Journal of Information and Knowledge Management (JIKM) Volume 13 Number 1 (2023)

Information Security Risk Management Framework for A Governmental Educational Institute

Fajer Al-Mudaires, Aida Al-Samawi, Ahmed Aljughaiman and Liyth Nissirat

College of Computer Sciences and Information Technology, Department of Computer Networks, King Faisal University, Al-Ahsa, 31982, Saudi Arabia

Email: aalsamawi@kfu.edu.sa

Received Date: 21 November 2022
Acceptance Date: 7 December 2022
Published Date: 1 April 2023

Abstract. As the high increase usage of technology, the higher the risks that are associated with it. Therefore, it has become a necessity for organizations to rely on an information security risk management framework as a defense mechanism against these risks. This paper discusses information security risk management approaches available with an emphasis on the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27005 method to propose an information security risk management framework that suits a governmental educational institute in Saudi Arabia. This framework will be designed and implemented for a governmental educational institute that lacks adequate information security risk management while being out of compliance with Saudi Arabia's Essential Cybersecurity Controls (ECC). In this framework, 34 application assets have been analyzed and 37 controls have been recommended in order to meet the minimum requirements of ECC.
Keywords: Information security risk management, ISO/IEC 27005, ECC, Regulatory Compliance, information management

1 Introduction

Information security risk management is the application of management policies, processes, and methodologies to the context-setting, identification, analysis, evaluation, treatment, monitoring, and communication of information security risks. Security risk management can be implemented in accordance with the organization's size. Cybersecurity risk management is crucial and should be investigated as a serious business activity by the organization's stakeholders and executive leadership. This must be at the same level as operational, financial, and reputational risks, with corresponding requirements and consequences. National Institute of Standards and Technology (NIST) 800-30, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), CCTA Risk Analysis and Management Method (CRAMM), and Fenz et al. ISO/IEC 27005 are examples of national and international standards that outline risk procedures. Each of these specifications has a unique number of operation stages. NIST 800-30 is

a five-step information security risk management framework, whereas OCTAVE and CRAMM are three-phase methods to information security risk management. ISO/IEC 27005 is a six-phase information security risk management standard developed by Fenz et al.

ISO/IEC 27005:2018 is considered the best-suited standard for governmental educational institutes that lack adequate information security risk management. ISO/IEC 27005 has been chosen for its flexibility, the way in which it can be utilized with other standards, its completeness of structure, the requirements of the organization, and its design orientation (Badamasi and Utululu, Putra and Matijarasa and Wangen et al.). The adopted method will be in compliance with the Essential Cybersecurity Controls (ECC-1:2018) of the National Cybersecurity Authority (NCA). The educational institute is a governmental university specializing in health sciences that was established in 2005. It has 14 colleges on three campuses in Riyadh, Jeddah, and Al-Ahsa. The NCA is a governmental organization that regulates cybersecurity controls in Saudi Arabia that was established in 2017 and acts as the national expert on its associations. The NCA developed ECC-1: 2018, which consists of five cybersecurity main domains, 29 sub-domains, and 114 controls. The main domain is called cybersecurity governance, where sections 1–5 represent cybersecurity risk management, which is the subdomain concerned with risk management to be used in this project (NCA). The ISO and IEC are the collaborations that form the expert system for worldwide standardization that has been approved and implemented in highly critical organizations internationally. The ISO/IEC 27005 standard for information security risk management consists of six phases: Context Establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment and Risk Acceptance (ISO-ISO/IEC27005:2018). This project aims to develop an information security risk management framework for the institute, applying ISO/IEC 27005 and being in compliance with Saudi Arabia's (ECC-1:2018) controls. The modification of this analysis bias is abandoning the sole reliance on technology factors and shifting focus to the subjectivity inherent in human people, their relationships, and organizational behavior, since such behavior has a significant impact on information security management. Even when other equally significant aspects are taken into account, Colwill (2010) argues that overconfidence in technology will lead to unexpected outcomes when addressing a very critical internal security threat: the human element. This factor creates information security threats since individuals may get legitimate access to information, are familiar with the company, and are aware of the location of significant assets.

This article focused on identifying the human factors that interfere with information and knowledge management techniques pertaining to information security. People's behavior, relationships, and behaviour impact the corporate environment on a spectrum of varied degrees where information security is required.

Businesses arrange themselves to retain their competitiveness and work quality in global marketplaces. Technology is the catalyst that provides efficiency and effectiveness to businesses. Regardless matter how complex a technological solution may be, it will be but one component of the organization's efforts to retain its competitiveness. People and processes are crucial components, and only strategic management that

includes all organizational components—planning, effective action, and strategic information management—can reach the required levels of competitiveness for the business.

When considering how human resources affect the information security of a company, it is simple to conclude that the "people" aspect is weak. This weakness emerges in two interrelated dimensions, both of which compromise information security and make the human element the weakest link. First, employees should have sufficient information security expertise to implement and maintain security policies effectively, which is not always the case; Second, personnel must have the proper attitude toward information security, but this is not always communicated to them (Niekerk and Solms, 2010).

This first method emphasizes the need of openness, management, and efficient communication with reference to the information security principles implemented by an organization. All aspects of the organization must be involved in a synergistic manner if they are to address security challenges with completeness of action and genuine knowledge of the need to protect organizational assets. Kraemer, Carayon, and Clem (2009) add to this viewpoint by highlighting that users are not inherently anti-security but are frequently unable to discern the security consequences of their actions.

This situation prompts a consideration of how a lack of knowledge causes inap-propriate conduct as a result of expected information security measures, since responding appropriately is wholly dependent on understanding how to behave. For corporate information and knowledge management, as well as for a better understanding of their users' demands, it is therefore essential for businesses to keep and share accurate information. Information users should be viewed as individuals who are not only motivated to seek information for cognitive reasons, but also as individuals who live and work in social environments (such as corporations) and who, in their context, generate their own motivations for learning, seek information, and satisfy their needs (Wilson, 2006b). This article defines this information user as one who is highly dependent on information and utilizes it for particular objectives, including professional ones.

2 Preliminaries and Related Work

This section presents the most relevant literature review of the previous work done by experts, researchers, and the national and international standards used for information security risk management. The literature review is dedicated to information security risk management to show that researchers addressed the importance of implementing an information security risk management framework and that they proposed different methodologies to implement information security risk management for different types of organizations.

Singh and Joshi presented a quantitative information security risk management framework that is suitable for the university computing environment. The framework’s aim is to reduce the risk of security breaches by implementing one of the most popular risk management frameworks, called OCTAVE.

The framework consists of three phases: Phase one identifies the threats and vulnerabilities in educational systems by evaluating them. Phase two emphasizes the most critical risk and initiates an actionable remediation plan, and Phase three recognizes the vulnerability management compliance requirement in order to enhance the university's security status. The model takes quantitative data from 1–10 and presents it in a qualitative manner (high, medium, low, informational). The proposed model was implemented in the Vikram University in India by measuring actual risk scenarios, applying the phases, and quantifying each phase with the support of scanner tools, and the implementation of the model proved an improvement in the security level in the university. However, their work only focused on network assets.

Fenz et al. proposed an information security risk management framework named Automated Risk Utility Management (AURUM) with four phases: Business Importance Determination, Inventory Phase, Threat Probability Determination, Risk Determination, and Control Identification. Their work adapted the ISO/IEC 27002 standard, a German standard from the German IT Grundschutz Manual, NIST SP 800-30. They validated their work by conducting two case studies on small and large European enterprises.

Fahrotuzi et al. proposed an information security risk management method based on risk management of ISO/IEC 27005 standard for the Data and Information Center of Ministry of Defense in Indonesia. Their work focused on applying the information security management by using ISO/IEC 27001, ISO/IEC 27002 and adopting ISO/IEC 27005 security risk management. ISO/IEC 27001 and ISO 27002 summarized in Plan, Do, Check, Act and repeat framework. The result of their work is an output paper in the form of information security risk management plan.

Chapman discussed the critical need for an appropriate level of cybersecurity protection in the United Kingdom's Universities. The author highlighted that in 2018, 12% increase in comparison to the previous year of higher education institutions were prone to cyberattacks. In addition, the author emphasized that the government should enforce more policies and regulations for higher education to be in compliance with and enforce them to reduce cybersecurity threats.

Badamasi and Utululu investigated the cybersecurity issues in Nigerian Universities and mainly highlighted their poor management of their cyberspace and resources and that they do not have an adequate risk management process. As an initiative to improve Nigerian Universities cybersecurity risk management, they proposed a cybersecurity risk management framework based on a literature review for Nigerian Universities. The framework was derived from an intensive literature review. However, their work is only an empirical research study that was not implemented in an actual University in order to get real data and accurate observation.

Fenz et al. overviewed the current information risk management and outlined their communalities and differences for current information security risk management frameworks summarized in the following:

NIST SP 800-30 is considered as the updated information security risk management framework developed by Ghallaler in 2012 includes components of framing risks, assessing risks, responding to risks and monitoring risks.

ISO 27005 standard framework which is divided into the phases of risk assessment, risk treatment and risk acceptance.

Expression of Needs and Identification of Security Objectives (EBIOS) is a French information security risk management framework that consists of five phases that is similar to the phases of NIST SP 800-30 with some differences.

OCTAVE is also a three-phase information security risk management framework: identification of vital assets, identification of vulnerabilities, and identification of hazards pertinent to key assets in order to reduce risk to an acceptable level.

CRAMM is a risk analysis and management system created in 1991 by the CCTA, a British government agency. It consists of three phases: asset identification and value, threat and vulnerability assessment, and countermeasure selection and recommendation.

Four steps comprise the Factor Analysis for Information Risk (FAIR) paradigm suggested by an association seeking for IT standards.

Information Security Assessment and Monitoring Method (ISAMM) is a quantitative technique developed by the Telindus group that estimates yearly loss of expectation and consists of four phases: defining the scope, identifying the danger, validating the threat, and calculating the loss.

Information Security Forum (ISF) standard of good practice is produced by the ISF and offers organizations with guidance for implementing the standard as a framework for information security risk management.

Custer discussed that information security threats such as traditional threats via human factor such as stolen laptops. Application and server infrastructure threats and vulnerabilities on databases and websites are significantly increasing on a daily basis. These breaches occur on higher educational institutes information assets. The accumulation of information in higher education produces risks and systematic managed crimes by hackers. The author emphasized the serious need for an information security risk management plan that is operational and follows a specific standardization to solve this issue.

Putra and Matijarasa designed an information security risk management for an Indonesian governmental agency based on the ISO 27005:2018 and NIST 800-30. The result of their validation was that their information security risk management works with the agency's policy and meets the organization's goals for identifying and managing risks while doing daily tasks.

Nunes and Sergio presented a systematic literature review of 40 published journal articles concerning information security risk management for the period of years from 2010 to 2015. They categorized their work into technical, formal and informal. The authors highlighted that most authors of the analyzed articles focused on developing an information security risk management method without how to communicate these results with decision makers.

According to Brunner et al. presented a survey resulting in a 64 response investigating the practice of implementing information security risk management. They found out that the present practices of information security risk management are in need of enhancement due to manual data collection, complex subjective decision making process while relying on multiple stakeholders decisions. They recommended the use of

general purpose tools instead of information security risk management frameworks. However, the number of responses used in their survey is limited.

Zhang developed a new information security risk management framework for information security risk management in big data organizations based on differential algorithm protocol for big data environment. However, they did not validate their work.

Bergstromet et al. discussed the challenges that occur when implementing an information security risk management plan. Six challenges were introduced asset and countermeasure inventory, assigning asset values, failed prediction of risks, overconfidence effect, knowledge sharing and cost versus cost trade-offs. Their work was an empirical study through interviews with representative from public sector. Their results were validated by an expert panel.

Zhang et al. proposed a seven process information security risk management framework for cloud computing environments based on ISO/IEC 27002 and NIST 800-30 methods in terms of cloud information security risk managment. Their framework is dedicated to cloud providers to consider when implementing an information security risk management in the cloud. Nevertheless, they did not validate their work or implement it in a cloud computing environment.

Putra et al. implemented ISO/IEC 27001 and ISO/IEC 27005 information security risk management planning for telecommunication companies with the use of Nvivo qualitative analysis tool. Their work resulted in a 26 impact scenarios as highest rank and 12 priority impact scenarios. They recommended set of controls based on ISO 27001 to support their information security risk management framework. However, the recommended controls provided were not comprehensive.

Aleksandrova et al. stated that implementing an information security risk management plan doesn't just reduce the risks occurring in an organization but increase the organization's competitive advantage. Their work recommended the use of ISO/IEC 27001 as an information security risk management approach. Implementation of such approach includes the following tasks: support of top management, project management method, information security scope determination, information security policy development, risk assessment and risk assessment register. However, their work focused on one standard only.

Valerie et al. argued that the application of mathematical fuzzy logic in the information security risk management of risks allows to develop expert systems assisting in the information security risk management tasks. However, their work focused on assisting in the overall assessment process and there were no common standards used.

Bakaret et al. proposed an Internet of Things (IoT) information security risk management framework with the adaptation of ISO/IEC 27005:2018. Resulted in a preliminary information security risk management design for IoT in health care.

Whereas Hamit et al. adapted ISO/IEC 27005: 2018 information security risk management framework for protecting patients' data. Their work resulted in the identification of thirty risks and a risk treatment plan. Their work focused on the treatment plan more than the overall information security risk management plan.

Safonova et al. discussed the approach of creating, implementing and assessing the effectiveness of ISO/IEC 27001 and ISO/IEC 27005 in terms of information security

risk management. Their work resulted in a process approach for information security risk management as per ISO/IEC 27001 and ISO/IEC 27005. They discussed the requirements for ISO/IEC 27001 in plan, do, check and act with ISO/IEC 27005 tasks as a methodology. They stated that the creation of an information security risk management plan is complex. However, their work was a theoretical study without validation.

Lanz and Sussam raised the issues of information security risk management during the pandemic of COVID-19.

Grishavea, and Borzov discussed the importance for enterprises to consider implementing a security risk management plan.

According to Kaspersky lab's statistics conducted in 2018, 30.1% of worldwide computers were infected with malware, 1876998691 attacks from internet resources, 55415962 unique URLs recorded web antivirus, 21643946 malicious objects, 765538 ransomware attacks, 5638828 miner attacks and 830135 bank accounts attacks.

Almomani et al. argues that NCA's ECC lack of a practical, published mechanism that constantly measures organization's security level and higher educational institutes in particular.

Alshafreef stated that there is a poor research area in implementing information security risk management framework in Saudi Arabian organizations.

Monev argued that the use of popular commercial software third party off the shelf solutions are insufficient to assist in risk assessment process as defined in ISO/IEC 27005 or NIST 800-30. Then proposed a solution framework for third party companies to follow when designing a commercial software for risk assessment.

Sensuse et al. proposed an information security risk management framework for digital certificate management organization. Their framework combined the use of ISO/IEC 27005 and NIST SP 800-30 standards. Their work resulted in the identification of 27 assets, 26 threat scenarios to be reduced and 38 risk scenarios are accepted by the organization.

Argawal proposed an information security risk management framework as per the ISO/IEC 27005 standard with the guideline provided in UNINET information classification scheme. The author validated their work by implementing their framework in a health clinic case scenario. However, results and UNINET scheme were ambiguous.

Wei et al. discussed a risk recommendation mechanism that utilizes data mining in the threat and vulnerability identification process during the information security risk management process. The result of their recommendation showed that risk identification process is conducted faster via data mining tools than being conducted in a traditional process.

Wangen et al. reviewed and evaluated multiple information security risk management frameworks and stated that ISO/IEC 27005 standard for information security risk management to be the most complete framework in comparison to other frameworks.

The literature review papers have been classified into two classifications: technical and informational. Technical classification refers to papers that proposed an information security risk management framework. Citation numbers for technical papers are (Singh and Joshi, Fenz et al., Fahrotuzi et al., Badamasi and Utululu, Putra and Matijarasa, Zhang, Zhang et al., Putra et al., Valerie et al., Bakaret et al. Hamit et al., Safonova et al., Monev, Sensuse et al., Argawal, and Wei et al.). Informational refers

to papers that provide information in regards to information security risk management whether it is to promote the idea of information security risk management or to emphasize the importance of implementing such mechanism or giving an overview over its approaches. Citation numbers for informational papers are (Chapman, Fenz et al., Custer, Nunes and Sergio, according to Brunner et al., Bergstromet et al., Aleksandrova et al. , Lanz and Sussam , Grishavea, and Borzov, Kaspersky lab's, Almomani et al., Alshafreef, and Wangen et al.). Next, in Table 2.1 Technical papers were further classified based on similarities of methodologies used, year of publications, results, limitations and uniqueness. Uniqueness column discusses the differences when a methodology is similar.

As per the literature review there are multiple approaches for information security risk management such as AURUM, OCTAVE and NIST 800-30. However, ISO/IEC 27005:2018 information security risk management approach has been selected to be the standard for X based on their business requirements, and due to the flexibility of the standard in which it was implemented in various fields for organizations and has been approved and recognized as the best fitted information security risk management approach. In this project, ISO/IEC 27005:2018 will be used with a consideration of Saudi Arabia's ECC-1:2018 controls and regulations. The difference between the proposed work and existing work is that it will propose an information security risk management framework with compliance to Saudi Arabia's laws and regulations in terms of information security risk management.

Table 1: Related Work Technical Papers Analysis

Citation No.	Year	Methodology	Results	Limitations	Uniqueness
Singh and Joshi	2017	OCTAVE	Implemented in university. Improvement of security.	Only network environment analyzed.	-
Fenz et al.	2011	AURUM approach, ISO27002 standard, NIST SP 800-30, Geman standard	Conducted twocase studies	in small to large enterprises.	-
Fahrotuzi et al.	2020	ISO27005	Output paper in theform of an information security risk management plan.	Their frame work was not implemented.	Used ISO 27005 with ISO 27002. Designed for Ministry of defense.
Putra and Matijarasa	2021		Results in an operational information security risk management design.	Their design can be refined to be more comprehensive.	Combined ISO 27005 method with NIST 800-30.

Citation No.	Year	Methodology	Results	Limitations	Uniqueness
Putra et al.	2020		Results in 26 impact scenario as highest rank and 12 priority impact scenario.	Depended on an expensive software for data collection and analysis. Results does not provide controls and recommendations.	Used ISO 27005 with ISO 27002. Designed for Telecommunication company.
Bakaret et al.	2019		Information security risk management framework.	Preliminary design was not implemented.	Designed for IoT in healthcare.
Whereas Hamit et al.	2020		Risk treatment plan.	Theirwork focused more on creating a risk treatment plan than proposing a continues framework.	Used ISO 27005 withISO 27001. Designed for protection of patient's data.
Safonova et al.	2020		A process approach on how to implement	They did not validate or implement	Used ISO 27005 with ISO 27001.

3 Methodology

This project is aiming to develop an information security risk management framework for an educational institute. In order to achieve that, we need to study the ISO/IEC 27005 standard, NCA's ECC-18:1 controls, and related works of experts, how to implement and adapt them. Then, develop an information security risk management framework with the Lucidchart tool. The utilized standards and controls can be represented in Microsoft Excel and validated against actual university information assets available at the institute. This will be achieved by classifying the risks based on the institute's business requirements and ISO/IEC 27005:2018. Microsoft Excel will be used to determine the criteria and other phases for this information security risk management approach and risk register.

At the beginning of this project, several meetings have been conducted with the main stakeholders, which are the institute's information security team. Based on the meeting with the stakeholders, data collection and requirements gathering have been done. It

was decided to adapt the ISO/IEC 27005 standard as an information security risk management framework. In this project, the ISO/IEC 27005 approach to information security risk management is used. The framework consists of six phases: Context Establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment and Risk Acceptance.
The phases are briefly explained as follows:

Context Establishment Phase: determines the basic criteria that we will follow for risk management and will be further explained.
Risk Identification Phase: identifies the assets, threats, and vulnerabilities related to the institute in order to identify threats in the next phase.
Risk Analysis Phase: calculates the impact level of assets and asset valuation rates that were identified in phases 1 and 2.
Risk Evaluation Phase: calculates risk value and determines risk priority with the use of a risk evaluation criteria.
Risk Treatment Phase: evaluates risk mitigation, risk acceptance, risk avoidance, and risk transfer. The choices in determining risk management come from the results of the risk assessment derived from the choices based on analysis and with a consideration of the opportunities that each asset has.
Risk Acceptance Phase: evaluates, monitors, and coordinates the risk management processes that have been determined. Implement the control recommendations that aim to reduce information security risk. While dealing with risks, it is essential to point out the responsible parties in the information security team to deal with each control.

The information security risk management framework is an iteration process framework. In all phases, risk should be monitored, documented, and reviewed. Moreover, risk should be communicated with all concerned parties and decision makers while being in compliance with NCA's ECC-2018 controls. Table 2 is used to evaluate the framework's compliance with ECC-2018. Figure 1 demonstrates the information security risk management framework phases as per ISO/IEC 27005.

Table 2: NCA's Cybersecurity Risk Management Controls

Cybersecurity Risk Management (CSRM) Controls **Objective**: to guarantee management of cybersecurity risks in an operational approach in order to protect organization's information assets.	
Control No.	Controls
1.5.1	CSRM approach must be defined, documented, and approved as per CIA reflection of information assets.
1.5.2	CSRM must be implemented in a cybersecurity function.
1.5.3	CSRM must be implemented in the following cases: 1-5-3-1 at early phases of technology projects. 1-5-3-2 before attempting

Cybersecurity Risk Management (CSRM) Controls **Objective**: to guarantee management of cybersecurity risks in an operational approach in order to protect organization's information assets.	
	major modifications to technology infrastructure. 1-5-3-3 through the planning stage of acquiring third party. 1-5-3-4 through the planning stage and before launching of new technology or online service.
1.5.4	CSRM approach and process must be reviewed continuously to planned intervals or upon modification to associated laws while being approved and documented.

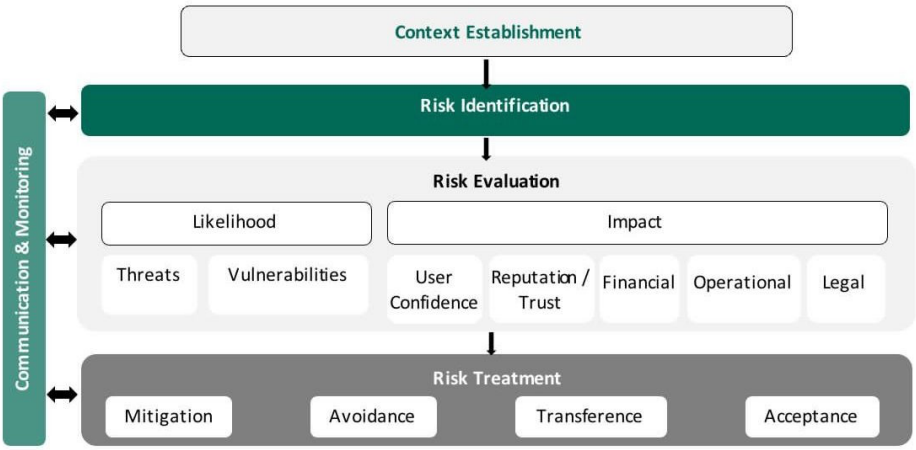

Figure 1 : Information Security Risk Management Framework for the educational institute

3.1 Phase 0: Data Collection

For the data collection phase, it was crucial that, for the applications in scope, we get accurate information from all the stakeholders and application owners and get their input on how important an application asset is to the organization and the impact of each application on the overall operation of software assets in the organization.
Data collection process was achieved by the following activities:
Meeting with application owners.
Meeting with the institute's stakeholders to understand the overall impact on business.
Impact analysis questionnaire designed to capture the levels of impact on the organization due to the loss of Confidentiality, Integrity, and Availability (CIA).

3.2 Phase 1: Context Establishment

The scope of the information security risk management procedure should be defined to guarantee that all assets and supporting systems are included in the risk management

process. The scope of the organization's risk management depends on its business drivers and objectives, the processes in place, and the available human and technological resources.
The following drivers should be taken into consideration when establishing and updating the scope and limitations of the risk management (ISO-ISO/IEC27005:2018):

- External drivers that can impact the strategic objectives of the organization. For example, changes in legal or regulatory requirements.
- Internal drivers that impact the internal environment of the organization

3.3 Phase 2: Risk Identification

Risk is the potentiality of loss, harm, or destruction of an asset as a consequence of a threat leveraging a vulnerability. The risk identification process determines the level of risk for each potential threat and vulnerability to the business assets. The risk must be identified as the occurrence of a threat against the asset due to the vulnerability that exists or may exist on the asset (ISO-ISO/IEC27005:2018). In the risk identification phase, the organization's assets will be identified, along with asset valuation criteria, identification of vulnerabilities and threats, and identification of the existing controls in the institute (ISO-ISO/IEC27005:2018).

3.3.1 Asset Identification

An asset is defined as any entity that holds value for the organization and that therefore requires safeguarding. Based on the scope of the risk assessment, all assets need to be identified based on the following asset categories: hardware, software, network, personnel, site, and organization (ISO-ISO/IEC27005:2018).

3.3.2 Asset Valuation

The next step after asset identification is to agree upon the scale to be utilized and the criteria for assigning a value to each asset. In this process, two options were used as asset valuation criteria. Business impact criteria are determined as per the reputational, public safety legal, operational, and financial impacts of the organization. The second option for asset valuation is CIA impact criteria. By assessing the CIA attributes of each asset, we can determine the asset value of each identified asset.
Asset Valuation - Business Impact Analysis. In this phase, we need to determine business impact criteria for the risk management framework. Risk ratings are determined as low, medium, high, and critical. The impact level is determined by the reputational level, public safety, legal and regulatory consequences, operational level, and financial impact level for the organization, as demonstrated in Table 3.
Asset Valuation - CIA Impact Analysis. CIA impact analysis has been conducted with the support of the information security team in the organization. CIA impact analysis consists of three categories: Confidentiality, Integrity and Availability. These categories are evaluated based on a set of questions as per ISO/IEC 27005 that must be answered for each asset to determine asset value (ISO-ISO/IEC27005:2018). The result of

the above questionnaires shapes the criticality of the asset in five dimensions from 1 to 5 using the weighted average of the CIA score and the following formula (ISO-ISO/IEC27005:2018):

ASSET VALUE= (SUMPROD- UCT

[Count of Yes (C1:C5);Count of Yes (I1:I5); Max(A1:A5)]) / (SUM[Count of Yes (C1:C5); Count of Yes (I1:I5); Max(A1:A5))

3.3.3 Identify Threats and Vulnerabilities

Before to calculating the effect and probability, we must determine the threats and vulnerabilities against each asset. A threat is any entity that can purposefully or inadvertently exploit a vulnerability to cause damage or destroy an asset. Threats may have a natural or human origin and may be unintentional or intentional. Both incidental and deliberate danger sources must be identified. An organization may face an internal or external threat. Threats should be recognized generally and by category (e.g., illegal acts, physical damage, and technological failures), and when necessary, individual threats within a generic class can be identified (ISO-ISO/IEC27005:2018).

3.3.4 Identify Existing Controls

Existing controls implemented by the management should be identified and their effectiveness weighed against the threats to avoid unnecessary work or cost in reducing the risk. Any planned controls as part of a development project or risk treatment plan should also be considered to avoid duplication. In addition, while identifying the existing controls, a check should be made to ensure that the controls are working correctly. A control library can be maintained within the ISRM risk register. This library will consist of all the security controls identified. It is important to identify controls from a strategic point of view, considering people, processes, and technology.

Table 3: Risk Evaluation and Impact Criteria for the Educational Institute (ISO-ISO/IEC27005:2018)

Rating	Reputational	Public Safety	Legal	Operational	Financial
Low	Limited effect to reputation	Insignificant injury or discomfort to one individual	No regulatory consequences or minor areas of improvements communicated by the regulation	Operational: Limited service disruption	Low or no financial impact to the organization
Medium	Considerable to reputation	Minor injury or discomfort to one individual	Recommendations considerable from regulator and or other stakeholders	service disruption	Moderate financial damage to the organization (1 to 499,999.99 SAR)

Rating	Reputational	Public Safety	Legal	Operational	Financial
			to improve Severe financial		
High	Serious loss to reputation at a National level	Significant injury to an individual or small group	Corrections and warnings from regulator and or other stakeholders	Serious service disruption	Severe financial damage to the organization (500,000 to 1 M SAR)
Critical	Catastrophic loss to reputation at an International level	Severe injury or loss of life to one or more individuals	High penalties from regulator And or other stakeholders	Prolonged service disruption	Severe financial damage to the organization (1 Million & above

3.4 Phase 3: Risk Analysis

In this phase, a risk register template via Microsoft Excel should be created as per the previously agreed-upon and defined criteria. Risk register was created for the organization. Furthermore, the analysis of impact levels of assets against each threat and the identification of impact rates and likelihood of occurrence of each vulnerability based on the organization's software and application assets that should be analyzed Impact analysis, CIA impact analysis, identification of threats and vulnerabilities, and identification of existing controls must be assessed and analyzed.

3.5 Phase 4: Risk Evaluation

Once the risks have been identified and documented, it is necessary to assess the size/significance of the risk. This is established by estimating the potential business impact of the risk if it were to occur and the potential likelihood of the risk occurring. Risk can be grouped into 2 categories: Inherent and Residual.

3.5.1 Inherent Risk Analysis

Inherent risk can be calculated using following formula (ISO-ISO/IEC27005:2018):
INHERENT RISK = ASSET VALUE + LIKELIHOOD + IMPACT

3.5.2 Residual Risk Analysis

Residual risk can be calculated using the following formula (ISO-ISO/IEC27005:2018):
RESIDUAL RISK = INHERENT RISK
– CONTROL EFFECTIVENESS

3.5.3 Assess Likelihood of Occurrence

Likelihood is the probability that an existing vulnerability will be successfully abused by identified threats. Once the threats have been identified, a valuation of the likelihood of their occurrence can be determined by the asset owner, user, manager, or other relevant entities. The likelihood of occurrence can be determined using the scale in Table 4.

3.6 Phase 5: Risk Treatment

Risk treatment includes identifying the series of choices for treating risks, assessing these options, and preparing and application of treatment plans. Risk treatment may involve a recurring procedure of evaluating a risk treatment, determining that existing risk levels are not acceptable, producing new treatments, and measuring the validity of those treatment options until a level of risk is reached that the educational organization can accept (ISO-ISO/IEC27005:2018).

3.7 Phase 6: Risk Acceptance

In this phase, the organization will evaluate, monitor, and coordinate the risk management processes that have been determined. Implement the control recommendations that aim to reduce information security risk. While dealing with risks, it is essential to point out the responsible parties in the information security team to deal with each control. Table 5 demonstrates the risk acceptance criteria for the organization's assets.

3.8 Communication and Monitoring

Continued monitoring and reporting are essential to ensure risks are identified, evaluated, and treated based on the organization's risk requirements in order to protect their environment from new and emerging cybersecurity threats. The information security risk management process will include a number of stakeholders as part of the risk audit and compliance activity to:

Align and update the information security risk register.
Report risk evaluation and risk treatment plan.
Get support and approval for risk treatment actions.

The identified information security risks must be populated within the risk register, and the associated assets, threats, vulnerabilities, and controls must be linked. The risk treatment plan must be integrated to allow for regular monitoring of the risk status per asset.

4 Results and Discussion

In this project, 43 of the educational institute's application assets have been analyzed in terms of information security risk management. These application assets have been evaluated with their associated threats, vulnerabilities, calculation of asset value, residual risks, control effectiveness, and risk treatment and option options. The analysis resulted in a 5 as Critical, 23 as High, 12 as medium and 3 as low impact. It resulted in a high-risk priority for 24 assets and a medium-risk priority for 19 assets. There were found to be inadequacies in the organization's asset management, system security testing, information security awareness, cryptographic controls, and malware protection. Risk treatment options were selected to mitigate the risks, and controls were recommended. There are four controls recommended from NCA's controls and 32 controls from ISO/IEC 27001. ISO/IEC 27001 controls were utilized as per the ISO/IEC 27005 recommendation.

Table 4: Likelihood Criteria (ISO-ISO/IEC27005:2018)

Score	Rating	Description
1	Rare	Once a year
2	Unlikely	Once in 3 months
3	Possible	Once a month
4	Likely	Once a week
5	Frequent	Once daily

Table 5: Risk Acceptance Criteria (ISO-ISO/IEC27005:2018)

Score	Rating
Acceptable Risk	Less than 7
Non-Acceptable Risk	7 and above

5 Conclusions

The information security perspective developed in this article reported on issues. Information security risk management is a major aspect to be considered by organizations in order to maximize their information security defense mechanisms. This project proposed an information security risk management framework for a governmental university in Saudi Arabia, adapting ISO/IEC 27005 standardization for information security risk management while evaluating its compliance with NCA's ECC-2018 controls. The framework consists of six phases: Context Establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment and Risk Acceptance. The framework proposed will strengthen the educational institute's software information security and organize their information assets in one framework to have full insights into all the

information assets they have. Furthermore, it will significantly decrease the information security costs for the organization. In this project, 43 software application assets have been analyzed, the criticality of their impact determined, existing controls identified, lists of threats identified, risk treatment options determined, and effective controls recommended to mitigate the risks associated with each asset.Further research needs to be conducted to set an example for other Saudi Arabia's universities to follow and implement this information security risk management framework. Moreover, to expand the scope of the risk analysis of information assets and analyze hardware and network assets in the information security risk management framework.

References

Singh, U. K., & Joshi, C. (2017). Information Security Risk Management Framework for University Computing Environment. Int. J. Netw. Secur., 19(5), 742-751.

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing?. Communications of the Association for Information Systems, 28(1), 22.

Fahrurozi, M., Tarigan, S. A., Tanjung, M. A., & Mutijarsa, K. (2020, October). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). In 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE) (pp. 86-91). IEEE.

Chapman, J. (2019). How Safe is Your Data?: Cyber-security in Higher Education (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.

Badamasi, B., & Utulu, S. C. A. (2021). Framework for Managing Cybercrime Risks in Nigerian Universities. arXiv preprint arXiv:2108.09754.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410-430.

Custer, W. L. (2010). Information security issues in higher education and institutional research. New Directions for Institutional Research, 146, 23-49.

Putra, I. M. M., & Mutijarsa, K. (2021, April). Designing information security risk management on bali regional police command center based on ISO 27005. In 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT) (pp. 14-19). IEEE.

Nunes, S. (2019). INFORMATION SECURITY RISK MANAGEMENT: A SYSTEMATIC LITERATURE REVIEW. Journal of Information System Security, 15(3).

Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. Computers & Security, 92, 101776.

Zhang, Z. (2020, December). A New Method for information security risk management in big data environment. In 2020 2nd International Conference on Information Technology and Computer Application (ITCA) (pp. 1-4). IEEE.

Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting information security risk management challenges: a practice perspective. Information & Computer Security.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010, June). Information security risk management framework for the cloud computing environments. In 2010 10th IEEE international conference on computer and information technology (pp. 1328-1334). IEEE.

Putra, S. J., Gunawan, M. N., Sobri, A. F., Muslimin, J. M., & Saepudin, D. (2020, October). Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company. In 2020 8th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.

Aleksandrova, S. V., Vasiliev, V. A., & Aleksandrov, M. N. (2020, September). Problems of implementing information security management systems. In 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) (pp. 78-81). IEEE.

V. G. Semin, E. G. Shmakova and A. B. Los, 2017, "The information security risk management," 2017 International Conference "Quality Management, Transport and Information Security, Information Technolo- gies", pp. 106-109, (IT&QM&IS)

Bakar, N. A. A., Ramli, W. M. W., & Hassan, N. H. (2019). The internet of things in healthcare: an overview, challenges and model plan for security risks management process. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 15(1), 414-420.

Hamit, L. C., Sarkan, H. M., Azmi, N. F. M., & Naz'ri, M. Adopting an ISO/IEC 27005: 2011-based Risk Treatment Plan to Prevent Patients from Data Theft.

Safonova, O. M., Lontsikh, N. P., Golovina, E. Y., Elshin, V. V., & Koniuchov, V. Y. (2020, September). Methodology for Creating, Implementing and System Effectiveness Evaluation of the Business Processes' Information Security System. In 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) (pp. 127-131). IEEE.

Lanz, J., & Sussman, B. I. (2020). Information Security Program Management in A COVID-19 World. The CPA Journal, 90(6), 28-36.

Grishaeva, S. A., & Borzov, V. I. (2020, September). Information security risk management. In 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) (pp. 96-98). IEEE

Kaspersky Lab (2020). Available at: https://www.kaspersky.ru

National Cybersecurity Authority, 2018. Essential Cybersecurity Controls(ECC-1:2018). Saudi Arabia,p.40.

Framework for higher education institutions in Saudi Arabia. PeerJ Computer Science, 7,e703.

Alshareef, N. (2016). A Model for an Information Security Risk Management (ISRM) Framework for Saudi Arabian Organisations. International Association for Development of the Information Society.

Monev, V. (2021, September). The" Self-Assessment" Method within a Mature Third-Party Risk Management Process in the Context of Information Security. In 2021 International Conference on Information Technologies (InfoTech) (pp. 1-7). IEEE.

Sensuse, D. I., Syahrizal, A., Aditya, F., & Nazri, M. (2020, November). Information Security Risk Management Planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik. In 2020 Fifth International Conference on Informatics and Computing (ICIC) (pp. 1-7). IEEE.

Agrawal, V. (2017, June). A framework for the information classification in ISO 27005 standard. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 264-269). IEEE.

Wei, Y. C., Wu, W. C., & Chu, Y. C. (2018). Performance evaluation of the recommendation mechanism of information security risk identification. Neurocomputing, 279, 48-53.

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. International Journal of Information Security, 17, 681-699.

ISO-ISO/IEC27005:2018-Information technology—Security techniques—Information security risk management, [online] Available: https://www.iso.org/standard/75281.html.References