INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Global Advanced Research Publication House Journal

Home page: www.ijaite.co.in

Study of Data Security Frameworks Implemented in University Environment

[1]Anup Ralegaonkar, [2]Dr. Nilesh Ware

[1,2]Department of Technology Management, Defence Institute of Advance Technology Girinagar Pune, Maharashtra, India

[1]anup.raleg@gmail.com, [2]nilesh.ware01@gmail.com

Article History

Received on: 12 Feb 2023

Revised on: 28 Feb 2023

Accepted on: 18 March 2023

Keywords: Information Security Framework, Standard, Strategy, University, And Higher Education Institutions.

e-ISSN: 2455-6491

DOI:

Production and hosted by
www.garph.org

ABSTRACT

University information infrastructure is frequently targeted by cyber attackers due to the large volume of critical data being handled by such institutions. University networks are generally designed for open and free access for students and staff with no centralised control. The purpose of this research paper is to study the literature describing different information security frameworks used by various academic institutions. The literature review was conducted in a systematic manner consisting of three important phases: planning, conducting and reporting the review. The process involves identification, interpretation and evaluation of the research that is carried out in to a particular field. The study has brought out that, ISO 27001, COBIT, ITIL and NIST are the most widely used information security standards worldwide. Hence, majority of researchers recommend, designing a customised security strategy for higher educational institution, which is based on one of the international standards. However, it was observed that, the scientific papers analysed for this study are not covering this important aspect in sufficient depth. Effective IT Governance and adhering to strict security policies within the institution, have been identified as effective methods to strengthen the information security. Case studies and surveys have been suggested for validation of the framework, during pre-implementation and post-implementation phases. The field of research has proved to be very interesting and highlighted specific issues about developing a comprehensive and cost-effective info security strategy for higher education institutions.

1. INTRODUCTION

In the recent past, the use of information technologies has increased considerably in higher education institutions. Moreover, the use of new technologies has become even more indispensable during COVID-19 lockdowns, to ensure continuity of the education process through online mode of knowledge delivery.

Access to information technology is very important for the development of modern learning environments. University provides extended Wi-Fi connectivity for students and staff, digitally connected libraries, online learning platforms such as Moodle, virtual classes and web conferencing through MS Teams, Zoom, WebEx etc. All this, makes university campuses one of the most technologically developed institutions, but on the other hand, it also increases the vulnerability of communication networks and associated threats [1]. University information systems had significant vulnerabilities even before the pandemic as they are generally designed for open and free access for students and staff with no centralised control. This exposes valuable academic and personnel data and makes them an easy target for cyber-attackers [2].

According to cyber security research conducted by IBM & Ponemon Institute [3], the education domain lost US $ 3.90 million alone in year 2020 due to data breach. Another study by CheckPoint [4] which is a leading provider of cyber security solutions globally, discovered that the average number of weekly cyber-attacks on academic institutions, increased by more than 20% in 2020 - 21.

The implementation of an information security management framework (ISMF) within the university is very important to ensure information security. The ISMF is a comprehensive solution which consists of detailed security policies, tools and procedures for strengthening cybersecurity and maintaining the information system [1]. There is enough work available on the info security strategies for all other sectors. However, the studies on ISMF for the education sector are very limited and lacks detailed procedure for implementation of security frameworks in higher education institutes [5]-[6].

The scope of this paper is to review the scientific literature in the field of "Information security framework for higher education institutions". The study attempts to identify important elements which will facilitate to evolve an ISMF, that is easy to implement and cost-effective. The main research objective is to identify the widely used info security frameworks/strategies for universities, worldwide. The research will mainly focus on following issues: analysis of the info security strategy for higher education institutions, identification and management of risk, functions and implementation phases of the security framework, and validation methods.

To achieve this goal, the search was performed in the main scientific databases such as, ACM Digital Library, ScienceDirect, Google Scholar, IEEE Xplore and Springer as these databases are the most widely used platforms for the study in the field of information security.

The article is organized as follows: initially, the method proposed for planning and conducting the literature review is discussed, the next part brings out the report of literature review which is based on the results found in first part, and finally, the conclusions of the author and future research directions are discussed in the last part.

2. RESEARCH METHOD

In this paper, a systematic literature review method which is specifically aimed at the Information Technology (IT) community, is used to study the literature. The systematic literature review involves identification, interpretation and evaluation of the research that is carried out in to a particular field. The systematic review process involves following three important phases: planning, conducting and reporting the review [7].

A. Planning the Literature Review

The planning stage includes the methods selected for the systematic review of the literature. The first step is to describe the background and establish the research questions.

There are several info security frameworks such as ISO 27001, NIST, COBIT, ITIL, which are used to implement the Information Security Management System (ISMS) within the organization. However, several researchers have pointed out that, all these frameworks are aimed at commercial organizations and there is no framework that is designed specifically to address the info security issues in the higher education institutions. Moreover, the existing international frameworks are difficult to align and implement for the academic institutions and are not cost-effective [8].

So, the main Research Questions (RQ) are:

- RQ1: What is the information security management framework recommended by researchers for university environment?
- RQ2: What are the mechanisms for identifying information security risks in a university environment?
- RQ3: What are the implementation phases of the information security framework in higher education institutions?
- RQ4: What are the relevant functions for the info security framework?
- RQ5: What are the methods for evaluating the effectiveness of the security framework?

Next, the search terms and resources were decided to search the maximum possible literature available on the internet. Literature review was carried out on scientific articles and international conference papers, indexed in popular databases such as ScienceDirect, ACM Digital Library, IEEE Xplore, Springer. The search was performed using the metadata: the title, the keywords and the abstract of the scientific article; based on the search terms as given below:

- [Information Security Management Framework] or [Information Security] or [Cyber Security] or [IT governance] and

- [Policies] or [Standard] or [Strategy] and
- [University] or [Higher Education Institutions] or [Academic Institution] or [College].

Inclusion Criteria for the Articles: The main inclusion criteria for this research are to include previous studies on information security in education sector. The literature published during last ten years was taken into consideration for inclusion in the search criteria. The IT sector is very dynamic and changing very rapidly. Hence, the relevant papers, which are not outdated, were selected carefully for analysis. The detailed inclusion criteria for the search are as given below:

- Research papers that describe information security management in academic institutions.
- Research presenting tools or policies relevant to the implementation of the security standard/framework in a university environment.
- White papers, technical reports or websites dedicated to above mentioned topics.

Exclusion Criteria for the Articles

- Literature not written in English
- Studies that do not directly focus on information security framework related topics (e.g., papers on cybersecurity education, legal issues, or issue specific topics in higher education).
- Studies published in the year 2010 or older.
- Inclusion of reports from security vendors have been restricted to those either containing empirical data on academic institutions or containing expert insights.
- News reports and articles have not been included in the study.

B. Conducting the literature review

Total 212 scientific papers were searched according to the search criteria; however, a large number were excluded because they were not relevant as per the inclusion criteria decided in the previous step, or because they matched the exclusion criteria. Total 82 articles were selected for study and further 36 articles were excluded after abstract reading. So finally, 46 articles were analysed as per the results given in table 1.

C. Results of the literature review

The results of the literature review to answer the research questions (RQ1-RQ5) are discussed in succeeding sections.

3. RQ 1: ISMF RECOMMENDED BY RESEARCHERS FOR UNIVERSITY ENVIRONMENT

It is very important for universities to establish security policies and control measures. "The security framework is a complete solution that contains security policies, tools and procedures for strengthening cybersecurity and maintaining the information system" [8]. In other words, Information Security framework provide a complete solution for implementation of an Information Security Management Systems (ISMS) by combining policies, tools and procedures for enhancing and maintaining a secured information system [9]-[10]. The search criteria used to identify the literature on the internet for the recommended ISMF for university environment are: recommended information security framework/standard for higher education institution.

Table 1: Search Results

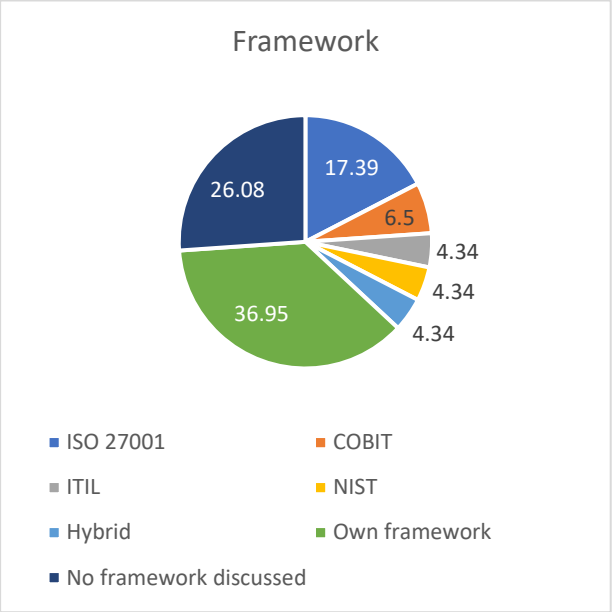
Source	Applied filters	No. of selected articles
ScienceDirect	Title, Abstract, Keywords	13
Scopus	Title, Abstract, Keywords	9
Google Scholar	Title, Abstract, Keywords	10
IEEE Xplore	Title, Abstract, Keywords	7
ACM Digital Library	Title, Abstract, Keywords	3
Springer	Title, Abstract, Keywords	4
Total		**46**

In order to answer the RQ1, the selected papers were analysed to identify the recommended frameworks/standards for the university environment. The results of the analysis are given in Table 2 and Fig 1. It can be concluded that the standardized security frameworks recommended by most of the researchers are: ISO27001, COBIT, ITIL and NIST or hybrid solution. Many researchers have also pointed out that the

standards listed above are not designed for implementation in academic institutions and hence, suggested to derive own infosecurity strategy based on any of the standardised framework.

Table 2: Recommended Information Security Standards for Higher Education Institutions

Criterion	Framework	Scientific Paper	%
Recommended info security framework/standard for higher education institutions	ISO 27001	8	17.39
	COBIT	3	6.5
	ITIL	2	4.34
	NIST	2	4.34
	Hybrid	2	4.34
	Own framework	17	36.95
	No framework discussed	12	26.08
Total		**46**	**100**



Out of total 46 articles selected for the study, use of ISO27001 has been recommended by 8 researchers, 3 scientific articles recommend COBIT, ITIL and NIST is recommended by 2 articles each and 2 other articles recommends the hybrid version, which is a combination of all the 4 standards. Majority of the researchers (17) have recommended deriving own framework as the existing frameworks are not suitable for the education institutions.

4. Analysis of Security Frameworks

The recommended security frameworks for implementation in academic institutions are discussed in the following section.

ISO 27001

ISO 27001 standard is the most widely used information security standard worldwide [10]. In education sector as well, increasing number of educational institutions are opting for ISMS ISO 27001 certification. As per the annual reports published by ISO, total 137 higher education institutions opted for ISO 27001 certification in year 2018 internationally while the number increased to 176 institutions in 2019. Most ISO 27001 certified education institutions are in Japan, Greece, Italy, Poland, and the Czech Republic [11]-[12].

A. Confidentiality, Integrity, Availability (CIA) Triad

The ISMS ISO 27001 is implemented for protection of information assets which mainly focuses on three main principles of info security: confidentiality, integrity and availability, popularly known as CIA Triad [11]-[13]-[14].

Confidentiality measures are designed to prevent unauthorized users from accessing sensitive information. It ensures that only authorized persons can have access to organization data.

Integrity ensures maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data should not be changed during storage, transit, and steps must be taken to ensure data cannot be altered by unauthorized people.

Availability means information is readily accessible for authorized parties whenever required. It ensures properly maintaining technical infrastructure and systems that hold and display the information.

B. Plan-Do-Check-Act (PDCA) Cycle

The ISO 27001 standard involves creation of an information security management system (ISMS) within the institutions. For the implementation of ISMS, ISO 27001 uses the PDCA model (Planning, Implementation, Verification and Action) [13], as shown in figure 2.

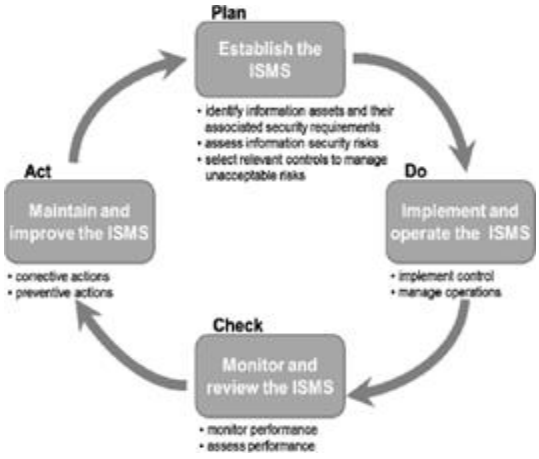


Figure 2: PDCA Cycle for ISMS ISO 27001

Information security is not just about Information Technology (IT) and depends more on the human factors than on the various technologies used. The security threats due to careless attitude of the employees of an organization are far more compared to the threats from external people. Hence, ISO 27001 standard also contains specific controls for human resource management, organizational management and legal constraints [10]-[11].

The ISO 27001 standard is organized into 14 sections, 35 objectives and 114 security controls. All sections of the standard are not applicable for higher education institutions, as the standard is primarily developed for non-academic and commercial organizations. For higher education institutions, it is recommended to use at least 8 sections: asset management, human resources management, physical controls, access control, communications control, operational control, incident management, information system control and business continuity. Due to the generalised nature of ISO 27001 standard, it is difficult to identify the targeted strategy specifically for educational institutions. [9], [15].

C. Control Objectives for Information Technology (COBIT)

COBIT standard is developed by Information Systems Audit and Control Association (ISACA), which is an international professional association focused on IT.

COBIT describes effective practices and establishes specific activities for info security in an organized and flexible manner. COBIT mainly focuses on generating a structured set of principles, such as IT assets, organizational requirements and information security processes. It facilitates creation of IT control policies and promotes best practices at the organizational level [16]. Most of the organizations implements some controls to ensure information security. COBIT provides a well-defined strategy consisting of check lists and industry best practices. This facilitates an auditor or even to the common user, to assess info security risks, depending on the controls implemented and the technical problems faced by the organization [17].

Similar to ISO 27001, COBIT is also focused on risk management and IT Governance. According to COBIT, "control objectives mainly refer to policies, procedures, practices and organizational structures that ensure the organization's objectives". It has proved very useful for early detection and prevention of any undesired activity [16]. The COBIT Framework principle is shown in Fig 3.

COBIT consists of 34 IT processes and 13 control objectives. Each process is described by a RACI diagram, which shows the role of each process in a managerial activity. All activities have a detailed structure and are identified from the control objectives. COBIT controls are mainly focused on achieving organizational objectives. It was suggested that the model should comply with the controls of the ISO 27001 standard, in order to achieve an optimal level of cyber security. The researchers have recommended to use COBIT in the educational environment, mainly to evaluate IT processes and to verify the maturity level of the model used [14]-[16].

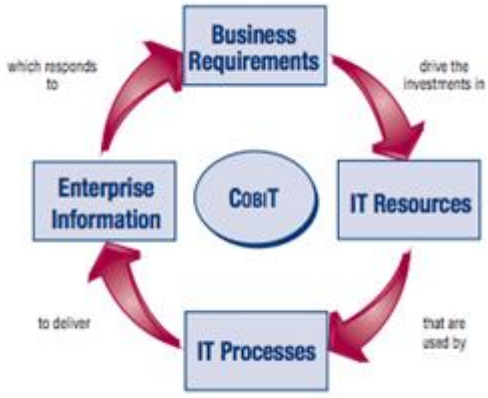


Figure 3: COBIT Framework Principle

D. Information Technology Infrastructure Library (ITIL)

ITIL provides a set of detailed practices for IT activities, such as IT asset management and IT service management (ITSM), that mainly focus on aligning IT services with the business needs. ITIL consists of procedures, processes, and checklists that are not necessarily specific to an organization or technology, but are still applicable towards wide range of organizational strategies.

ITIL is a library containing a set of 5 books and 26 processes that provides a systematic approach to IT Governance, operations management and control of IT services [18]. The ITIL standard

provides an association between different processes and operations for better management of IT services. These services are characterized as a means of providing value to customers without increasing info security risks or cost [17]. The ITIL Framework is as shown in the figure 4. It mainly consists of three phases: Service Design, Service Transition and Service Operation.

Figure 4: ITIL Framework

As in the case of COBIT, the ITIL standard is also recommended to be used in combination with the ISO 27001 standard. The combination of both the standards, will integrate the security practices recommended by ISO 27001, with the best process management services recommended by ITIL. This will help provide effective risk management and reduce the costs of maintaining an acceptable level of security at all levels [17].

E. National Institute of Standards and Technology (NIST) Cyber Security Framework

The NIST Cybersecurity Framework is published by National Institute of Standards and Technology at the US Dept of Commerce. The standard is mainly developed to help private organizations, to implement cybersecurity strategies. The framework provides standards, guidelines and best practices to facilitate the protection of information and information systems.

The NIST cyber security framework mainly consists of three parts: Framework Core, Framework Implementation Levels and Framework Profiles as shown in Fig 5.

The framework components mainly define the alignment of cyber security functions, categories, and subcategories with business requirements, risk tolerance, and resources of the organization (Fig 6). It enables

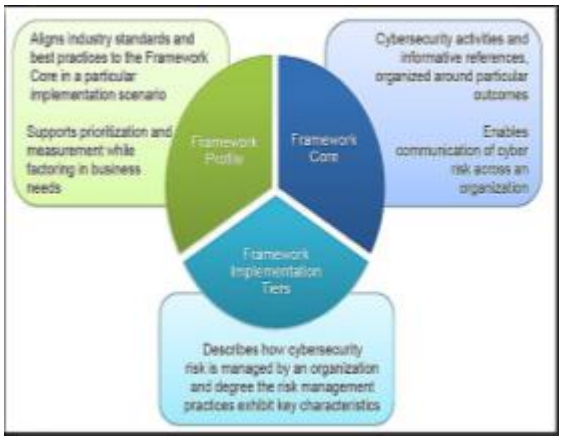


Figure 5: NIST Framework Components

organizations to establish a roadmap for reducing Cybersecurity risk that is aligned with organizational and sector goals, industry best practices, considers legal/regulatory requirements and reflects risk management priorities. The framework is used to describe current state of cyber security, identify gaps in the present setup and derive target state of desired Cybersecurity activities [19].

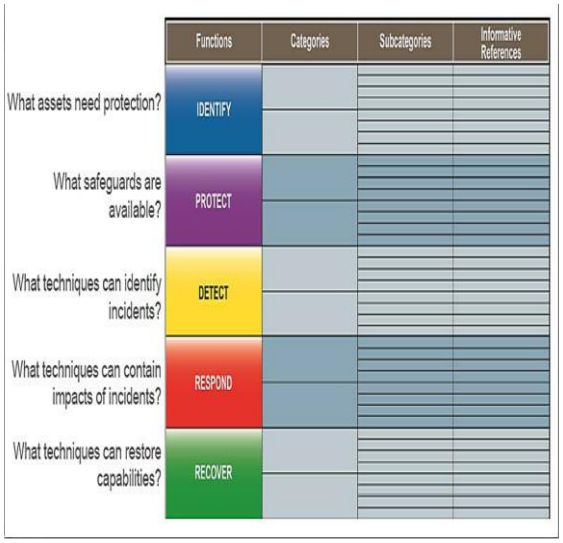


Figure 6: Framework Core Structure

The NIST Cybersecurity Framework provides a detailed classification of cybersecurity outcomes and a methodology to assess and manage those outcomes. It is intended to help private sector organizations to protect critical information infrastructure, along with relevant protections for privacy and civil liberties.

F. Hybrid Strategy

The hybrid strategy is recommended by several studies [17], [20]. The Hybrid strategy entails alignment of ITIL, COBIT and ISO27001 standards

to allow the implementation of a more comprehensive information security management system. The researchers generally agreed that ISO27001, COBIT and ITIL, are the most popular standards that can be combined and adapted as per the requirements of the organization [21]. ISO27001 mainly focuses on information security management, while ITIL and COBIT focus on information security and the relationship between project management and IT Governance [22].

One of the arguments used to combine the three standards is that, monitoring is the key process in order to provide efficient IT services. Thus, it is recommended to use COBIT for evaluation and monitoring at the highest level, by establishing a general control framework which will be applicable to any type of organization. Specific strategy for the education institutes can be devised by associating the processes recommended by ITIL with the ISO27001 controls and the general COBIT framework. The recommended association between three standards is shown in Table 3 [17]. Although it would appear that these three standards contain identical clauses, but the implementation requirements are very different, which drastically affects the implementation process, especially the budget. Therefore, before using any of the recommended standards, it is necessary to assess the implementation costs, which are usually a major constraint within the university.

Table 3: Combining Security Standards

COBIT 4.1	ITIL V3	ISO 27001
Service support DSS02 Service and incident demand management AP011 Quality management	Service Office	6.3.2 Reporting security vulnerabilities
DSS02 Problem and Incident Management	Incident Management	13.2.1 Establishing Liability for Incidents and Procedures
DSS04 Problem management	Problem management	13.2.1 Establish responsibility in case of incidents and procedures
BAI010 Configuration management	Configuration management	
BAI106 Change management	Change management	10.5.1 Modification of control procedures 8.2.1 Control of operational changes
BAI106 Change Management	Launch Management	10.4.1 Operational Software Control 10.5.2 Technical review of operating system changes
Service delivery APO09 Management of service agreements	Service level agreements	4.2.2 Security requirements for third parties 10.2.1 Management of agreements for services provided by third parties
APO006 Budget and cost management	Financial management	
DSS04 Continuity Management	Continuity Management	14 Business Continuity Management
BAI04 Availability and capacity management	Capacity management	8.2.1 Capacity planning
BAI04 Availability and capacity management	Availability management	8.5.1 Network control 9.5.5 Use of system utilities

Summary

As discussed above, many researchers have recommended ISO27001 standard for use within the higher educational institutions. So, it can be concluded that it is the easiest standard to implement, and implementation costs are lower compared to COBIT, ITIL and NIST. Even those researchers who recommended to implement their own strategies, does not deny the need for ISO 27001 certification, to have international recognition. ISO 27001 has emerged like English language, which has a proven international value.

5. RQ2: Risk Management Framework for University Information Infrastructure

The information security management system (ISMS) mainly focusses on risk management in the context of confidentiality, integrity and availability (CIA) of data, related to the critical information

assets in a university. Risk management lead to info security policy creation that can help reduce the risks to important processes, financial losses or damage to reputation of the university due to loss of confidential data [23], [24]. Hence, analysing the recommended risk management strategies, along with the identification of ISMS, is an integral part of the ISMS implementation process in higher education institutions.

Risk management, which is integrated with the ISMS, has become absolutely essential, because of the increasing need for implementation of information technologies in the university environment [25]. Risk management mainly includes 3 processes: Risk Assessment, Risk Estimation and Risk Mitigation.

There are several models available for risk management, with the common aim of determination of value estimation of risk. These models are mostly classified as qualitative or quantitative models. The main purpose of applying a risk management model within the institute, is to quantitatively and qualitatively measure the level of risk for university assets. The model should be selected carefully, to include security controls, that are based on the actual risks to the organization's assets and operations [1], [26].

The study of literature has identified that the main recommended models for risk management in educational institutions are: ISO 27005, OCTAVE and OCTAVE Allegro, which is shown in Table 4. Few scientific papers have also recommended the use of risk management strategies based on the network penetration tests, to identify security risks [27]. However, although risk management is a mandatory process for implementation of ISMS, much of the research in this field has not included any mechanism for risk management in the university.

Table 4: Risk Management Framework

Criterion	Risk Management Framework	Scientific Paper	%
Standard Risk Management framework	ISO 27005	5	10.86
	OCTAVE/ OCTAVE Allegro	7	15.21
	Own framework	8	17.39
	No framework discussed	26	56.21

A. ISO 27005

ISO 27005 is an international standard recommended by various researchers that mainly contains step by step approach for risk management [10]-[14]. The information assets of any organization are mainly classified into two types: primary assets and support assets. The primary assets are all the processes and activities specific to the organization; whereas the assets like hardware, software/applications, network, staff, website are classified as support assets [26].

As per ISO 27005 standard, classification of cyber security vulnerabilities according to the asset class to which they belong, is an important step for risk management. There are a number of vulnerabilities in the information infrastructure that need to be analysed for risk management. Some of the common vulnerabilities are discussed below:

Hardware components may get affected by moisture, dust, dirt and unprotected storage [10]; Vulnerabilities in software applications can be easily exploited by unauthorized persons, if not sufficiently tested before being put to use. Internal/external testing of software applications minimize cyber security risk [27]–[29];

- Communication networks, unprotected transmission lines or network architectures that do not use specialized security devices such as firewalls, are prone to frequent cyber-attacks [30];
- Computer users, if not trained properly are the biggest threat to information security. 90% of all cyber-attacks happen due to human negligence [31];
- Unavailability of information assets when needed, the risk that university web sites will not be accessible due to DDOS/DOS attacks is quite high. Similarly, the power failure that can cause disconnection of servers on which web pages are hosted, is quite ubiquitous [32].

B. Operationally Critical Threat Asset and Vulnerabilities Evaluation (OCTAVE)

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a methodology used to identify and evaluate information security risks. It is a collection of techniques, methods, and tools for evaluating information security risk assessment. OCTAVE defines a risk-based strategic assessment and planning technique for ensuring info security. The OCTAVE model works by identifying the causes that make the university information system vulnerable to attacks. The model is very useful for risk management and is often implemented in university security models to reduce the risk of cyber threats. It involves, first identifying university assets, and then evaluating asset-specific vulnerabilities and threats [1]-[33].

OCTAVE list specific activities to be carried out in 3 phases, that can be easily implemented in the university environment. The first phase consists of dynamically identifying the weaknesses in the system, i. e. each new technology added is first subjected to risk analysis before use. The second phase focuses on high-risk areas, for which the risk score published in Common Vulnerability Scoring System (CVSS) is used to validate the vulnerability. The final phase involves the creation of a security risk remediation plan to monitor risk assessment activities [1], [33]. The main steps defined for implementing the OCTAVE model are: identifying information assets, identifying and evaluating security vulnerabilities, understanding security requirements, analyzing the effectiveness of security controls, assessing risk through the frequency and impact of cyber threats, designing remediation plans and making decisions based on comprehensive security reports [1] (Fig 7).

The OCTAVE model facilitates creation of a well-defined structure for info security associated with the academic environment, and hence is recommended by many researchers for implementation in higher educational institutions. It is also very cost effective as it focuses only on critical assets that are at risk [1]-[33].

Figure 7: OCTAVE Process

C. OCTAVE Allegro

OCTAVE Allegro is the latest version of the OCATVE framework. It provides a methodology to streamline and optimize the process of information security risk assessment, with a small investment in time, people, and other limited resources. OCTAVE Allegro has been recommended by researchers because it allows a more comprehensive assessment of the operational risk environment, without the need of extensive knowledge about risk assessment [24]. This approach differs from the previous OCTAVE approach. The OCTAVE-Allegro focuses more on information assets, especially where the data is stored and processed, how it is transported, how the data is exposed to threats, potential vulnerabilities, and disruptions. The OCTAVE Allegro method is implemented in eight steps which are organized into four stages as follows [23] (Fig 8):

- Establish drivers
- Assets profile
- Identifying threats
- Identify and mitigate risk

OCATVE Allegro model offers several advantages, as the score associated with the information risk is calculated based on the quantitative assessment of the threat. For example, if for a university, the loss of reputation is the most important factor, then it will be assigned a higher score and higher risk mitigation measures [24].

6. RQ3: Implementation Phases of an Information Security Framework

The RQ3 is based on implementation phases of an info security framework for the educational institutions. It is necessary to know the implementation phases for deciding a relevant security framework for the university. The best of the info security framework also, if not implemented correctly, can cause severe damage to the organization instead of benefits. This section mainly attempts to find the details about the implementation of the info security framework recommended by researchers.

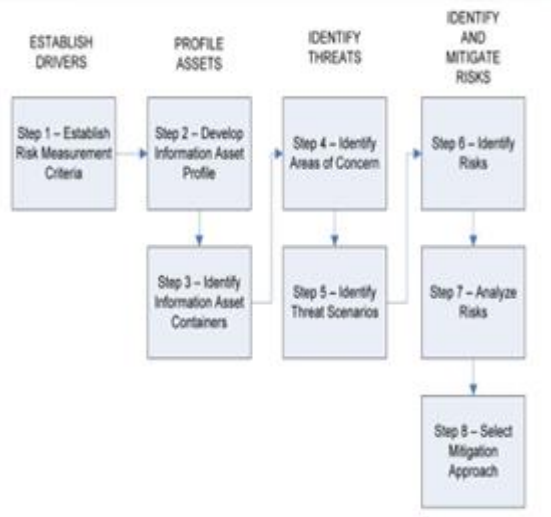


Figure 8: Eight steps and four phases OCTAVE Allegro model

The study has attempted to identify the widely used implementation phases recommended for the info security model within the university. Szczepaniuk E, et.al [34], suggested the classification for info security implementation phases in public organizations. As per his research, there are six phases of implementation of info security models in public organizations: formulating security policies, defining the purpose, security risk assessment, risk management, selection of controls, and deciding the applicability.

These phases were taken into account to identify the implementation phases suggested by the research papers. The summary of the research papers that has discussed implementation phases is given in Table 5.

The phases are non-exclusive, i. e. an article may include 1 or more phases. Thus, 8 scientific papers were found focused on formulating security policies, 5 papers on defining the purpose, 10 papers each on security risk assessment and risk management, 11 papers on the selection of security controls and 10 papers on the declaration of applicability.

Table 5: Info security Framework Implementation Phases

Implementation Phases of info security framework in higher education institutions	No of papers	%
Formulating security policies	8	17.39
Defining the purpose	5	10.86
Security risk assessment	10	21.73
Risk management	10	21.73
Selection of controls	11	23.91
Declaration of applicability	10	21.73

7. RQ4: Information Security Framework Functions for University

It is necessary to analyse the functions of the info security framework in order to develop an efficient strategy that will enhance information security in the university. In this regard, the RQ4 has been defined to review the selected scientific articles and identify the important functions considered relevant by researchers for an effective info security framework.

To answer RQ4, it is necessary to identify the relevant functions of an info security framework in higher education institutions. NIST standard has defined five functions of the security framework: identification, protection, detection, response, and recovery [29] as shown in Fig 6 above. It was found that the scientific papers analyzed for this study have discussed one or more functions simultaneously. The summary of the research papers that has discussed relevant functions of the framework are given in Table 6.

Thus, 14 papers are focused on identifying infosecurity risks, 16 papers on the protection of information assets, 12 research papers focus on detecting threats and vulnerabilities in the university information system, 5 papers are focused on making strategies to respond to info security breach incidents and 3 works on the implementation of incident response plans for mitigating security incidents. It can be concluded that, researchers have recommended the important functions of the infosecurity framework for the university environment, as: Identification (30.43%), Protection (34.78%) and Detection (26.08%). However, comparatively, less research material is available on Response (10.86%) and Recovery (6.52%).

Table 6: Functions of Info security framework

Relevant functions of info security framework for higher education institutions	No of papers	%
Identify	14	30.43
Protect	16	34.78
Detect	12	26.08
Response	5	10.86
Recovery	3	6.52

8. RQ5: Evaluate Effectiveness of the Infosecurity Framework in University Infrastructure

Two research criteria are generally defined by researchers to evaluate the effect of the implementation of the info security framework in a university: The operational architecture on which the framework is based, and the validation methods through which the effectiveness of the security framework can be tested.

A. Operational Framework Architecture

In most of the research papers analysed, it was noted that the analysis and evaluation of the implemented security strategies is mainly based on three criteria: IT Governance, security policies, and proposed security objectives.

IT Governance (ITG): IT governance (ITG) can be defined as a set of structures, processes, and mechanisms that support the top hierarchy to ensure efficient management of the organization's IT resources. Thus, ITG can be described as a guide for the implementation of the information security control system. Some researchers pointed out that efficient management of the university IT infrastructure is possible through the implementation of ITG [16]-[18]-[35]-[36].

Universities are complex organizations carrying out the process of teaching, learning, and conducting research activities. This necessitates the use of different types of information systems such as computer applications, software platforms, academic systems, cloud applications, etc; which make the system totally heterogeneous in nature. It has been emphasized that the implementation of ITG is essential to manage the efficient use of heterogeneous university IT resources [35]-[37]. Effective IT Governance includes participation and interaction between IT administrators and users. It also includes educating employees and students to match the institution's expectations with user behaviour. ITG is also involved in creating platforms for the distribution of best security practices within institutions (for e.g., EDUCAUSE in the USA and UCISA in UK), and the certification of specialists in this regard [16]-[18]-[35].

Security Policy: The aim of security policies is to provide guidelines for the end users on the safe and secure use of information assets. A well-structured security policy enables top management to address information security risks and ensure the implementation of appropriate security controls. The research has found that some higher education institutions develop a single document containing all security policies and procedures, while few other institutions develop different documents as per the best practices defined in ISO 27001. Some researchers have recommended that security policies are the best strategy for ensuring information security in the case of university IT networks [25], [38].

Control Objectives: Control objectives help to reduce info security risks associated with data, such as the risk of data loss, by enforcing data security policies and best practices. Controls such as software and hardware access restrictions and protocols for data handling can help Keep data safe and accessible. There are three primary areas or classifications of control objectives namely: management control objectives, operational control objectives and physical security control objectives (Fig 9).

Figure 9: Three Categories of Security Controls

Management control objectives also referred to as administrative controls, provide the overall design of organization info security controls. These controls provide the guidance, rules, and procedures for implementing a security environment in the university. Operational control objectives also referred to as technical controls, provide the measure for the effectiveness of controls. These include access controls, authentication mechanisms, and security topologies applied to networks, systems, and applications. The physical security control objective is the protection of data, hardware, etc., from physical threats that could harm, damage, or disrupt operations or impact the confidentiality, integrity, or availability of systems and data [39].

B. Recommended validation methods

The validation methods are essential to test the efficacy of the proposed info security framework. These methods are generally applied in the pre-implementation and post-implementation phases. The common validation methods suggested by researchers to analyse the efficiency of the model are:

- Case studies (14 articles) that include the analysis of info security system and network penetration tests [25]-[38], and
- Surveys (12 articles) that include the interview and the Delphi method [40]. The summary of the articles is shown in Table 7 below.

Table 7: Validation Methods

Validation Method	No of Papers	%
Case Studies	14	30.43
Survey (Interview and Delphi methods)	12	26.08
Not provided	20	43.47

9. FINDINGS

This study was initiated to answer the main research question (RQ1): "What is the information security management framework recommended by researchers for the university environment?" The aim was to identify important contributing factors of the information security framework, with an aim to strengthen the security in higher education institutions.

As the technologies in IT sector are very dynamic and changing rapidly, the research papers that are published after 2010 and are not outdated, were selected carefully for analysis. A sincere effort was made to identify the info security frameworks which are recommended and analysed by researchers worldwide, for

implementation in the university environment. Other research questions (RQ2 – RQ5) which are based on risk analysis, implementation phases, and functions of the framework as well as the validation methods to test the effectiveness of the framework, helped to analyse the subject in great detail.

The findings of the study, which provided answers to all the research questions are summarized below:

- In order to have international value, the majority of the researchers recommend deriving their own information security framework based on ISO 27001 certification. It is necessary to identify and include security controls in the framework, which are focused on university information assets.
- Risk management is identified as a key activity to implement an effective info security framework. Risk mitigation plans are designed by estimating the impact of the security risks on the information assets of the university. The research papers that included risk management strategies, recommended the use of the ISO 27005 and OCTAVE Allegro model for risk management in academic institutions.
- The implementation phases of the security frameworks were described in some of the selected articles. However, no article could be found that comprehensively discusses all the phases recommended for the implementation of ISMS in academic institutions.
- The researchers identified the following relevant functions that the academic institution-oriented info security framework should perform: Identification, Protection, Detection, Response, and Recovery.
- The validation methods recommended for educational institutions are case studies, and surveys. These methods are mainly used to identify the strengths and weaknesses of a security framework which is a very important step in evaluating a security framework.

CONCLUSION

International info security standards, such as ISO 27001, COBIT, ITIL or NIST, are mainly designed for non-academic organizations, and hence are not cost-effective and more difficult to implement in the university environment. Certification costs for these standards are also high, whereas the IT security budget in the university is always limited. Hence, most of the researchers have recommended designing their own security models for implementation in educational institutions. Such models can be aligned to the institutional requirements and modeled to fit into the budgetary constraint of the institution. However, while developing the security model for the institution, it is advisable to take into account the security controls proposed by international standards such as ISO 27001, as it has excellent controls, which have proven very effective over time and are internationally appreciated.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

FUNDING SUPPORT

The author declares that they have no funding support for this study.

REFERENCES

[1] C. Joshi and U. K. Singh, "Information security risks management framework – A step towards mitigating security risks in university network," J. Inf. Secur. Appl., vol. 35, pp. 128–137, Aug. 2017, doi: 10.1016/j.jisa.2017.06.006.

[2] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, Aug. 2014, doi: 10.1016/j.jcss.2014.02.005.

[3] IBM, "Cost of a Data Breach Report. Ponemon Institute and IBM, 2020. Available online: https://www.ibm.com/security/digital-assets/cost-data-breach-report."

[4] Check Point, "Cyber Security Report. Check Point Research, 2020. Available: https://www.checkpoint.com."

[5] S. Hina, D. D. D. Panneer Selvam, and P. B. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," Comput. Secur., vol. 87, p. 101594, Nov. 2019, doi: 10.1016/j.cose.2019.101594.

[6] I. Scalabrin Bianchi, R. Sousa, and R. Pereira, "IT governance Mechanisms at Universities: An Exploratory Study," Aug. 2017.

[7] B. Kitchenham, "Procedures for Performing Systematic Reviews," Keele UK Keele Univ, vol. 33, Aug. 2004.

[8] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," Ann. Telecommun., vol. 76, no. 3–4, pp. 255–270, Apr. 2021, doi: 10.1007/s12243-020-00783-2.

[9] S. K. S. Cheung, "Information Security Management for Higher Education Institutions," in Intelligent Data analysis and its Applications, Volume I, vol. 297, J.-S. Pan, V. Snasel, E. S. Corchado, A. Abraham, and S.-L. Wang, Eds. Cham: Springer International Publishing, 2014, pp. 11–19. doi: 10.1007/978-3-319-07776-5_2.

[10] A. Itradat, S. Sultan, M. Al-Junaidi, R. Qaffaf, F. Mashal, and F. Daas, "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study," Financ. Sci. Res. Support Fund, vol. 8, p. 102, Jan. 2014.

[11] A. Alexei, "ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE REPUBLIC OF MOLDOVA THROUGH THE ISO 27001 STANDARD," J. Soc. Sci., vol. IV(1), Mar. 2021, doi: 10.52326/jss.utm.2021.4(1).11.

[12] A. Alexei and A. Alexei, "Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning," Int. J. Sci. Technol. Res., vol. Volume 10, pp. 128–133, Mar. 2021.

[13] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," J. Inf. Secur., vol. 04, no. 02, pp. 92–100, 2013, doi: 10.4236/jis.2013.42011.

[14] W. Yustanti, A. Qoiriah, R. Bisma, and A. Prihanto, "An analysis of Indonesia's information security index: a case study in a public university," IOP Conf. Ser. Mater. Sci. Eng., vol. 296, p. 012038, Jan. 2018, doi: 10.1088/1757-899X/296/1/012038.

[15] D. E. I. Esparza, F. J. Diaz, T. K. S. Echeverria, S. R. A. Hidrobo, D. A. L. Villavicencio, and A. R. Ordonez, "Information security issues in educational institutions," in 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, Jun. 2020, pp. 1–7. doi: 10.23919/CISTI49556.2020.9141014.

[16] R. A. Khther and M. Othman, "Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review," Int. J. Inf. Technol. Converg. Serv., vol. 3, no. 1, pp. 21–29, Feb. 2013, doi: 10.5121/ijitcs.2013.3102.

[17] M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann, and K. Sakurai, "An Analysis of IT Assessment Security Maturity in Higher Education Institution," in Information Science and Applications (ICISA) 2016, vol. 376, K. J. Kim and N. Joukov, Eds. Singapore: Springer Singapore, 2016, pp. 701–713. doi: 10.1007/978-981-10-0557-2_69.

[18] M. Gërvalla, N. Preniqi, and P. Kopacek, "IT Infrastructure Library (ITIL) framework approach to IT Governance," IFAC-Pap., vol. 51, no. 30, pp. 181–185, 2018, doi: 10.1016/j.ifacol.2018.11.283.

[19] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[20] Athabasca University, Canada, S. Haji, Q. Tan, Athabasca University, Canada, R. S. Costa, and University of Zaragoza, Zaragoza, Spain, "A Hybrid Model for Information Security Risk Assessment," Int. J. Adv. Trends Comput. Sci. Eng., pp. 100–106, Feb. 2019, doi: 10.30534/ijatcse/2019/1981.12019.

[21] R. Almeida, R. Lourinho, M. Mira da Silva, and R. Pereira, "A Model for Assessing COBIT 5 and ISO 27001 Simultaneously," in 2018 IEEE 20th Conference on Business Informatics (CBI), Vienna, Jul. 2018, pp. 60–69. doi: 10.1109/CBI.2018.00016.

[22] H. Susanto, M. N. Almunawar, and Y. Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five," Int J Electr Comput Sci IJECS-IJENS, vol. 11, Jan. 2011.

[23] W. Hommel, S. Metzger, and M. Steinke, "Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization," p. 12.

[24] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," Procedia Comput. Sci., vol. 135, pp. 202–213, Jan. 2018, doi: 10.1016/j.procs.2018.08.167.

[25] I. Gunawan, A. Noertjahyana, and H. Rusli, "Analysis And Implementation Of Operational Security Management On Computer Center At The University X," p. 9, 2014.

[26] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of ISMS," in 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, Kish Island, Iran, Apr. 2013, pp. 1–17. doi: 10.1109/ECDC.2013.6556730.

[27] Z. Sahri, E. Aziz, K. Zolkefley, R. Sadjirin, and Mohd. I. Md. Raus, "Implementing IT Security Penetration Testing in Higher Education Institute," Aust. J. Basic Appl. Sci., vol. 8, pp. 67–72, Jun. 2014.

[28] C. M. Kang, P. S. JosephNg, and K. Issa, "A study on integrating penetration testing into the information security framework for Malaysian higher education institutions," in 2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC), Ipon, Perak, Malaysia, May 2015, pp. 156–161. doi: 10.1109/ISMSC.2015.7594045.

[29] L. Johnson, Security controls evaluation, testing, and assessment handbook, 2nd ed. San Diego: Academic press is an imprint of Elsevier, 2019.

[30] K. Mishima, T. Sakurada, Y. Hagiwara, and T. Tsujisawa, "Secure Campus Network System with Automatic Isolation of High Security Risk Device," in Proceedings of the 2018 ACM SIGUCCS Annual Conference, Orlando Florida USA, Sep. 2018, pp. 107–110. doi: 10.1145/3235715.3235738.

[31] A. Alexei, P. Nistiriuc, and A. Alexei, "Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions," in Proceedings of the 11th International Conference on "Electronics, Communications and Computing (IC|ECCO-2021)," Apr. 2022, pp. 241–245. doi: 10.52326/ic-ecco.2021/NWC.05.

[32] I. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, "Web Vulnerability Assessment and Maturity Model Analysis on Indonesia Higher Education," Procedia Comput. Sci., vol. 161, pp. 1165–1172, 2019, doi: 10.1016/j.procs.2019.11.229.

[33] S. Das, A. Mukhopadhyay, and B. Bhasker, "Today's Action is Better than Tomorrow's Cure - Evaluating Information Security at a Premier Indian Business School:," J. Cases Inf. Technol., vol. 15, no. 3, pp. 1–23, Jul. 2013, doi: 10.4018/jcit.2013070101.

[34] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," Comput. Secur., vol. 90, p. 101709, Mar. 2020, doi: 10.1016/j.cose.2019.101709.

[35] I. S. Bianchi and R. D. Sousa, "IT Governance Mechanisms in Higher Education," Procedia Comput. Sci., vol. 100, pp. 941–946, 2016, doi: 10.1016/j.procs.2016.09.253.

[36] C.-W. Liu, P. Huang, and H. C. Lucas, "Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions," J. Manag. Inf. Syst., vol. 37, no. 3, pp. 758–787, Jul. 2020, doi: 10.1080/07421222.2020.1790190.

[37] A. Wilmore, "IT strategy and decision-making: a comparison of four universities," J. High. Educ. Policy Manag., vol. 36, no. 3, pp. 279–292, May 2014, doi: 10.1080/01587919.2014.899056.

[38] A. Ghazvini, Z. Shukur, and Z. Hood, "Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 8, 2018, doi: 10.14569/IJACSA.2018.090853.

[39] S. Hina and D. D. Dominic, "Information security policies: Investigation of compliance in universities," in 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, Aug. 2016, pp. 564–569. doi: 10.1109/ICCOINS.2016.7783277.