Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:07:2022
DOI 10.17605/OSF.IO/F935H

A SYSTEMATIC LITERATURE REVIEW ON IT SECURITY STANDARDS FOR HIGHER EDUCATION INSTITUTION

ALI MOHAMMED ALWAHAIBI[1], WAN AZLAN BIN WAN HASSA[1], WAN BASRI WAN ISMAIL[1] and MOHAMMED ALMAMARI[2]

[1]Universiti Selangor (UNISEL), Bestari Jaya, Malaysia.
[2]University of Technology and Applied Sciences, Salalah, Oman.

Abstract

Cybersecurity has taken on a wider role, especially in the present era due to an increase in high-risk cyber-attacks. The greatest objective of adapting to cybersecurity is only to protect organizations and users in possible environments like networks, devices, software, etc. Multiple information security policy compliances were created to keep cyber-attacks at bay. Several IT security standards are available at present in different sectors like healthcare, education, and various industries. The aim behind this Systematic Literature Review (SLR) is to analyze the optimistic model of IT security policy compliance from an educational perspective. This research's main objective is to find the number of papers published in past years on IT security standards. We have several IT security policy compliance models like COBIT, ISO/IEC 27001, ITIL, NIST, SAS 70, CMMI, etc. In all, 593 articles were stored in the database, out of which 143 were valid articles related to IT security policy standards, whereas others were duplicates. From the count of 143, the full-text open access articles were 63, which were used further to build the SLR. Prior to the research, the SLR captures a detailed comparison of the NIST, ISO 27001and COBIT IT security policy models using particularly PRISMA check methodology in higher education institutions to reduce the risk of cyberattacks. To drive deeper research over SLR, multiple publications had been referred to like IEEE, Scopus, ScienceDirect, etc. Additionally, some key points are discussed that analyze the scope, mechanism, and technology used in the respective models. In addition, a brief introduction to various types of IT Security Policy Compliance, such as ISO 270001, NIST, and COBIT, is provided in this SLR. In the result section, based on the maintained database that contains the number of published papers and corresponding year, a scatter plot is drawn. The plot helps to get more clarity about the analysis done for IT security policy compliance models preferred by the higher education institutions in the past years. Further, future research can be done into IT security policy compliance that will act as a turning point for all the researchers in higher education sectors.

Keywords: Cybersecurity, Information Security Policy Compliance in Higher Education, Cybersecurity model, NIST cybersecurity model for education.

1. Introduction

The need for cybersecurity is aroused by the term "cybercrime." Cybercrimes are done by computer experts as another way to threaten higher education institutions, organizations, etc. A group of activities are involved in cybercrime, like network disruptions, getting access to private networks, hacking bank accounts and transferring the accounts to their own accounts, gathering confidential information from several organizations, and exploiting them [1,2,3]. To stop these mishaps, cybersecurity came into the picture with the aim of protecting software, networks, systems, etc. Even higher education institutions and organizations have implemented IT security policy compliance on a priority note. Earlier, IT security policy compliance was not given much attention due to the minor set of activities going across institutions and organizations[3,4,5]. But now, at this time, the requirement to handle information security management has increased to a wider extent. Hence, organizations as well as higher education institutions are thinking of hiring a team of IT security professionals who can focus in particular on protecting students' personal data [6,7,8] . Due to such importance, higher education institutions have decided to maintain integrity and confidentiality via setting up an information security management [9,10]. By adapting Information Security Policy compliance, schools and institutions are expressing their assurance to protect students' data.

Several information security policy compliance models are available today, and it is difficult to understand which will be the most suitable structure to define information security policy [11,12]. Hence, a certain level of information security policy compliance development is needed. An Information Security Policy Compliance is defined as a high-level formal statement that incorporates the safety of institutional resources or any information. It is also used for defining a set of actions against an institutional course. These policies must have the institution’s goals, beliefs, and objectives clearly defined from an information security perspective [13,14,15]. There is a set of criteria for IT security policy compliance that must be effective to deal with cyber-attacks. These are mentioned as it Requires Consent which means it is compulsory for the intended audience. Defined policies must be implementable. Be payable which means if failed to comply then strict action must be taken. Must be easy to understand and explainable in brief [16,17,18].

Information security policy compliance must also take into account the following points: Design the procedures and standard structures that are to be followed. Mention the reason for the need for an IT security policy. To focus mainly on acceptable inputs and outputs, define roles and assign responsibilities. A proper management team to oversee compliance with information security policies [19,20,21]. Also, a concern raised by higher education institutions indicates the lack of understanding about these Information Security Policy models. Hence, this SLR contains the difference between the above-mentioned models.

Maintaining the confidentiality and integrity of employee and student personal data is a challenge for higher education institutions. To overcome this challenge, the best way to adapt is to information security policy compliance. Certain management teams are required in each institution to link up and understand the information security policy compliance. Also, the management must be aware of various information security models and their pros and cons.

It is difficult to choose the correct model without any assurance about which policy model works best for the institution? Hence, this SLR is a unique contribution to provide clarity about various information security policy models and their comparison so that it will be feasible for educational institutions to consider any information security policy model that is best in use. Initially, the various information security policy models like ISO 270001, NIST, and COBIT are defined in detail, and later on, the comparison between ISO 270001, NIST, and COBIT is shown to analyze and select the best one.

2. Objectives

The aim for this paper is to understand and explain various IT security policy compliance models for higher education institutions. The SLR takes through a road map by defining certain research questions to get more clarity.

3. Research Questions

The questions determined by the study included the following:

1. What are the various Information Security Policy models suitable for higher education institutions?
2. How to select the best model from an education perspective?
3. What are the additional ways that can help educational institutions data security administrators to improve the data confidentiality?

4. Purpose of the Study

The purpose behind representing the Systematic Literature Review (SLR) of research is to find the best-fit information security policy compliance model for higher education institutions. Specifically, the SLR has been presented based on certain parameters obtained during the analysis. The consideration of these parameters was done by using the PRISMA guidelines. As per PRISMA, inclusion and exclusion criteria are set to pick the best information security policy model; each model is explained along with the research questions.

5. Methodology

Preferred Reporting Items for Systematic Reviews and Meta-Analyses is abbreviated as PRISMA. This technique guides better for gathering systematic reviews. It holds a set of records identified following the inclusion and exclusion criteria. The Prisma Flow Diagram explains the total number of articles researched. Furthermore, the duplicate records were deleted from the database. Also, the exclusions were made concerning the criteria to filter out the data by the year. The flow diagram takes us through various phases of SLR. These different phases map the systematic review as identifiable records, exclusion, inclusion, and the reason for exclusion [21].

6. Data Sources:

The study presents a systematic literature review on IT security Policy Compliance models using PRISMA Methodology. The researchers had put their efforts to search relevant pieces of articles or published papers related to IT security standards from IEEE, Springer Nature, Elsevier, Scopus, etc. Based on the parameters like Cybersecurity policy models, IT security standards, ISO 27001, NIST Model, COBIT IT security standards, its limitations are evident mapping with the list of references from year 2012 to 2022. The researchers had kept a quiet observation on the title and abstract of research papers based on IT security Policy Compliance standards from 2012 to 2022.

The present SLR is based on the "Information Security Policy Compliance Model for Higher Education Institutions." Moving forward for this research, multiple searches have taken place that involve various conference journals, research articles, published papers, blogs published on various sites, and so on. Data collection is the key step to be followed before beginning with SLR[22,23]. Hence, to begin with SLR, a valid data source is mandatory to ensure the research is worthwhile. In this Systematic Literature Review, the references of the following number of research papers are mentioned in table format along with the year of publication.

7. Inclusion and Exclusion Criteria:

In this SLR, the main concern is to capture different IT security policy compliance models that higher education institutions can apply to lower the risk of cyber-attacks. Overall, the research papers that contain various IT security policy compliance models from an educational perspective are importantly considered in this SLR [24,25]. A list of articles is cited, and multiple references are added, but only those articles are considered that are published in conference journals like Scorpius, ScienceDirect, ResearchGate. Journals that are less than ten years old are not included in this SLR. Only the journals from an educational perspective that hold on to various IT security policy models are filtered out. In this entire research, various tables are mentioned that hold the number of published papers related to the IT security policy model[26,15]. The research papers which had information subject to health were excluded from SLR. Also, the records are mainly focused on COBIT, ISO 27001 and NIST IT security model. The records present in the database hold the papers that are focused on the above-mentioned IT security models.

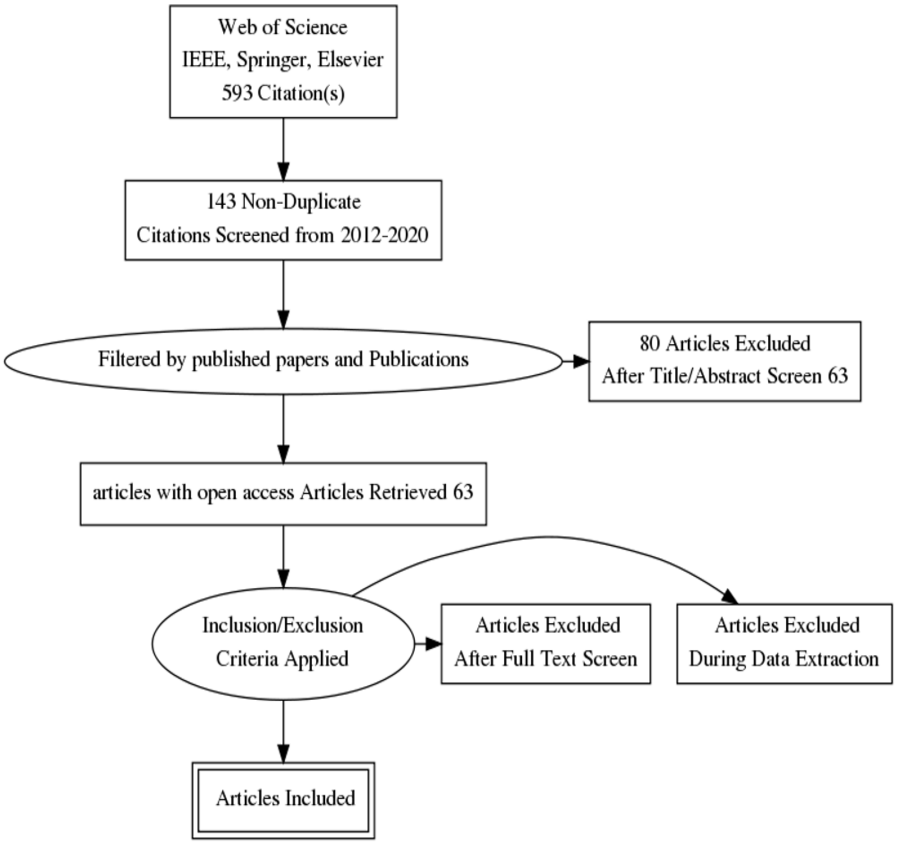


Figure 1: PRISMA Flowchart for Article Screening using Prisma Generator

8. Study Selection and Data Extraction

Depending upon PRISMA Methodology, a restricted model is prepared that undergoes screening to identify articles that must be included or excluded. Once the screening process is achieved, further the researchers can put this information into a tabular format to get a clear view. Table 1, 2, and 3 combines information, statements about various IT security policy compliance models, and the comparison too.

9. Result

The below figures 1 and 2 represents the flow chart of various research papers published at different conferences. The flowchart begins with different conference journals starting from 2012 till 2022, further the one which is cited and is non-duplicated. Moving ahead, the above criteria is followed and the articles with no mentioned IT security policy models are excluded. Out of 592 articles, only 63 articles were considered that had research content about IT security policy compliance models.

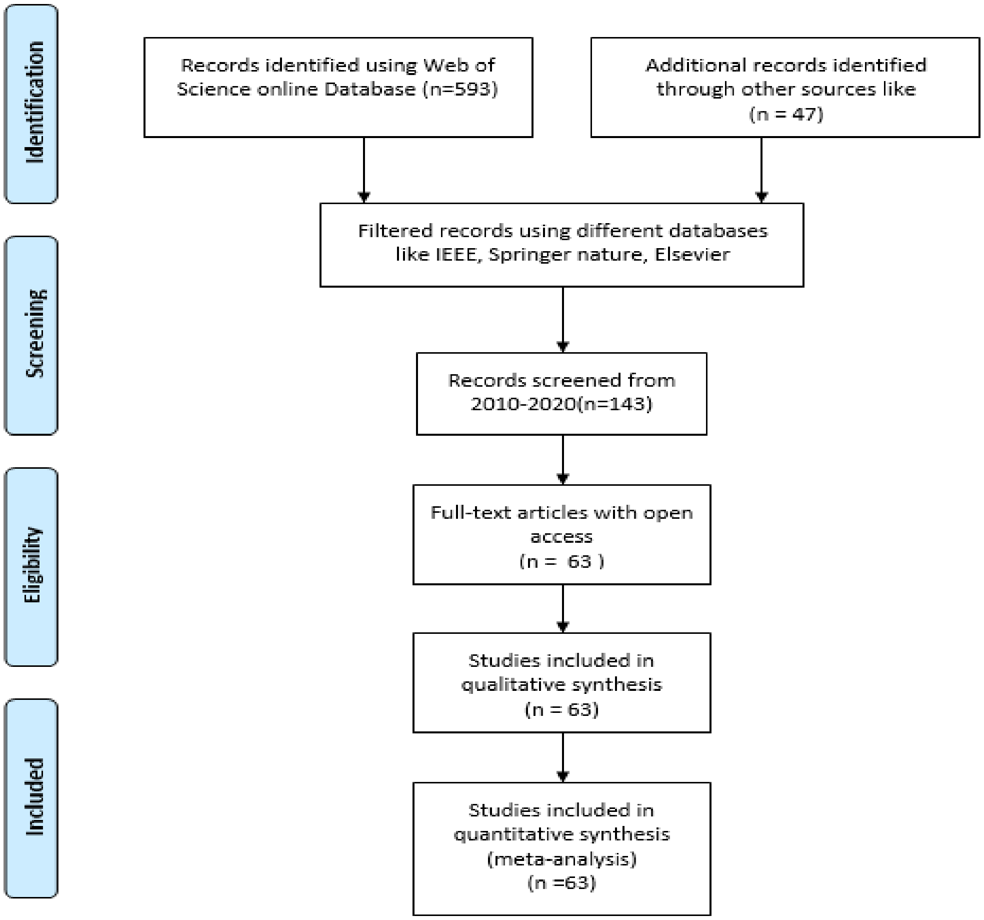

Identification
Screening
Eligibility
Included
Records identified using Web of Science online Database (n=593)
Additional records identified through other sources like (n = 47)
Filtered records using different databases like IEEE, Springer nature, Elsevier
Records screened from 2010-2020(n=143)
Full-text articles with open access (n = 63)
Studies included in qualitative synthesis (n = 63)
Studies included in quantitative synthesis (meta-analysis) (n =63)

Figure 2: Data Source and Extraction

The figure 3 and table 1 under this section captures the relevant data that grants a clear analytical view of the number of papers published between 2012 to 2022. In the Web of Science Database engine, we used the keyword “IT security standards in Higher Education”. We found a count of 592 articles. Based on the initial screening process where titles and abstract were preferred, a count of 143 articles was finalized. In this SLR, as the researchers consider only full text open access articles, hence on review only 63 articles were considered that represents some relevance towards IT security standard policy compliance models. At the end, those 63 articles were selected ranging from 2012 to 2020 which contains strong evidence for various IT security standard models like ISO

27001, COBIT, NIST model, cyberattacks in education institutions, limitations and future research enhancements in IT security policy compliance standards.

Table 1: Number of articles published in past years on IT Security Policy Compliance

Year of Publication	No of articles published
2012	2
2013	4
2014	3
2015	5
2016	2
2017	3
2018	7
2019	8
2020	7
2021	17
2022	5

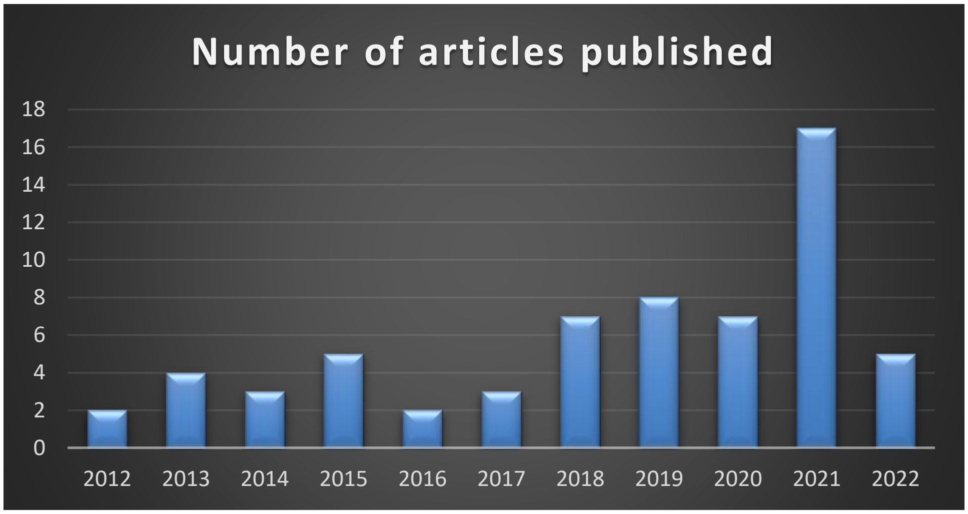


Figure 3: No of Articles published following the years under various IT security Standards

10. Findings

Based on the research questions, certain outcomes are presented in this section. As per the Prisma Methodology, the final dataset has 63 articles, referring the same all the research questions are answered in tabular format.

First question:

There are various Information Security Policy models available in the current era to protect the higher education institutions from any cyberattack or threat. The popular IT security standards are COBIT, ISO/IEC 27001, ITIL, NIST, SAS 70, and CMMI. Which support the management to stay safe from cyberthreats. Out of these many IT security policy models, researchers have considered ISO 27001, NIST and COBIT as these models demonstrates certification to a particular organization. The major reason to focus on only ISO27001, COBIT, and NIST is to get the lower risk that can corrupt or attack sensitive data in a business, organization, and school.[27,28,29]. The best-practiced frameworks against cyberattacks are ISO 27001, COBIT, NIST, and ITIL as they have efficient and best guidelines to control cyberattacks and grant cybersecurity [30,31,32]. Hence NIST IT security model is efficient to deal with cyberattacks and is majorly focused on information security but lacks in boosting the overall IT security compliance model. On the other hand, ISO 27001 holds the power to identify the lapses and manage them. On a real-time basis, it’s difficult for the IT team to take an effort against cyberattacks, hence ISO 27001 information security policy compliance model takes an initiative to manage Cyberattacks. Whereas COBIT allows the business organization, higher education to focus on policies, innovation, and risk management policies that can lower the risk of cybersecurity [33, 34 ,35]. The leftover other IT security policy compliance models are neglected as they are not playing a major role in controlling the risk [36],28,37] . Table 2 shows the various IT security standards filtered to only consideration of three IT security policy compliance models. The models were filtered through various criteria like trusted access, change management, business continuity.

Table2: Various IT security Policy Compliance Standards available

	Trusted Access	Change Management	Business Continuity and Availability	Operation Monitoring and Report	Records Managem ent	Audit and Risk Management	Operational Transparency	Segregation Of Duties	Operational Control
Joint EU Framework (ISO/IEC 27001:2005, ITIL and COBIT)	×	×	×	×	×	×	×	*	*
COBIT	×	×	×	×	×	×	*	×	*
ISO/IEC 27001:2005	×	*	×	×	×	×	×	×	*
ITIL	*	×	×	×	×	×	*	*	*
BSI IT-Grundschutz Methodology	×	×	×	×	×	×	×	*	×
Capability Maturity Model Integration (CMMI)	×	×	×	×	×	*	*	*	*
ISF Standard of Good Practice (SoGP)	×	×	×	×	*	*	×	*	*
GAIT and GAISP	×	*	*	*	*	×	×	*	*
NIST	*	*	*	*	×	×	*	×	*
COSO and Turnbull Guidance	×	*	*	×	×	×	×	×	×
SAS 70	*	×	×	×	*	×	*	×	×

where:

(X) Denotes the model may be used to measure the control requirement.

(*) Denotes the model does not express a metric used to measure the control requirement.

1) International Organization for Standardization (ISO 27001) Information Security Policy model

ISO 27001 information Security Policy is one of the well-renowned and standard sets of information security management systems. Multiple organizations as well as other industries had adopted ISO 27001 and implemented it widely. Why do organizations need ISO 27001? As organizations need to gain trust about the information security management, hence having ISO 27001 supports the organization to take care of information breaches [6 ,38].

Table 3: Definition of ISO 27001

References	Definition of ISO 27001
[39],[40],[41],[42]	To define ISO 27001 in terms of IT security policy compliance, it is a systematic approach that organizations, as well as higher education institutions, accept to secure the personal data, process, and technology. ISO 27001 certification demonstrates the organization that is aligned with security.
[39],[40],[41],[42]	It is a model that involves continuous improvement in any organization moving from various stages like establish, implement, operate, maintain, and review
[39],[40],[41],[42]	ISO 27001 defines methods and practices of implementing information security in organizations with detailed steps on how these are implemented. They aim to provide reliable and secure communication and data exchange in organizations. Also, it stresses on a risk approach to accomplishing its objectives
[39],[40],[41],[42]	This standard dives deep into ways to implement its sub objectives. This puts managers who are looking for clarifications on implementation, at an advantage. However, it fails to achieve the goal of integrating into a larger system. It is standalone in its nature and does not work as a complete ISM solution.

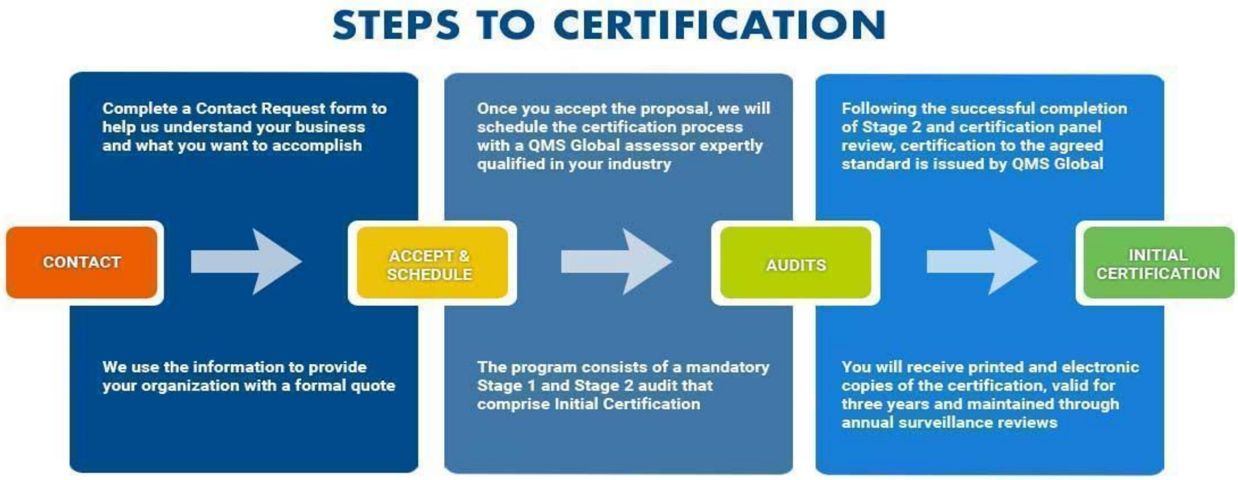
Table 4: ISO 27001 Requirements

References	ISO 27001 three major requirements
[39],[40],[41],[42]	● Systematic Examination: To identify the information security risks, vulnerabilities, and impact over it. ● To design and implement a coherent and comprehensive bulk of information security risk so that the risks are transferred to address the deemed one. ● To adopt a proper management procedure for ensuring that information security controls the integrity and requirements of the ISO organization.

The above table 3 and table 4 represents the data which contains a set of definitions for ISO 27001 commenced by the various authors. The next table holds three major requirements that help the higher education institutions to identify vulnerabilities and examine risk. The next is to design and implement models so that it is addressable. And the end is to set up proper management to get a security about the integrity of the institution. The procedure to get ISO 27001 Certification is illustrated in the below figure4

From the above findings, the clear steps that are required for an ISO 27001 certification are presented. These steps will help higher education institutions take over the ISO 27001 certification.

Figure 4: Steps to Certification in ISO 27001[43]



STEPS TO CERTIFICATION

Complete a Contact Request form to help us understand your business and what you want to accomplish

We use the information to provide your organization with a formal quote

Once you accept the proposal, we will schedule the certification process with a QMS Global assessor expertly qualified in your industry

The program consists of a mandatory Stage 1 and Stage 2 audit that comprise Initial Certification

Following the successful completion of Stage 2 and certification panel review, certification to the agreed standard is issued by QMS Global

You will receive printed and electronic copies of the certification, valid for three years and maintained through annual surveillance reviews

2) National Institute of Standard and Technology (NIST)

The National Institute of Standards and Technology (NIST) is an IT security policy compliance model that provides specific guidelines, standards, and practices for dealing with risks and reducing them to a much greater extent [44]. The NIST model is not only designed to handle cybersecurity risks, but also to manage cybersecurity communications held within internal and external organizations and even stakeholders [44]. From a higher education institution's perspective, there can be different threats, different risks, attacks arising every moment, hence, to safeguard this risk the better way is to apply the model to get a positive outcome [45]. As shown in Figure 5 and Table 5, the NIST cybersecurity model undergoes a set of controls that assists the higher education institution to decide how this model can be prove effective [46].

Table 5: NIST Cybersecurity Policy Model controls [46]

References	NIST Cybersecurity Model's Control
[43],[44],[45],[46]	Identify: To recognize what is to be managed. Protect: To define appropriate control for defining data. Detect: To Monitor process, monitor network continuously. Respond: To improve continually on response Recover: To Confirm resilience.

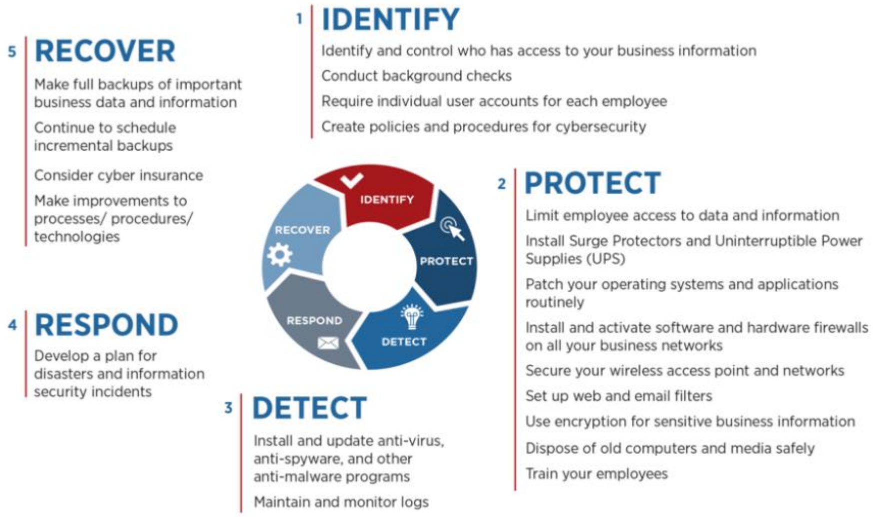

1 IDENTIFY
Identify and control who has access to your business information
Conduct background checks
Require individual user accounts for each employee
Create policies and procedures for cybersecurity
2 PROTECT
Limit employee access to data and information
Install Surge Protectors and Uninterruptible Power Supplies (UPS)
Patch your operating systems and applications routinely
Install and activate software and hardware firewalls on all your business networks
Secure your wireless access point and networks
Set up web and email filters
Use encryption for sensitive business information
Dispose of old computers and media safely
Train your employees
3 DETECT
Install and update anti-virus, anti-spyware, and other anti-malware programs
Maintain and monitor logs
4 RESPOND
Develop a plan for disasters and information security incidents
5 RECOVER
Make full backups of important business data and information
Continue to schedule incremental backups
Consider cyber insurance
Make improvements to processes/ procedures/ technologies
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Figure 5: NIST IT Security Policy Compliance model [47]

The above results show how the NIST IT security model controls go through different stages before being put into place to protect against cyberattacks.

3) Control Objectives for Information and Related Technologies (COBIT)

COBIT is a high-level IT governance and management model. It focuses on the broader decisions in IT management and does not dwell into technical details. It is a model of best practices in managing resources, infrastructure, processes, responsibilities, controls, etc. COBIT contains 34 IT processes, each with high-level control objectives (COs) and a set of detailed control objectives (DCOs) [48,49,50]. In total, there is a sum of 318 DCOs defined for these processes. It is a good solution when managers are looking for a model which serves as an integrated solution within itself, rather than having to be implemented along with other IT governance models. However, its biggest shortcoming is that it does not give “how to” guidelines to accomplish the control objectives. This is not preferred when the trust is on correct implementation of security Controls [51,52].

The answer to the first research question explains the three different IT security policy compliance standards in detail with respect to the procedure of following them in any educational institution [51]. The findings from the first RQ1, strongly highlight the reason behind selecting the three IT security policy compliance standards, which are ISO 27001, COBIT, and NIST models. Each IT security policy compliance model is explained well in this RQ along with particular definitions, the functionality of the model, and also about the outcome. The findings that we have achieved depict a strong word for the ISO 27001 IT security policy compliance model that is suitable for higher education institutions from a security perspective [51,52].

Second question:

The second research question provides a better understanding about the three IT security policy compliance models like ISO 27001, NIST and COBIT. The comparison captures briefly the scope, structure, paradigm, organizational model, and focus. From the comparison below, the researchers got varied differences. The first difference is that ISO 27001 IT security Policy model approaches standard guidelines and promised to provide a proper certification to respective organization [53,54]. The second difference is that NIST IT security policy model focused more on implementing the risk against cyberattacks in institution. The third difference is that COBIT IT security policy model is focused more on IT organizations, it is setup for the same as compared to higher education institutions.

Table 6: Comparison between ISO 27001, NIST, and COBIT IT Security Policy Compliance Models

References	Parameter	ISO 27001	NIST	COBIT
[2],[3],[4]	SCOPE	Standalone guidance for security	Optional guidelines, best-practices and standards for implementing and improving cybersecurity programs.	Complete IT governance of organization, including security planning. It is an integrated solution.
[2],[3],[4],[10],[11],[12],[13]	STRUCTURE	11 sections with 36 objectives which are further divided into sub objectives	Core is divided into 5 functions, 22 categories and 98 subcategories, 4 implementation tiers.	34 IT processes grouped in 4 domains: Plan and organize, Acquire and Implement, Deliver and support, Monitor.
[2],[3],[4],[10],[11],[12],[13]	PARADİGM	Not specified	Information security management system.	Planning of IT Processes.
[2],[3],[4],[10],[11],[12],[13]	ORGANİZATİONAL MODEL	All Stakeholders	Management, IS departments.	All stakeholders.
[2],[3],[4],[10],[11],[12],[13]	FOCUS	On guidelines and standards to reduce approach	Implementation of security controls, stress on risk— management approach.	Business orientation and IT governance in its entirety.

From the above findings, a clear view is achieved that ISO 27001 is standalone guidance for security, whereas NIST has optional guidelines that need implementation, which is time-consuming, and COBIT has an integrated solution but from an IT governance perspective, and not from a higher education institution’s purpose. Hence, it is simply proven that ISO 27001 is the IT security policy compliance model to be implemented across higher education institutions. So, when all the possible situations are taken into account, it is said that ISO 27001 can be used perfectly as an IT security policy compliance model in higher education [55,56].

Third question:

Apart from IT security Policy Compliance model, there are some other ways that education institutions can take care to safeguard the confidential data.

1) Minimize Data Collection

The first most thing that higher education institutions can do is to reduce the collection of student’s personal information. They can avoid storing it at one place. In this way, the risk of losing sensitive data will be due to some extent, and it will be easier even to grab control on it [57].

2) Encrypt Data at Rest

Despite of purging unnecessary data or minimizing it, the best way is to encrypt the sensitive data like student's and parent's information, student's medical record, etc. Here, the role of technology matters those who can manage the IT security policies. Higher education institutions must apply various Data Encryption techniques and then store it safely with respect to files [57].

3) Monitor User Activity over school networks

There must be various users who have access to certain sensitive data, possibilities of data leakage are mostly through internal team. Hence, it is necessary to monitor the network continuously, to track or identity any suspicious activities. Multiple techniques are available like IDS firewall systems to trace the day-to-day activities [57].

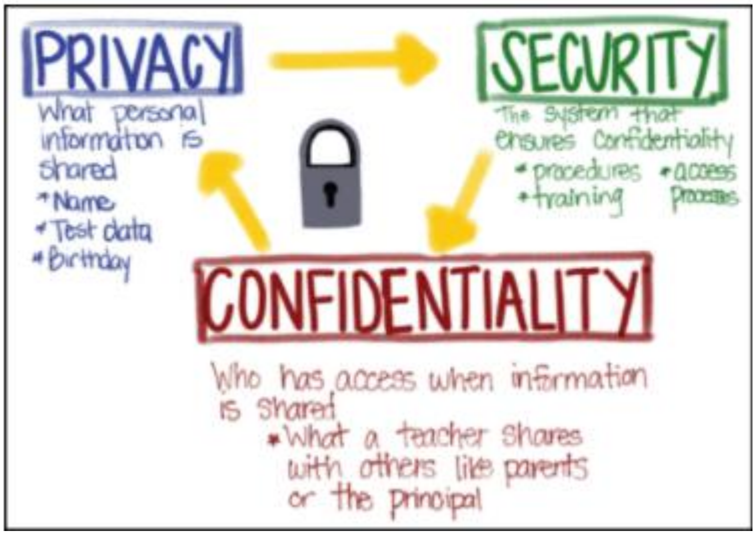

PRIVACY
What personal information is shared
*Name
*Test data
*Birthday
SECURITY
The system that ensures confidentiality
*procedures
*training
*access processes
CONFIDENTIALITY
Who has access when information is shared
*What a teacher shares with others like parents or the principal

Figure 6: Important Data from Higher Education Institution perspective[58]

The third question shows the importance and measures the sensitivity of data that every higher education institution holds. Hence, the findings show that higher education institutions need to keep an eye on these cyberattacks and implement the best practices for cyberattack protection. As for any higher education institution to maintain Privacy, Security and Confidentiality are most important [59,60]. The above figure highlight what privacy contains like personal shared information, and what security includes the system that ensures confidentiality like training materials, modal, access, and staff information. All of these indicators, that how much it is important to maintain the IT security standards in higher education institutions [59,60].

11. Conclusion

The IT security Standards gave higher education institutions a new ray of hope to fight against ongoing cyberattacks and threats. The IT security management team can now lower the risk of cyber threats and protect the educational institutions from higher risk. The above SLR consists of deep research content from various articles, blogs, research papers published in reputed conferences and journals. The research is customized, and its main focus is to find the better IT Security Policy Compliance model for Higher Education Institutions. Initially, three research questions were raised, that involved first to find out the various IT security Policy Compliance models present. Secondly, a short comparison is mentioned on these models that indicates most of the education institutions prefer ISO 27001 IT security Policy compliance model as it demonstrates multiple benefits and pointing majorly for providing certification. NIST IT security policy compliance model has five different controls that initiates proper guidance to higher education institutions against cyber threats. COBIT is another IT security Policy Compliance model that undergoes an approach of Plan, Implement, Monitor and Acquire to identify the cyber threats and lower down the risk. To summarize, the three models have their own aspects like ISO 27001 is more focused on security and guidelines of organization, whereas the NIST IT security policy model is focused more on the implementation of the approaches that reduce risk. The least one, i.e., COBIT is focused more on IT organizations that might lack from an education perspective. Although, the mixture of these three models can give rise to a variant which can assist in reducing the cybercrime happening in higher education institutions. This model can reduce the risk, implement the guidelines to recover the risk, and also will convert the institution into a well-known certified educational institution.

Acknowledgments

My sincere appreciation and deep gratitude go to my research supervisors for providing me with the opportunity and guidance in doing this research paper.

References

[1] M. Raditya, P. Dewanto, T. Oktavia, and D. Sundaram, "COMPARATIVE STUDY OF INFORMATION SECURITY EVALUATION MODELS FOR INDONESIA GOVERNMENT," vol. 100, no. 4, 2022.

[2] V. Arora, "Comparing different information security standards : COBIT v s . ISO 27001," Carnegie Mellon Univ. Qatar, pp. 7–9, 2005, [Online]. Available: https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf.

[3] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," 2020 Natl. Conf. Emerg. Trends Sustain. Technol. Eng. Appl. NCETSTEA 2020, vol. 53, pp. 27001–27003, 2020, doi: 10.1109/NCETSTEA48365.2020.9119914.

[4] R. Ross, P. Viscuso, G. Guissanie, K. Dempsey, and M. Riddle, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," NIST Spec. Publ. 800-171, no.

February, pp. 1–34, 2014, [Online]. Available: http://csrc.nist.gov/publications/drafts/800-171/sp800_171_draft.pdf%5Cnpapers3://publication/uuid/941C6670-6154-4B0B-A575-AF606C6EF829.

[5] J. B. Ulven and G. Wangen, “A systematic review of cybersecurity risks in higher education,” Futur. Internet, vol. 13, no. 2, pp. 1–40, 2021, doi: 10.3390/fi13020039.

[6] A. Alexei, “Cyber Security Strategies for Higher Education Institutions,” J. Eng. Sci., vol. XXVIII, no. 4, pp. 74–92, 2021, doi: 10.52326/jes.utm.2021.28(4).07.

[7] Angraini, R. A. Alias, and Okfalisa, “Information security policy compliance: Systematic literature review,” Procedia Comput. Sci., vol. 161, pp. 1216–1224, 2019, doi: 10.1016/j.procs.2019.11.235.

[8] 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, 2019, doi: 10.1016/j.cose.2019.101594.

[9] Marlin Pohlman, “Compliance Frameworks,” 2010. http://ittoday.info/Articles/Compliance_Frameworks.htm (accessed Jun. 25, 2022).

[10] H. E. Excellence, “NIST Special Publication 800-171 for higher education.”

[11] OSA, “13-05 Control mapping (NIST 800-53 vs ISO 17799 / PCI-DSS v2 / COBIT 4.1,” 2012. https://www.opensecurityarchitecture.org/cms/library/0802control-catalogue/256-control-mapping (accessed Jun. 11, 2022).

[12] The ISO 27000 Directory, “ISO 27000 - ISO 27001 and ISO 27002 Standards,” Mar. 12, 2012. https://www.27000.org/index.htm (accessed Jun. 25, 2022).

[13] NIST, “NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments,” NIST Guid. Conduct. Risk Assessments, no. September, p. 95, 2012.

[14] C. Okoli and K. Schabram, “Working Papers on Information Systems A Guide to Conducting a Systematic Literature Review of Information Systems Research,” Work. Pap. Inf. Syst., vol. 10, no. 2010, 2010, doi: 10.2139/ssrn.1954824.

[15] E. G. Alisa, “Cybersecurity Framework or ISO 27001,” 2018. https://www.securitynewspaper.com/2018/02/24/cybersecurity-framework-iso-27001/ (accessed Apr. 02, 2022).

[16] A. Rabii, S. Assoul, K. Ouazzani Touhami, and O. Roudies, “Information and cyber security maturity models: a systematic literature review,” Inf. Comput. Secur., vol. 28, no. 4, pp. 627–644, 2020, doi: 10.1108/ICS-03-2019-0039.

[17] E. A. Rigon, C. M. Westphall, D. R. Dos Santos, and C. B. Westphall, “A cyclical evaluation model of information security maturity,” Inf. Manag. Comput. Secur., vol. 22, no. 3, pp. 265–278, 2014, doi: 10.1108/IMCS-04-2013-0025.

[18] Š. Orehek and G. Petrič, “A systematic review of scales for measuring information security culture,” Inf. Comput. Secur., vol. 29, no. 1, pp. 133–158, 2020, doi: 10.1108/ICS-12-2019-0140.

[19] J. Sun, P. Ahluwalia, and K. S. Koong, “The more secure the better? A study of information security readiness,” Ind. Manag. Data Syst., vol. 111, no. 4, pp. 570–588, 2011, doi: 10.1108/02635571111133551.

[20] A. A. Ganin et al., “Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management,” Risk Anal., vol. 40, no. 1, pp. 183–199, 2020, doi: 10.1111/risa.12891.

[21] M. Nicho, “A process model for implementing information systems security governance,” Inf. Comput. Secur., vol. 26, no. 1, pp. 10–38, 2018, doi: 10.1108/ICS-07-2016-0061.

[22] D. I. K. Meranti, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” vol. II, pp. 1–15, 2015.

[23] Rhand Leal, “NIST vs. ISO 27001 | Which one is better for your company?,” 2014. https://advisera.com/27001academy/blog/2014/02/24/which-one-to-go-with-cybersecurity-framework-or-iso-27001/ (accessed Feb. 24, 2014).

[24] Dejan Kosutic, “Implement ISO 27001 | Easy ISO 27001 implementation checklist.” https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/ (accessed Apr. 02, 2022).

[25] D. Ochel, “Comparing NIST’s Cybersecurity Framework with ISO/IEC 27001,” Mar. 16, 2014. https://secuilibrium.com/2014/02/14/comparing-nists-cybersecurity-framework-with-iso-iec-27001/ (accessed Apr. 02, 2022).

[26] Alou MrA, “Why you should adopt the NIST Cybersecurity Framework,” no. May, 2014.

[27] D. R. Alison, “How to choose the right cybersecurity framework | TechRepublic,” Mar. 07, 2019. https://www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ (accessed Apr. 02, 2022).

[28] F. Stohlman and G. Brecher, “Humoral regulation of erythropoiesis III. Effect of exposure to simulated altitude,” J. Lab. Clin. Med., vol. 49, no. 6, pp. 890–895, 1957.

[29] D. Kosutic, “List of ISO 27001 mandatory documents and records,” 2013. https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-2013-revision/ (accessed Apr. 02, 2022).

[30] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,” TQM J., vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/TQM-09-2020-0202.

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

[32] 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, 2017, doi: 10.1016/j.jisa.2017.06.006.

[33] A. Arina, “Network Security Threats to Higher Education Institutions,” Cent. East. Eur. eDem eGov Days, vol. 341, pp. 323–333, 2022, doi: 10.24989/ocg.v341.24.

[34] 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.

[35] I. S. Bianchi, R. Pereira, and R. D. Sousa, “IT governance Mechanisms at Universities: An exploratory study,” AMCIS 2017 - Am. Conf. Inf. Syst. A Tradit. Innov., vol. 2017-Augus, no. 351, 2017.

[36] 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. des Telecommun. Telecommun., 2020, doi: 10.1007/s12243-020-00783-2.

[37] H. Rehman, A. Masood, and A. R. Cheema, “Information security management in academic

institutes of Pakistan," Conf. Proc. - 2013 2nd Natl. Conf. Inf. Assur. NCIA 2013, pp. 47–51, 2013, doi: 10.1109/NCIA.2013.6725323.

[38] W. Hommel, S. Metzger, and M. Steinke, "Information Security Risk Management in Higher Education Institutions : From Processes to Operationalization," EUNIS J. High. Educ. IT, no. 2015/3, pp. 1–12, 2015.

[39] 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, 2018, doi: 10.1016/j.procs.2018.08.167.

[40] M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann, and K. Sakurai, "An analysis of IT assessment security maturity in higher education institution," Lect. Notes Electr. Eng., vol. 376, pp. 701–713, 2016, doi: 10.1007/978-981-10-0557-2_69.

[41] J. S. Pan, V. Snasel, E. S. Corchado, A. Abraham, and S. L. Wang, "Preface," Adv. Intell. Syst. Comput., vol. 297, p. 5, 2014, doi: 10.1007/978-3-319-07776-5.

[42] F. Sanchez-Puchol, J. A. Pastor-Collado, and B. Borrell, "Towards an Unified Information Systems Reference Model for Higher Education Institutions," Procedia Comput. Sci., vol. 121, pp. 542–553, 2017, doi: 10.1016/j.procs.2017.11.072.

[43] X. Li, "The Design of Information Security Management System in College," DEStech Trans. Soc. Sci. Educ. Hum. Sci., no. eeres, 2017, doi: 10.12783/dtssehs/eeres2016/7612.

[44] A. Elgelany and W. Gaoud, "Cloud Computing: Empirical Studies in Higher Education A Literature Review," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 10, 2017, doi: 10.14569/ijacsa.2017.081017.

[45] A. Alexei and A. Alexei, "Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning," Artic. Int. J. Sci. Technol. Res., vol. 10, no. 3, pp. 128–133, 2021, [Online]. Available: www.ijstr.org.

[46] 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," Iber. Conf. Inf. Syst. Technol. Cist., vol. 2020-June, no. June, pp. 24–27, 2020, doi: 10.23919/CISTI49556.2020.9141014.

[47] A. R. Ahlan and M. Lubis, "Information security awareness in university: Maintaining learnability, performance and adaptability through roles of responsibility," Proc. 2011 7th Int. Conf. Inf. Assur. Secur. IAS 2011, no. December, pp. 246–250, 2011, doi: 10.1109/ISIAS.2011.6122827.

[48] A. Da Veiga, "The influence of information security policies on information security culture: Illustrated through a case study," Proc. 9th Int. Symp. Hum. Asp. Inf. Secur. Assur. HAISA 2015, no. Haisa, pp. 22–33, 2015.

[49] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," Int. J. Inf. Manage., vol. 36, no. 2, pp. 215–225, 2016, doi: 10.1016/j.ijinfomgt.2015.11.009.

[50] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: A systematic review of quantitative studies," Inf. Manag. Comput. Secur., vol. 22, no. 1, pp. 42–75, 2014, doi: 10.1108/IMCS-08-2012-0045.

[51] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.

[52] M. Information, "Qjarterly," vol. 34, no. 3, pp. 523–548, 2016.

[53] J. Y. Son, “Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies,” Inf. Manag., vol. 48, no. 7, pp. 296–302, 2011, doi: 10.1016/j.im.2011.07.002.

[54] H. Chan and S. Mubarak, “Significance of Information Security Awareness in the Higher Education Sector,” Int. J. Comput. Appl., vol. 60, no. 10, pp. 23–31, 2012, doi: 10.5120/9729-4202.

[55] A. A. Norman and N. M. Yasin, “Information systems security management (ISSM) success factor:Retrospection from the scholars,” 11th Eur. Conf. Inf. Warf. Secur. 2012, ECIW 2012, vol. 7, no. 27, pp. 339–344, 2012, doi: 10.5897/AJBM11.2479.

[56] C. Mike, “5 Ways to Safeguard Student Information | EdTech Magazine,” Apr. 10, 2019. https://edtechmagazine.com/k12/article/2019/04/5-ways-safeguard-student-information (accessed Apr. 02, 2022).

[57] NIST, “MEP Centers Aid Manufacturers on Cybersecurity,” 2018. https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity (accessed May 03, 2018).

[58] UNC University, “Write the Review - Systematic Reviews - LibGuides at University of North Carolina at Chapel Hill,” 2022. https://guides.lib.unc.edu/systematic-reviews/PRISMA (accessed Jun. 11, 2022).

[59] Wembley Partners, “NIST, ISO, COBIT, ITIL – Which Cyber Framework Rules Them All?,” 2021. https://www.wembleypartners.com/post/nist-iso-cobit-itil-which-cyber-framework-rules-them-all (accessed Jan. 18, 2021).

[60] 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. des Telecommun. Telecommun., vol. 76, no. 3–4, pp. 255–270, 2021, doi: 10.1007/s12243-020-00783-2.