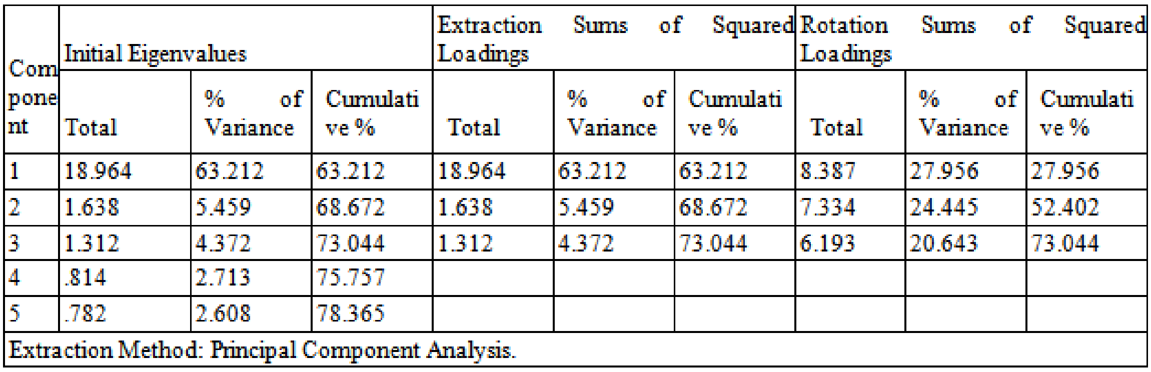
KMO and Bartlett's Test. To ensure that the construct can be tested for factor analysis, the Kaiser Meyer-Olkin Measure (KMO) of Sampling Adequacy and Bartlett’s test of sphericity were performed. It can be gleaned from Table 1 that the KMO value is .933, which is above the recommended value of .6, indicating that the sample is meritorious and adequate for factor analysis. The magnitude of observed correlation coefficients is compared to the magnitude of partial correlation coefficients using the KMO sampling adequacy measure.

Table 1. KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.933
Bartlett's Test of Sphericity	Approx. Chi-Square	3423.108
	Df	435
	Sig.	.000

Total Variance Explained. The total variance explained is used to determine the number of factors of the leadership scale. Three factors were extracted from the original size of 30 components with the use of the initial Eigenvalues, which were set to a standardized value of 1. The three dimensions' factors are the Security Management of the Registrar's Office of USeP.

Table 2. Total Variance Explained



Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	18.964	63.212	63.212	18.964	63.212	63.212	8.387	27.956	27.956
2	1.638	5.459	68.672	1.638	5.459	68.672	7.334	24.445	52.402
3	1.312	4.372	73.044	1.312	4.372	73.044	6.193	20.643	73.044
4	.814	2.713	75.757						
5	.782	2.608	78.365						
Extraction Method: Principal Component Analysis.									

Scree Plot. To further reinforce the findings from the previous table, Figure 2 presents the scree plot, which illustrates the relationship between the number of factors and their corresponding Eigenvalues. The scree plot is the graphical explanation of the total variance explained. The scree plot shows the gradual trailing of the eigenvalues and shows the relative fit of each principal component. It does this by plotting the proportion of the variance of the data that is fit by each component versus the number of components. The plot shows the relative importance of each component in fitting the data. The components are always sorted according to their relative importance, so initial components will always explain more variance than those in subsequent positions.

This aligns with the observation of Mangale (2020), that a standard method for determining the number of Scree Plot Criterion (SPCs) to be retained is a graphical representation known as a scree plot. A Scree Plot is a simple line segment plot that shows the eigenvalues for each individual PC. Most scree plots look broadly similar in shape, starting high on the left, falling rather quickly, and then flattening out at some point. This is because the first component usually explains much of the variability, the next few components explain a moderate amount, and the latter components only explain a small fraction of the overall variability.

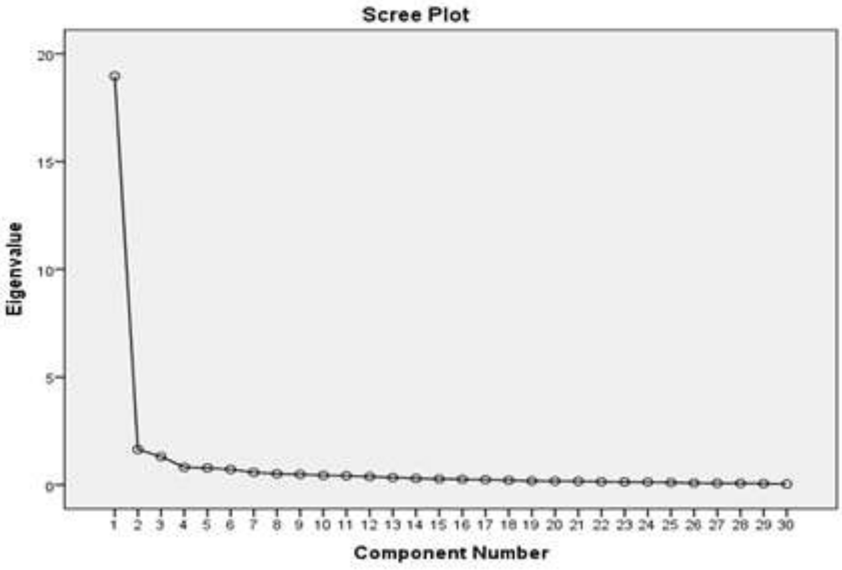


Figure 2. Scree Plot

Rotated Component Matrix. After identifying the number of factor structures, the 30-item construct is subjected to rotation. Table 3 shows the pattern matrix using Principal Component Analysis with a rotation method of Varimax with Kaiser Normalization. According to the standard rule of factor analysis, items with a loading value of less than .60 should be excluded. The result reveals that three dimensions are taken from the result of the total variance explained. These dimensions are institutional commitment towards information security, assessment, on good governance in information security performance, and established procedure and transparent policy communicationThis is supported Hair et al. (2010) categorized these loadings using another rule of thumb as ±0.30=minimal, ±0.40=important, and ±.50=practically significant. If no correlations go beyond 0.30, then the researcher should reconsider whether factor analysis is the appropriate statistical method to utilize.

Table 2. Rotated Component Matrix

	Component		
	1	2	3
i12	.785		
i11	.734		
i25	.687		
i27	.684		
i26	.678		
i30	.673		
i5	.661		
i3	.653		
i10	.646		
i14	.635		
i28	.632		
i13	.623		
i4	.618		
i1			
i9			
i29			
i20		.738	
i23		.725	

i21		.714	
i22		.702	
i16		.686	
i15		.680	
i24		.672	
i19		.605	
i17			
i7			.760
i6			.695
i2			.638
i8			.604
i18			
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.			
a. Rotation converged in 52 iterations.			

Dimensions of Information Security Management (ISM).

Based on the criterion, 30 items were classified into three dimensions: institutional commitment towards information security, assessment, on good governance in information security performance, and established procedure and transparent policy communication. The cumulative load percentage of these nine dimensions was calculated at 73.757, implying that the three dimensions could explain 73.757% of the total variability. In addition, these dimensions and the categorized items are presented in tables and discussed with other related scientific studies.

Institutional Commitment Towards Information Security. The first dimension, as shown in Table 4, shows the twelve items under institutional commitment towards information security and the corresponding loading coefficient. As observed, the item “UseP keeps documented evidence showing that processes have been carried out as planned” obtained the highest loading coefficient of .785. The item “Measurable ISM objectives have been established, documented, and communicated throughout USeP” obtained a loading coefficient of .734. The item “There is a proper storage and retrieval system for data and records in case of emergencies such as fire, floods, and earthquakes” obtained a loading coefficient of .687. The item “USeP has developed and implemented a program to ensure the ISM achieves its outcomes, requirements, and objectives” obtained a loading coefficient of .684. The item “USeP has clearly identified the requirements of interested parties that will be addressed through the information security management system” obtained a loading coefficient of .678.

Furthermore, the item “USeP has a process to retain documented information on the results of the information security risk assessment” obtained a loading coefficient of .673. The item “USeP has a process to retain documented information on the results of the information security risk assessment” obtained a loading coefficient of .661. The item “USeP analyzes information security risks to assess the realistic likelihood and potential consequences if they occur, and determines the levels of risk” obtained a loading coefficient of .653. The item “USeP ensures that the ISM is aligned with other organizational policies, processes, and cultures” obtained a loading coefficient of .646. The item “USeP creates and maintains a supportive and collaborative security community where employees can share, learn, and emulate best security practices” obtained a loading coefficient of .635. The item “USeP optimizes the security environment so clients can easily access and use the security system” obtained a loading coefficient of .632. And the item who obtained the lowest loading coefficient of .623, is the item “USeP conducts regular information security awareness training for its staff”.

Table 4. Rotated Component Matrix with Items Grouped Under Environmental Awareness and Community Support.

Item No.	**Items**	**Factor Coefficient**	**Dimension**
12	UseP keeps documented evidence showing that processes have been carried out as planned.	.785	**Institutional Commitment Towards**

11	Measurable ISM objectives have been established, documented, and communicated throughout USeP.	.734	**Information Security**
25	There is a proper storage and retrieval system for data and records in case of emergencies such as fire, floods, and earthquakes.	.687	
27	USeP has developed and implemented a program to ensure the ISM achieves its outcomes, requirements, and objectives.	.684	
26	USeP has clearly identified the requirements of interested parties that will be addressed through the information security management system.	.678	
30	USeP sets high-level security standards to help drive IT security.	.673	
5	USeP has a process to retain documented information on the results of the information security risk assessment.	.661	
3	USeP analyzes information security risks to assess the realistic likelihood and potential consequences if they occur, and determines the levels of risk.	.653	
10	USeP ensures that the ISM is aligned with other organizational policies, processes, and cultures.	.646	
14	USeP creates and maintains a supportive and collaborative security community where employees can share, learn, and emulate best security practices.	.635	
28	USeP optimizes the security environment so clients can easily access and use the security system.	.632	
13	USeP conducts regular information security awareness training for its staff.	.623	

The study’s findings focus on the effectiveness of security awareness training, which has undergone significant changes over the years. The need for compliance drove most University of Southeastern Philippines programs — simply meeting regulatory requirements. Today, that focus has shifted to seeing cybersecurity awareness training to manage and mitigate organizational risk. Around 2014, security awareness training began shifting toward continuous education and improvement, in which a program includes ongoing cycles of assessments and training. The latest developments have been just-in-time and in-context training, which adds the ability to launch training in response to an end user exhibiting poor cybersecurity behavior, such as unsafe web browsing (Profpoint, 2023).

In addition, security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees of USeP to understand the role they play in helping to combat information security breaches. Effective security awareness training helps employees understand proper cyber hygiene, the security risks associated with their actions and to identify cyberattacks they may encounter via email and the web. Research suggests that human error is involved in more than 90% of security breaches. Security awareness training helps to minimize risk thus preventing the loss money or brand reputation. An effective awareness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world such as tailgating or improper document disposal (Mimecast, 2023).

Furthermore, if all employees of USeP get training in information security practices, there will be less likelihood of lapses in protection should someone leave the company. In other words, it will reduce the chances that a security breach occurs because a critical employee wasn’t at work that day. Finally, a company with security-aware personnel will have a better reputation with consumers since most are reluctant to do business with an untrustworthy organization. A business that is repeatedly subject to security breaches will lose customers due to negative publicity, regardless of the actual impact of any particular breach. To create this enhanced level of security, people need to be informed of best practices (Terra, 2023).

Assessment on Good Governance in Information Security Performance. The second dimension, as shown in Table 5, shows the eight items under assessment on good governance in information security performance. The item who obtained the highest loading coefficient of .738, is the item "Feedback on information security performance is considered as an input to management review". This is followed by the item "USeP conducts regular audits to ensure compliance with information security policies and procedures" who obtained a loading coefficient of ".725. The item "USeP considers feedback on information security performance as an input to management review" obtained a loading coefficient of .714. The item "USeP has determined what needs to be monitored and measured, by whom, the methods to be used, and when the results will be evaluated" obtained a loading coefficient of .702.

Table 5. Rotated Component Matrix with Items Grouped Under

Item No.	Items	Factor Coefficient	Dimension
20	Feedback on information security performance is considered as an input to management review.	.738	**Assessment on Good Governance of Information Security Performance**
23	USeP conducts regular audits to ensure compliance with information security policies and procedures.	.725	
21	USeP considers feedback on information security performance as an input to management review.	.714	
22	USeP has determined what needs to be monitored and measured, by whom, the methods to be used, and when the results will be evaluated.	.702	
16	There is an increased understanding of employees' perception of information security in USeP.	.686	
15	Faculties, registrar, and staff are trained in the proper use of information security technology and data security.	.680	
24	The Registrar's Office is fully electronic/digitized.	.672	
19	USeP establishes and uses appropriate indicators and metrics for the ISM and information security culture.	.605	

In addition, the item "There is an increased understanding of employees' perception of information security in USeP" obtained a loading coefficient of .686. The item "Faculties, registrar, and staff are trained in the proper use of information security technology and data security" obtained a loading coefficient of .680. The item "The Registrar's Office is fully electronic/digitized" obtained a loading coefficient .672. Lastly, the item that obtained the lowest loading coefficient of .605 is the item "USeP establishes and uses appropriate indicators and metrics for the ISM and information security culture".

These results align with Winkler's (2017) article, which states that the Information Security Governance Principles of the Australian Institute of Company Directors (AICD) strongly emphasize adopting a proactive and risk-based approach to enhancing governance in ISM. This comprehensive guide underscores the critical role of the information security framework in registrar's office of USeP. It highlights the importance of establishing well-defined policies, procedures, and frameworks to ensure compliance with relevant regulations and industry standards. Furthermore, the guide stresses conducting regular risk assessments, developing robust incident response plans, and continuously monitoring and reviewing cybersecurity controls.

Security behavior change is a crucial aspect of implementing and maintaining an effective Information Security Management System (ISMS) in the University of Southeastern Philippines. However, changing the habits, attitudes, and practices of employees, managers, and stakeholders is not an easy task. It requires a clear understanding of the common barriers and enablers that influence security behavior, as well as the strategies and tools that can help overcome or leverage them (Linkedin, 2023).

Another common enabler for security behavior change is the social influence that can shape or reinforce the security norms, attitudes, and behaviors of individuals or groups. This influence can come from various sources, such as peers, managers, leaders, or role models. To leverage these social enablers, company need to create and maintain a supportive and collaborative security community, where people can share, learn, and emulate best security practices (Macpherson, 2023).

Established Procedure and Transparent Policy Communication. The third dimension, as shown in Table 6, shows the four items under established procedure and transparent policy communication. The item "USeP has established, implemented, and maintained the necessary processes and their interactions for the information security management system" obtained the highest loading coefficient of .760. The item "USeP understands the threats and vulnerabilities in its information security network" obtained a loading coefficient of .695. The item "USeP has defined and developed a repeatable information security risk assessment process that ensures consistent, valid, and comparable results" obtained a loading coefficient of .638. Furthermore, the item "The information security policy has been communicated within USeP and to relevant interested parties" obtained the lowest loading coefficient of .604.

Table 6. Rotated Component Matrix with Items Grouped Under

Item No.	Items	Factor Coefficient	Dimension
7	USeP has established, implemented, and maintained the necessary processes and their interactions for the information security management system.	.760	**Established Procedure and Transparent Policy Communication**
6	USeP understands the threats and vulnerabilities in its information security network.	.695	
2	USeP has defined and developed a repeatable information security risk assessment process that ensures consistent, valid, and comparable results.	.638	
8	The information security policy has been communicated within USeP and to relevant interested parties.	.604	

Given this context, employees' Information Security Awareness (ISA) significantly impacts information security behaviors and employees' security policy compliance. Previous studies have argued that a lack of employees' ISA through Information Security Policies (ISP) and procedures was the primary cause of the mishandling of sensitive information. Further, ISA has become a top priority both in research and practice mainly in the University of Southeastern Philippines because humans are found to be one of the weakest links in attempts to secure systems and networks. It has been reported that 88% of UK data breaches were caused by human errors, not by cyberattacks. the most common error was sending sensitive data to the wrong recipient which mostly happened through email or via post or fax and other issues included the loss or theft of paperwork, forgetting to redact data or storing data in an insecure location, such as a public cloud server (Khando, 2021).

In today's interconnected world, international trade relies heavily on digital systems and data exchange. International standards and conformity assessment can help ensure the security and integrity of these digital transactions. Technical barriers to trade (TBT) can emerge when countries or organizations have varying cyber security practices, which hinder the smooth flow of goods and services. To address this issue, international standards provide a common framework for cyber security. Two of the best-known and most trusted cyber security standards are ISO/IEC 27001 for IT and IEC 62443 for the operational technology (OT) found in cyber-physical systems. Both standards contribute to removing TBT in several ways (International Electrotechnical Commission, 2023).

Information Security Framework of the Registrar's Office of USeP

As shown in Figure 3, the faculty, registrar's officer, and staff of the University of Southeastern Philippines have chosen three dimensions of information security management. These include institutional commitment towards information security, assessment on good governance in information security performance, and established procedure and transparent policy communication.

The first dimension is **Institutional Commitment Towards Information** Security, which means that USeP is dedicated to protecting its data by creating clear security policies and ensuring everyone knows about them. They keep data safe and easy to access, follow high-security standards, regularly check for and manage risks, improve security practices as needed, and provide ongoing training to keep everyone informed about security best practices.

The second dimension is **Assessment and Good Governance in Information Security Performance**, which evaluates how effectively USeP manages its information security. It includes gathering feedback on security performance, conducting audits, and monitoring and measuring security practices. The assessment also aims to enhance the understanding of employees' perceptions of security, provide necessary training to improve their knowledge and use digitized tools and appropriate indicators to track and assess security performance accurately.

Furthermore, the third dimension is **Established Procedure and Transparent Policy Communication**, which is how USeP sets up clear and necessary procedures for managing information security. It involves understanding potential threats, creating a repeatable method for assessing and managing security risks, and ensuring that information security policies are communicated to all members within USeP. This transparency ensures everyone is aware of and follows the established security protocols.

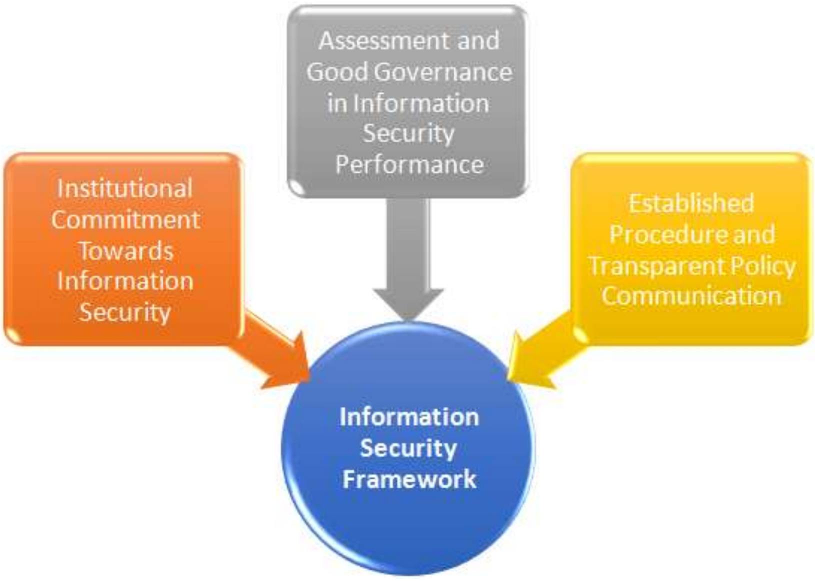

Assessment and Good Governance in Information Security Performance
Institutional Commitment Towards Information Security
Established Procedure and Transparent Policy Communication
Information Security Framework

Figure 3. ISM Model of the Registrar's Office of USeP

SUMMARY, CONCLUSION, AND RECOMMENDATION

Summary

This study aimed to determine the dimensions of the information security management of the registrar's office of USeP. The survey involved participants from all University of Southeastern Philippines campuses, including Tagum Mabini, Mintal, Malabog Extension, and the main Obrero Campus. 150 faculty members, registrar officers, and staff will be chosen to complete a 30-item survey questionnaire.

The items were categorized into three dimensions: institutional commitment towards information security, assessment on good governance in information security performance, and established procedure and transparent policy communication. These dimensions describe the different contributory dimensions in ISM of the registrar's office of USeP.

Conclusion

Based on the study's findings, the researcher concluded three underlying dimensions of information security management of the registrar's office of USeP: institutional commitment towards information security, assessment on good governance in information security performance, and established procedure and transparent policy communication.

Recommendation

Based on the findings, the researcher recommended the following:

Top Management of USePmay allocate an increased budget specifically for information security initiatives. This investment will enhance the security measures and implement advanced technologies and tools to protect the data better. Additionally, increasing the budget will facilitate hiring additional skilled personnel dedicated to information security. Expanding our team will ensure we have the expertise to effectively manage and address security risks, conduct regular audits, and maintain compliance with evolving standards and regulations.

The **System and Data Management Division (SDMD)** may enhance access control to ensure that only authorized personnel have access to sensitive information and continuously monitor the evolving threat landscape and update the information security framework accordingly. Stay informed about new security technologies, trends, and regulatory requirements that may impact the registrar's office. This helps the Office of the University Registrar at USeP strengthen its information security framework, mitigate risks, and protect sensitive data effectively.

The **Office of the University Registrar (OUR)** may implement comprehensive training programs for all personnel. These training sessions should focus on enhancing employees' skills in identifying, managing, and mitigating security threats and understanding best practices for protecting sensitive information. Additionally, investing in system improvements is necessary to ensure that our information security infrastructure remains robust and up to date. This includes upgrading current security systems, integrating n technologies, and addressing identif vulnerabilities.

Clientele may recommend that the Registrar's Office create thorough information security policies that include incident response, data protection, access controls, and regulatory compliance and update them regularly. Furthermore, clients suggest holding frequent training sessions and awareness programs on data handling protocols, phishing awareness, and information security best practices for the Registrar's office staff. Clients may assist the Registrar's Office in improving data protection procedures, strengthening information security management practices, and fostering stakeholder confidence in the security and integrity of sensitive information handled by the office by suggesting these actions.

Future researchers may suggest implementing advanced authentication techniques like biometrics or adaptive authentication systems to improve user verification and access control and lower the risk of unauthorized access. They may also mean developing and testing an incident response plan specifically suited to the Registrar's office operations, outlining protocols for identifying, handling, and recovering from security incidents. Clients can assist the Registrar's Office in improving data protection procedures, strengthening information security management practices, and fostering stakeholder confidence in the security and integrity of sensitive information handled by the office by suggesting these actions.

REFERENCES

[1]. Bhatnagar, N. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Information Systems Education Journal (ISEDJ).

[2]. Darby, M. (2019). Information Security Risk Management Explained – ISO 27001. Retrieved from https://www.isms.online/iso-27001/information-security-risk-management-explained/.

[3]. EIC. (2023). How cyber security standards help remove technical barriers to trade. Retrieved from https://iec.ch/blog/how-cyber-security-standards-help-remove-technical-barriers-trade.

[4]. Enisa. (2023). Risk Management & Information Security Management Systems. Retrieved from https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-isms.

[5]. Hanna, K. T. (2022). ISO 27001. Retrieved from https://www.techtarget.com/whatis/definition/ISO-27001.

[6]. Khando, K. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404821000912.

[7]. Linkedin. (2023). What are the common barriers and enablers for security behavior change in organizations? Retrieved from https://www.linkedin.com/advice/1/what-common-barriers-enablers-security.

[8]. Lobmeier, J. H. (2021). Non-experimental Designs. Retrieved from https://methods.sagepub.com/reference/encyc-of-research-design/n271.xml#:~:text=In%20nonexperimental%20designs%2C%20the%20groups,compares%20what%20is%20already%20established.

[9]. Macpherson, M. (2023). Social enablers. Retrieved from linkedin.com/advice/1/what-common-barriers-enablers-security.

[10]. Mangale, S. (2020). Scree Plot. Retrieved from https://sanchitamangale12.medium.com/scree-plot-733ed72c8608.

[11]. Mimecast. (2023). What is security awareness training? Retrieved from mimecast.com/content/what-is-security-awareness-training/.

[12]. Moallem, A. (2018). Cyber security awareness among college students. International Conference on Applied Human Factors and Ergonomics.

[13]. Padyab, A. (2021). Challenges of Managing Information Security during the Pandemic. Retrieved from https://www.mdpi.com/2078-1547/12/2/30.

[14]. Profpoint. (2023). What Is Security Awareness Training? Retrieved from https://www.proofpoint.com/us/threat-reference/security-awareness-training#:~:text=Security%20awareness%20training%20is%20a,threats%20from%20causing%20data%20breaches.

[15]. Rapid7. (2022). What is Information Security Risk Management (ISRM)? Retrieved from https://www.rapid7.com/fundamentals/information-security-risk-management/#:~:text=Get%20the%20Report-,What%20is%20Information%20Security%20Risk%20Management%20(ISRM)%3F,availability%20of%20an%20organization's%20assets.

[16]. Rivera, J. (2015). Undergraduate student perceptions of personal social media risk. Information Security Education Journal,.

[17]. SearchInform. (2019). IS Worldwide | The problems of information security in the world. Retrieved from https://searchinform.com/infosec-blog/2019/08/01/is-worldwide-the-problems-of-information-security-in-the-world/.

[18]. Terra, J. (2023). The Importance of Security Awareness Training. Retrieved from https://www.simplilearn.com/importance-of-security-awareness-training-article.

[19]. Thomas, L. (2020). Simple Random Sampling | Definition, Steps & Examples. Retrieved from https://www.scribbr.com/methodology/simple-random-sampling/#:~:text=Simple%20random%20sampling%20is%20a,possible%20of%20this%20random%20subset.

[20]. Unisys. (2019). The Philippines Shows the Highest Level of Concern Over Security Issues; One in Five Filipinos Have Stopped Dealing With an Organisation After a Data Breach - New Unisys Security Index. Retrieved from https://www.unisys.com/news-release/ph-

the-philippines-shows-the-highest-level-of-concern/.

[21]. Wiese, C. (2015). Non-experimental research: What it is, overview & advantages. Retrieved from https://www.questionpro.com/blog/non-experimental-research/.

[22]. Winkler, I. (2023). Information Security Governance Framework Guide for IT Activities. Retrieved from https://www.kiteworks.com/cybersecurity-risk-management/information-security-governance-framework-guide-for-it-activities/.

[23]. Zuazola, F. (2023). Information security problems of Usep. Retrieved from https://www.rappler.com/nation/mindanao/davao-regains-control-hacked-traffic-office-page-may-22-2023/.