Journal of Engineering Science *Vol. XXVIII, no. 4 (2021), pp. 74 - 92*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2021.28(4).07
CZU 004.49:378

CYBER SECURITY STRATEGIES FOR HIGHER EDUCATION INSTITUTIONS

Arina Alexei*, ORCID ID: 0000-0003-4138-957X

Technical University of Moldova, 168 Stefan cel Mare Blvd., MD-2004, Chisinau, Republic of Moldova
*Corresponding author: Arina Alexei, *arina.alexei@tse.utm.md*

Received: 09. 24. 2021
Accepted: 11. 02. 2021

Abstract. Due to the large volume of data they manage, Higher Education Institutions (HEIs) are perfect targets for cyber attackers. University networks are open in design, decentralized and multi-user, making them vulnerable to cyber-attacks. The purpose of this research paper was to identify which is the recommended cyber security strategy and how comprehensive are these studies, within HEIs. The method proposed by Kitchenham was used, focused on the information community. Thus, the following results can be communicated: researchers recommend their own security strategies, because the standards analysed in the papers are not oriented on HEIs, and require important adjustments to be implemented. Most scientific papers do not describe risk management process. The implementation phases are also insufficiently analysed. The functions that the strategy addressed by HEIs should fulfill include identification, protection and detection. The validation methods used in the pre-implementation and post-implementation phases are case studies and surveys. Most researchers recommend as final cyber security strategy IT Governance and security policies. The field of research has proved to be very interesting, the researches could contribute to the creation of a comprehensive cybersecurity strategy, focused on the specifics of HEIs, efficient, easy to implement and cost-effective.

Keywords: *cyber security, strategy, risk management, HEI, framework, standard.*

Rezumat. Datorită volumului mare de date pe care le gestionează, instituțiile de învățământ superior (IIS) sunt ținte perfecte pentru atacatorii cibernetici. Rețelele universitare sunt deschise în design, descentralizate și multi-utilizator, deci vulnerabile la atacuri cibernetice. Scopul acestei lucrări de cercetare a fost să identifice care este strategia de securitate cibernetică recomandată și cât de cuprinzătoare sunt aceste studii, realizate în cadrul instituțiilor de învățământ superior. S-a folosit metoda propusă de Kitchenham, axată pe comunitatea informațională. Astfel, se pot comunica următoarele rezultate: cercetătorii recomandă propriile strategii de securitate, deoarece standardele analizate în lucrări nu sunt orientate spre IIS și necesită ajustări importante pentru a fi implementate; majoritatea lucrărilor științifice nu analizează procesul de management al riscului; fazele de implementare sunt insuficient analizate. Funcțiile pe care strategia abordată de IIS ar trebui să le îndeplinească includ identificarea, protecția și detectarea. Metodele de validare

utilizate în fazele de pre-implementare și post-implementare sunt studii de caz și anchete. Majoritatea cercetătorilor recomandă ca strategie finală de securitate cibernetică Guvernarea IT și politicile de securitate. Domeniul de cercetare s-a dovedit a fi foarte interesant, cercetările ar putea contribui la realizarea unei strategii cuprinzătoare de securitate cibernetică, axată pe specificul IIS, eficientă, ușor de implementat și rentabilă.

Cuvinte cheie: *securitate cibernetică, strategie, management al riscului, IIS, cadru, standard*.

Introduction

With the development of information technologies, their use in HEIs has increased substantially. The year 2020 and the pandemic with Covid-19, made indispensable the use of new technologies to ensure the continuity of the university educational process, which passed in the online environment, requiring new technologies to be implemented. University networks had significant vulnerabilities even before the pandemic, as they are open in design [1], decentralized, multi-user and present data of maximum interest to attackers.

Universities are currently in the process of technological development. Access to technology is valuable in the development of modern learning environments, but on the other hand increases the vulnerability of communication networks and the number of threats. College campuses are some of the most technologically developed areas because it provides expanded support for Wi-Fi, online learning platforms (like Moodle), digital libraries, virtualization classes (teams, zoom, WebEx), web conferencing. All this, makes university networks very vulnerable due to large open networks, unlike other organizations [2].

Thus, in 2020 the education domain had a loss of $ 3.90 million for data breach, according to IBM & Ponemon Institute [3], which conducts cybersecurity research. Referring to another study realized by CheckPoint [4], a leading provider of cyber security solutions to governments and corporations globally and in Europe too, the average number of weekly cyber-attacks per academic organization in July-August 2020, increased by 24%. In contrast, the overall increase in the number of attacks in all sectors in Europe was only 9% [5].

The implementation of an information security management system within HEIs is an important step in ensuring cyber security. With all the above, the studies in this field are very limited and do not contain implementation details, efficiency analysis and implementation of security frameworks in HEIs, rather, they have a superficial character, a theory supported by several international researchers [6–8]. The security framework is a comprehensive solution containing security policies, tools and procedures for strengthening cybersecurity and maintaining the information system [9–12].

A laborious study of the scientific literature in the field, it is necessary, to identify several key moments that will later allow to create a cyber security framework that is easy to implement, efficient and cost-effective. The main research question is: to identify the recommended security frameworks/strategies for HEIs, at international level, and how comprehensive are these studies, based on the review of the literature, published in the last 10 years. The research will focus on the analysis of the risk management and cyber security strategy, implementation phases, the functions of the security framework, validation methods and the finality of this process.

To achieve this goal, the search was performed in the following five scientific databases: Scopus, ScienceDirect, ACM Digital Library, IEEE Xplore and Springer. These databases have been selected because they are the most used for the study in the field of information security [12].

The article is organized as follows: in the first section we analyse the method proposed for literature review, we are planning and conducting the literature review, in the second section can be seen the report of literature review, based on the results found in section 1. Section 3 contains conclusions of the author and future research directions.

1. Research method

The method that was used to study the literature is based on the systematic review proposed by Kitchenham [13], aimed at the software engineering community. The systematic review of the literature is carried out in order to identify, interpret and evaluate research, relevant to a particular field. The individual studies conducted by researchers that contribute to the systematic review are primary studies and secondary studies, that result from the literature review. Thus, by the proposed method, the systematic review process involves the following 3 important phases: planning, conducting and reporting the review.

1.1. Planning the systematic review

The literature review planning process involves establishing a protocol. The review protocol includes the methods selected for the systematic review of the literature. The first step is to describe the background and establish the research questions, which follows.

There are several security frameworks used to implement the information security management system within organizations, such as ISO27001 [14], NIST [15], COBIT [16], ITIL [17]. However, according to several researchers, there is no framework that focuses specifically on cybersecurity in HEIs, as most security frameworks are aimed at commercial organizations [9 – 12], [18], or are difficult to implement and are not cost-effective.

So, the main research question (MRQ) is:" What is the cyber security strategy recommended within HEIs, how comprehensive are these researches?"

Complementary research questions (CRQ), to respond as accurately as possible to MRQ, are:

- CRQ1 - What is the security framework / standard recommended by researchers for HEIs? Do scientific papers include mechanisms for identifying security risks?
- CRQ2 - What are the phases of implementing the security framework in HEIs? What functions are considered relevant to the security framework?
- CRQ3 – What methods for evaluating the effectiveness of applied strategies.

At this stage, it is necessary to set the search terms and resources. Literature review was oriented on scientific articles and international conference proceedings, indexed in one of the following databases: Scopus, ScienceDirect, ACM Digital Library, IEEE Xplore, Springer.

The search was performed in the following metadata: the title, the keywords and the abstract of the scientific article but also in the content for more accurate results; based on the search terms set out in Table 1.

Table 1

Search terms

No	Search terms
1	[Information Security] **or** [Information Security Management System] **or** [Cyber Security] **or** [IT governance] **and**
2	[Standard] **or** [Policies] **or** [Framework] **or** [Strategy] **and**
3	[Higher Education Institutions] **or** [HEI] **or** [Academia Institutes] **or** [University Campus] **or** [College]

The selection of primary studies is governed by inclusion and exclusion criteria [13]. The inclusion criteria of the scientific articles were:

- IC1: Studies that include research on security standards/frameworks;
- IC2: Studies that include the protocol for implementing the security standard/framework in HEI;
- IC3: Studies presenting categories, tools or policies relevant to the implementation of the security standard/framework in HEIs;
- IC4: Studies published since 2012 (to correspond to the objective of identifying the literature of the last 10 years).

The exclusion criteria from the research are:

- EC1: Only the abstract of the article is available;
- EC2: The study is not a research article or conference paper;
- EC3: The study contains the search terms in Table 1, because the authors work within HEIs and are not a study of information security in higher education institutions;
- EC4: Studies that reflect the importance of study programs (specializations) in the field of information security within the HEI.

1.2. Conducting the literature review

According to the search terms, 73 scientific papers were identified, however, a large part were excluded because they were not relevant according to the inclusion criteria set out in the previous step, or because they matched the exclusion criteria. So finally, were analysed 30 scientific articles, that were added in the Mendeley Reference Manager [19].

To perform a quality assessment, for each CRQ, has been set research criteria, reflected in table 2.

Table 2

Research criteria

No	**Complementary research questions (CRQ)**	**Research criteria**
1	What is the security framework/standard recommended by researchers for HEIs? Do scientific papers include mechanisms for identifying security risks?	Security framework or standard
		Risk Management framework
2	What are the phases of implementing the security framework in HEIs? What functions are considered relevant to the security framework?	Implementing phases
		Security framework functions
3	How is evaluated the effect of implementation of the security framework?	Operational architecture
		Validation methods

The relevance index [12] was calculated, according to the formula, each answer x_i can take the value 1, if the article solved all the research criteria and 0 otherwise:

$$\mathbf{Ri} = \frac{\sum_{i=1}^{n} x_i}{n} * 100\% \quad (1)$$

where: n = number of selected items, i = {1,...,n}

$x_i \in \{0,1\}$

Ri -can take values between 0 and 1, the value 1 takes if it meets all research criteria

It follows for each CRQ1, CRQ2, CRQ3, to extract, the research criteria, reflected in Table 2. Thus, the extracted data will be presented in the tables and graphically.

Using the method proposed by Kitchenham [13], based on formula (1), the relevance index (Ri) of the scientific paper was calculated, the results can be seen in Table 3, sorted by relevance.

Table 3

Selected scientific papers

Reference	Scientific Paper	Publishing year	R_i
[18]	Information Security Management in academic institutes of Pakistan	2013	0,89
[20]	An analysis of Indonesia's information security index: a case study in a public university	2018	0,89
[2]	Information security risks management framework – A step towards mitigating security risks in university network	2017	0,89
[21]	Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study	2014	0,89
[22]	Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization	2017	0,89
[23]	Today's Action is Better than Tomorrow's Cure - Evaluating Information Security at a Premier Indian Business School	2013	0,89
[24]	Emergence of Robust Information Security Management Structure around the world wide Higher Education Structure around the world wide Higher Education Institutions: Institutions: a Multifaceted Security Solution	2012	0,89
[25]	IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education	2016	0,89
[26]	A study on integrating penetration testing into the information security framework for Malaysian higher education institutions	2015	0,83
[27]	Defense-through-Deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack	2018	0,77
[16]	Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review	2013	0,72
[28]	Assessment of Information System Risk Management with Octave Allegro at Education Institution	2018	0,72
[29]	A generic framework for information security policy development	2017	0,72
[30]	Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education	2018	0,72
[31]	An Analysis of IT Assessment Security Maturity in Higher Education Institution	2016	0,68

Continuation Table 3

[32]	Information Security Management for Higher Education Institutions	2014	0,61
[33]	Information system and management for campus safety	2019	0,22
[34]	Towards an Unified Information Systems Reference Model for Higher Education Institutions	2017	0,61
[35]	Web vulnerability assessment and maturity model analysis on Indonesia higher education	2019	0,61
[36]	Implementing IT Security Penetration Testing in Higher Education Institute	2014	0,55
[6]	IT Governance Mechanisms in Higher Education	2016	0,50
[8]	Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behaviour in higher education institutions in the developing world	2019	0,50
[37]	Missing Values Prediction for Cyber Vulnerability Analysis in Academic Institutions	2018	0,44
[38]	Implications, Risks and Challenges of Cloud Computing in Academic Field – A State-Of-Art	2019	0,44
[39]	Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions	2020	0,44
[40]	Sixware Cybersecurity Framework Development to Protect Defence Critical Infrastructure and Military Information Systems	2021	0,39
[41]	The Design of Information Security Management System in College	2016	0,39
[42]	Analysis and Implementation of Operational Security Management on Computer Center At the University X	2014	0,33
[43]	An IT value management capability model for Portuguese universities: A Delphi study	2018	0,22
[44]	Cloud Computing: Empirical Studies in Higher Education A Literature Review	2017	0,22

Graphically, the results are shown in Figure 1.

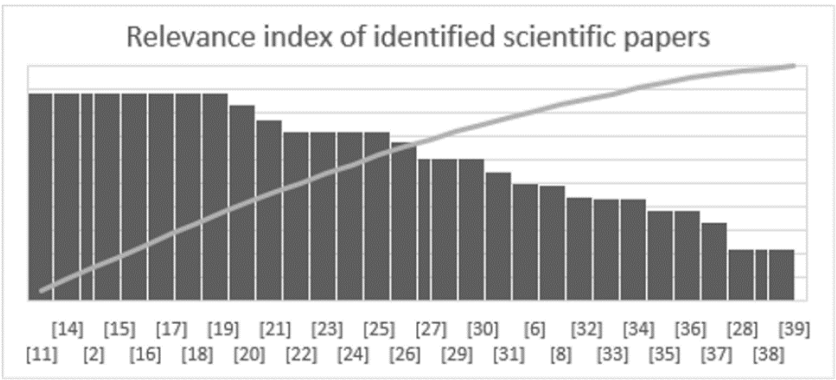

Figure 1. Relevance of identified scientific papers.

The descriptive method will be used for data synthesis. The information extracted from scientific papers will be presented graphically using Venn diagram [45] and the circular diagram, which will generate graphics data to allow the visualization of the investigated data distribution. Graphs are a form of data abstraction and constitute an essential part of the data scientist's toolkit [45].

2. Reporting the literature review

2.1 Answer to complementary research question CRQ1

As reflected in Table 2, the research criteria that help to obtain a comprehensive response to CRQ1 are: recommended security framework/standard and risk management framework.

It is very important for HEIs to establish policies and control measures [32]. Security frameworks that assist to implement an Information Security Management Systems (ISMS) provide a complete solution for a better information security experience by providing the needed policies, tools and procedures for enhancing and maintaining a secured information system [21]. Another approach, but which supports the same idea, is that "The security framework is a complete solution that contains security policies, tools and procedures for strengthening cybersecurity and maintaining the information system" [9 – 12].

For a more efficient information security management system, it is mandatory to perform risk management, which refers to the confidentiality, integrity and availability of data related to the critical assets of HEIs [22]. Risk management can reduce the risks of certain important processes, financial losses or damage to reputation of HEIs [28], and support security policies creation [22].

These arguments served as a reason for analysing the recommended risk management strategies, along with the identification of ISMS recommended by researchers, as an integral part of the ISMS implementation process in HEIs, and increasing cyber security.

2.1.1 Recommended framework/standard for security management

In order to answer at CRQ1, first criterion, it was necessary to identify, in the selected scientific papers, what are the recommended frameworks/standards. Table 4 reflects, the results of review, the recommended frameworks/standards are: ISO 27001, COBIT, ITIL, hybrid solution.

Many researchers provide own strategy, that confirms once again that the standards listed above are not oriented for implementation in HEIs, theory supported by several scientific studies.

Table 4

Recommended security framework/standard

Criterion	Framework	Scientific Paper	%
Recommended framework/standard for Information Security Management in HEIs	ISO 27001	5	16,67
	COBIT	1	3,33
	ITIL	1	3,33
	Hybrid	1	3,33
	Not including	8	26,67
	Own framework	14	46,67

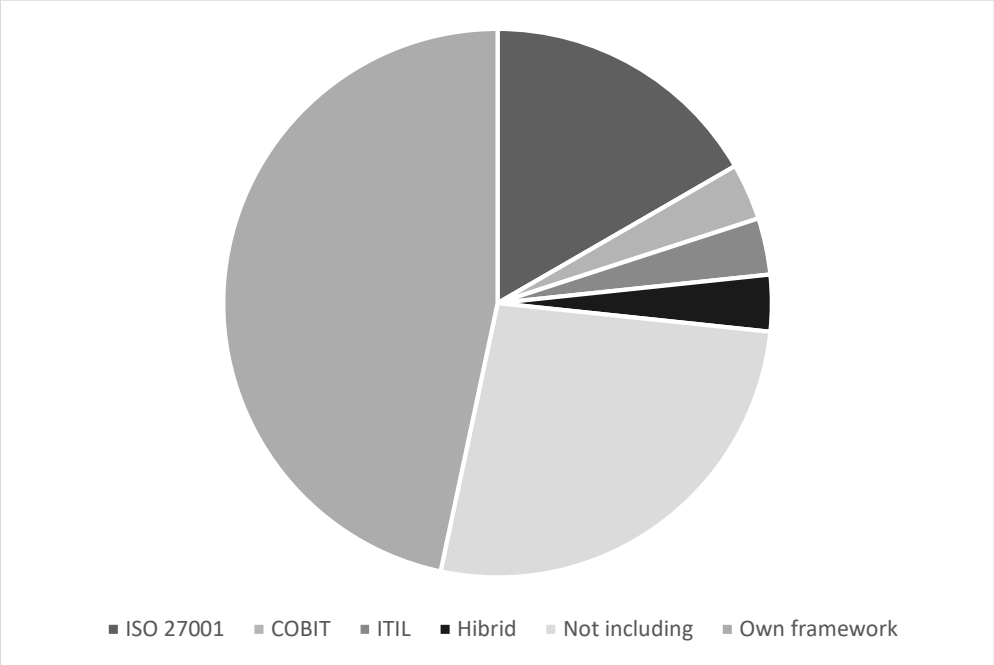

Figure 2. Recommended framework/standard.

ISO27001

ISO 27001 standard is the most widely used standard for information security at international level [18], [21]. In education, there has been a steady increase in the number of institutions certified to ISO 27001, so that in 2018 internationally certified were 137 institutions, in 2019, their number was 176 institutions certified [46], [47]. Most ISO 27001 certified institutions are in Japan (26), Greece (30), Italy (11), Poland (12), the Czech Republic (11).

The protection of corporate assets is achieved through the implementation of ISMS, which includes security risk assessment and is based on the CIA triad [14], [20], [47], [48].

The CIA triad refers to the three principles of information security [47]:

- Confidentiality, confirms that only authorized persons have access to information.
- Integrity, determines the accuracy with which data are processed.
- Availability, ensures that authorized persons access the data upon request.

As information security is not just about IT, the ISO 27001 standard also contains specific controls for human resource management, legal constraints and organizational management [47].

This is also due to the fact that cyber security depends more on the human factor than on the technology used [21], and the security threats coming from the employees of an organization are far superior to external threats [21].

The ISO 27001 standard is organized into 14 sections, 35 objectives and 114 security controls. For HEIs 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 [32], [49]. Not all sections of the standard are applicable in HEIs, as the ISO 27001 standard is aimed at non-academic and commercial organizations [18].

Due to the general nature of the ISO 27001 standard, it is difficult to identify the targeted strategy specifically for HEIs, so empirical research could elucidate new variables that are not provided by the standards.

COBIT

COBIT provides effective practices and establishes cybersecurity-specific activities in an organized and flexible structure. It enables the creation of IT control policies and promotes best practices at the organizational level [16]. COBIT focuses on generating a structured set of principles, such as organizational requirements, IT resources, IT processes and the provision of information [16]. The strategy proposed by COBIT is nothing more than a set of documents and good practices that support a specialist, auditor or user, to assess security risks, depending on the controls implemented and the technical problems faced by the organization [31].

COBIT is focused on risk management, as is ISO 27001, but it is a strategy that applies to IT Governance and is classified into 4 areas: Planning and Organization, Procurement and Implementation, Delivery and Support, Monitoring and Evaluation [50].

According to COBIT, control objectives refer to policies, procedures, practices and organizational structures that ensure the organization's objectives, as well as that any unexpected event is prevented or detected [16]. COBIT includes 34 IT processes and 13 control objectives. Each process contains a RACI diagram [16], which shows the role of each process in a managerial activity. The activities are identified from the control objectives and have a detailed structure.

As COBIT controls are mainly focused on achieving organizational objectives, it is further necessary for the security model to comply with the controls of the ISO 27001 standard, in order to ensure an optimal level of cyber security. Within the HEI, it is recommended to use COBIT to verify the maturity level of the model used [20] and to evaluate IT processes [16].

ITIL

The ITIL standard is an association between different practices and information technology services for better management of IT services [31]. Services are characterized as a means of providing value to customers without increasing security risks or cost. ITIL is a library containing a set of 5 books and 26 processes that describe different phases of implementation and provide a systematic approach to IT Governance, operations management and control of IT services [17].

As in the case of COBIT, it is recommended to use the ITIL standard combined with the ISO 27001 standard, to integrate the security practices recommended by ISO 27001 in providing the best practical process management services recommended by ITIL. This will reduce the costs of maintaining an acceptable level of security, provide effective risk management and reduce security risks at all levels [31].

As outlined above, ISO27001 is the standard recommended by many researchers, even those recommended to implement their own strategies, does not deny the need for certification to ISO 27001, to have international value approved.

2.1.2 Recommended Risk Management framework

With the increasing need for implementation and use of information technologies in HEI activity, risk management has become a mandatory process, integrated into the information security management system [42]. Risk management includes 3 processes [42]: Risk estimation, Risk mitigation and Assessment.

There are several models available for risk management, some are qualitative and others quantitative, the common goal being the value estimation of risk [2], [48]. The purpose

of applying a risk management model within the HEI is to quantitatively and qualitatively measure the level of risk for university assets [2].

The model selected must include security controls that are based on the real risks of the organization's assets and operations [2]. Following the study, it was identified that the main recommended models for risk management in HEIs are: ISO 27005, OCTAVE and OCTAVE Allegro, it can be seen in Table 5 and graphically in Figure 3. Also, in some scientific papers it is recommended to use strategies proposed by researchers, focused on the use of penetration tests to identify security risks [26], [35], [36]. However, although risk management is a mandatory process for ensuring cyber security in HEIs, much of the scientific work has not included a mechanism in this regard.

Table 5

Risk Management framework

Criterion	Framework	Scientific Paper	%
Security framework/standard for Risk Management	ISO 27005	3	10,00
	OCTAVE/ OCTAVE Allegro	3	10,00
	Not including	19	63,33
	Own framework	5	16,67

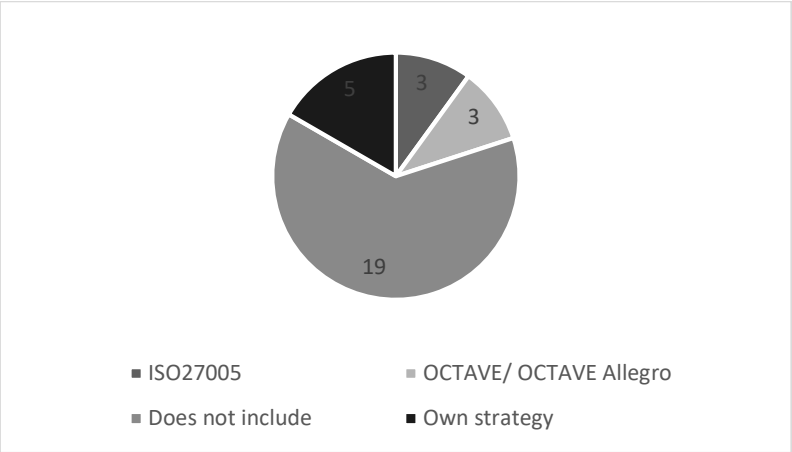

Figure 3. Recommended Risk Management strategy.

ISO 27005

ISO 27005 contains recommendations for risk management and is recommended by several researchers [18], [20], [21], [48]. The assets of the organization are classified into primary and support assets. The primary assets are all the processes and activities specific to the organization, and the assets: hardware, software, network, staff, website and organizational are support assets [48]. An important step for risk management, according to the ISO 27005 standard, is the classification of cyber security vulnerabilities according to the asset class to which they refer [21].

There are a number of vulnerabilities [21] that need to be analysed in the risk management process, which are further analysed:

- hardware components may be affected by moisture, dust, dirt and unprotected storage;
- software components can be easily exploited by unauthorized persons because they were not sufficiently tested before being exploited. Internal / external testing of software products could minimize cyber security risk [26], [36], [42], [51];

- security of communication networks [52–55], unprotected transmission lines or network architectures that do not involve the use of specialized security devices;
- personnel represent the most abstract category of vulnerabilities, attacks based on human behaviour represent 90% of all cyber-attacks [46];
- access to information assets, the risk that university sites will not be accessible due to flooding attacks is quite high, and the lack of power that can cause disconnection of servers on which web pages are hosted, is quite ubiquitous [35].

OCTAVE

The OCTAVE model is very often used for risk management and is implemented in university security models to reduce the risk of cyber threats, by identifying the causes that make the university system vulnerable [2]. This is done by identifying university assets and assessing asset-specific vulnerabilities and threats [23]. OCTAVE contains specific activities, carried out in 3 phases [2], [23] and the practical approach that can be easily used in the university environment. The first phase consists in identifying the weaknesses in the system, dynamically (each new technology added to be subjected to risk analysis). The second phase focuses on high-risk areas, which are based on the risk score, for which the Common Vulnerability Scoring System (CVSS) is used [56], to validate the vulnerability that can be exploited.

The final phase involves the creation of a security risk remediation plan to monitor recursive risk assessment activities [2].

The main steps in implementing the OCTAVE model are: identifying assets, understanding security requirements, estimating vulnerabilities, analysing 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 [2].

The OCTAVE model was recommended by [2], [23] for implementation in HEI, as it allows to create a well-defined structure of security issues associated with the academic environment. It is cost effective, because it focuses only on real assets that are at risk.

OCTAVE Allegro

OCTAVE Allegro has been recommended by researchers because it allows a more comprehensive assessment of the operational risk environment, in order to produce better results, without the need for extensive knowledge of risk assessment security [28]. This approach differs from the OCTAVE approach [28], focusing mainly on information assets in the context of how they are used, stored, processed and transferred, as well as extended to threats, vulnerabilities and any disruption [22].

The OCTAVE Allegro method is implemented in four stages:

- Setting up drivers
- Asset profile
- Identifying threats
- Risk identification and analysis

The advantages of this model are indisputable, because the score associated with the information risk is calculated based on the quantitative assessment of the threat, for example, if for a HEI the loss of reputation is important, then it will be assigned a higher score and risk mitigation measures, they will focus on information assets that contain more important data.

2.2 Answer to complementary research question CRQ2

CRQ2 is based on 2 research criteria: implementing phases and security framework functions. Having a relevant security framework for HEIs, it is necessary to know the phases of its implementation, because this is a very important process.

A security framework can be perfect but if it is implemented incorrectly, instead of benefits it could cause severe damage to organizations. So, the first criterion of CRQ2, allows to answer the scientific question which phases of the implementation of the security framework are recommended by researchers.

To create a security framework that will really enhance cybersecurity in HEIs, it is also necessary to analyse what functions it will have to perform. In this regard, the second criterion of CRQ2 has been defined, which will allow, after reviewing the selected scientific articles, to identify the functions considered relevant by researchers for an effective security framework.

2.2.1 Recommended implementing phases

Following the study, the common phases recommended for the implementation of the security model within the HEI can be identified.

According to the classification of the implementation phases in public organizations, made by Szczepaniuk E and others [57], there are 6 phases of implementation of security models in public organizations: defining security policies, defining the purpose, security risk assessment, risk management, selection of controls and the declaration of applicability.

These phases were taken into account in order to be able to respond to first research criterion of CRQ2. The purpose was to identify the implementation phases on which the scientific papers focused, the phases are non-exclusive (an article may include 1 or more phases).

Thus, 7 scientific papers focused on defining security policies, 4 papers on defining the purpose, 8 papers on security risk assessment, 8 papers on risk management, 9 papers on the selection of security controls and 8 papers on the declaration of applicability, on analysis of conformity for selected controls.

Using Venn's diagram (Figure 4), the analysis of scientific papers that recommended one or more phases of the implementation of security models in HEIs was performed.

Table 6

Security framework implementation phases

Phases of implementation of security models in HEIs	Scientific papers	No	%
Defining security policies	[18], [22], [24], [25], [30], [27], [31]	7	17,95
Defining the purpose	[21],[22],[24], [25]	4	10,26
Security risk assessment	[18],[2], [22], [23], [25], [29], [30], [31]	8	20,51
Risk management	[22], [2], [24], [29], [30], [27], [23], [39]	8	20,51
Selection of controls	[18], [21], [2], [32], [24], [33], [25], [30], [43]	9	23,08
Declaration of applicability	[18], [21], [2], [32], [22], [25], [27], [31]	8	20,51

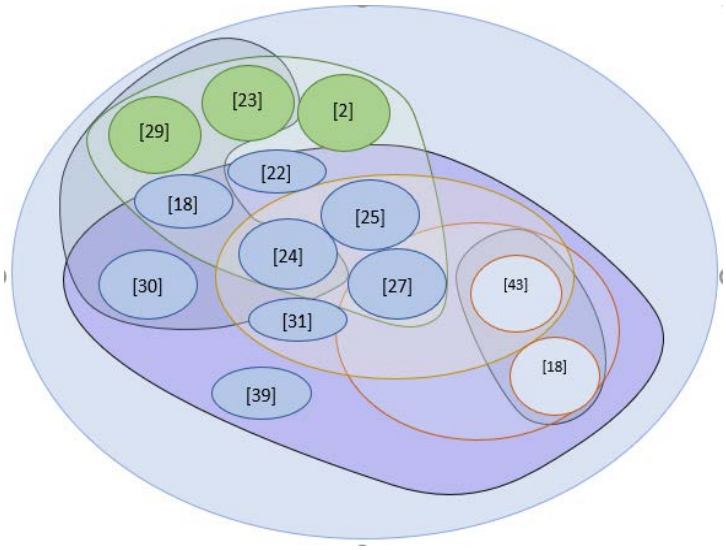

Figure 4. Implementation phases.

According to the relevance index calculated in section 2, the phases of implementing the security model within the HEI were found in 14 scientific articles, of which 3 papers contained 4 phases according to the classification [57], 7 papers focused on 3 phases, 6 papers they focused on 2 phases and 2 scientific papers described only one phase. However, no paper includes all the recommended phases [57].

2.2.2 Recommended security framework functions

To answer the second criterion of CRQ2, it is necessary to identify which are the relevant functions of a security framework in HEI, recommended by international researchers. NIST standard defines 5 functions of the security framework: identification, protection, detection, response and recovery [51].

The analysed scientific papers recommend one or several functions simultaneously. Thus, out of the 30 papers analysed, 14 are focused on identifying security risks, 15 papers on asset protection, 11 scientific papers focus on detecting threats and vulnerabilities in the university information system, 4 papers are focused on making plans to respond to incidents of security and 3 works on the implementation of incident response plans aimed at mitigating security incidents. In this sense, the Venn diagram (Figure 5) was used, which graphically reflects the common or unique recommendations, in order to identify the functions considered important for the security framework.

Table 7

Security framework functions

Relevant functions of the security framework for HEIs	Scientific Paper	No	%
Identification	[19], [20], [2], [15], [16], [23], [30], [17], [21], [31], [33], [34], [36], [38]	14	29,17
Protection	[22, [26], [17], [27], [18], [38], [35], [24], [6], [29], [25], [19], [14], [15], [16]	15	31,25
Detection	[20], [31], [33], [21], [39], [34], [14], [2], [17], [23], [30]	11	22,92
Response	[14], [2], [15], [17]	4	8,33
Recovery	[14], [2], [17]	3	6,25

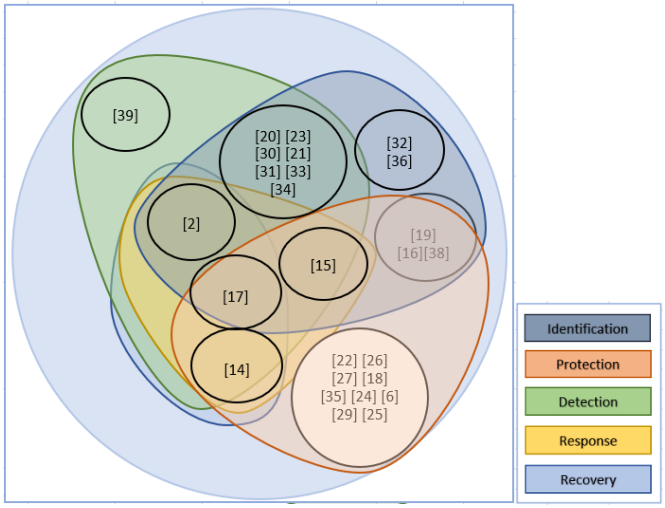

Figure 5. Relevant ISMS functions for HEIs.

Thus, it can be concluded that researchers recommend for the realization of the security framework, applicable in HEI, the functions of identification (29,17%), protection (31,25%) and detection (22,92%). The response (8,33%) and recovery (6,25%) functions are insufficiently researched.

2.3 Answer to complementary research question CRQ3

To evaluate the effect of implementation of the security framework, it was set 2 research criteria: the operational architecture on which they are based (criterion 1 of CRQ3), the validation methods (criterion 2 of CRQ3), by which the effectiveness of the security framework is tested.

2.3.1 Recommended operational architecture

The analysis and evaluation of the implemented security strategies is based on: risk assessment, control of the completeness of the proposed security objectives, security policies, IT Governance and regulations. Thus, were obtained the data reflected in Figure 6. In the case of university networks, some researchers recommend that security policies be the final strategy for ensuring cyber security [29], [30], [42]. The purpose of security policies is to issue recommendations to end users on what assets they can use [42].

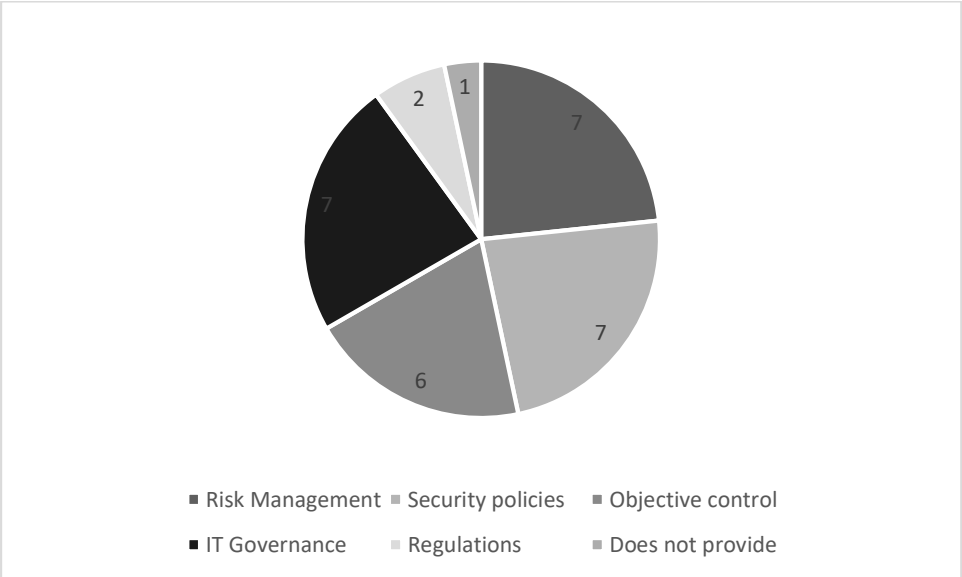

Figure 6. Evaluation of procedures.

A well-structured security policy should support top management to manage information risks and ensure the implementation of appropriate security controls [29]. According to research, some HEIs develop a single document containing all security policies and procedures, while other institutions develop different documents based on the requirements of ISO 27001, which is considered a best practice because it allows addressing to specific groups [30].

Several researchers [6], [16], [17], [39], [58] believe that efficient management of the IT infrastructure of the HEI is possible through the implementation of IT governance (ITG). ITG can be defined as a set of relational structures, processes and mechanisms that support the organization's management for the good management of the IT resources it manages. Thus, ITG can be analysed as a guide for the implementation of the cyber security control system [16]. Universities are complex organizations that require appropriate information systems to carry out their mission [6]. University information systems consist of different: applications, platforms, academic systems, cloud applications; which make the system heterogeneous [59]. All the above are necessary in the process of teaching, learning and conducting research activities, supported by university management.

Namely to manage with the efficient use of heterogeneous university IT resources it is necessary to implement ITG [6]. ITG relational mechanisms include participation and interaction between IT and administration [7], [16], but also educating employees and students to match the institution's expectations with user behaviour. Also, the creation of platforms for the distribution of successful practices for the implementation of ITGs within institutions, such as those in the UK (UCISA) or the USA (EDUCAUSE) and the certification of specialists in this regard, have increased the efficiency of ITGs in HEIs [7], [17], [58].

With all the above, studies in this field are very limited and do not contain implementation details, are relatively new and there are no relevant studies that would analyse the effectiveness and implementation of ITG in HEI, but are rather superficial, theory supported by several international researchers [6], [7], [60].

2.3.2 Recommended validation methods

The validation methods used by researchers to present the efficiency of their proposed framework, in the pre-implementation and post-implementation phases, are: case studies (15 scientific articles) that include the analysis of security systems and the use of penetration tests, surveys (11 scientific articles) that include the interview and the Delphi method [61].

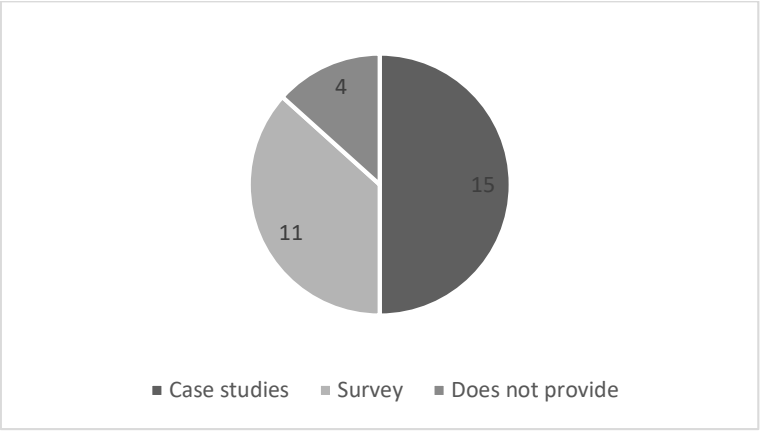

Figure 7. Validation methods.

Conclusions

This literature review was initiated to answer the main research question: " What is the cyber security strategy recommended within HEIs, how comprehensive are these researches?", in order to be able to build a security framework as comprehensive, efficient and cost-effective to increase cyber security under HEIs in the Republic of Moldova. It was very important to identify which security frameworks are recommended and analysed for implementation in HEIs, by researchers worldwide.

The 10-year period was chosen to analyse only scientific papers that are not outdated, because the IT sector is a very dynamic one. At the same time, this period allowed to analyse a larger number of scientific papers, which are still quite limited, few researchers focus on cybersecurity processes in HEIs, this statement is supported by several researchers, as specified in the introduction to this article.

Complementary questions helped to analyse these studies extensively, so the literature review did not focus only on metadata, such as: keywords, abstract or article title; but also on its content, because it was noticed that certain specifications found in the abstract of the article do not develop later in the content, from the perspective suggested at the beginning.

The method proposed by Kitchenham was applied, because it is "a guide for systematic analysis suitable for software engineering researchers" [13], a field related to cyber security. With this IT-oriented guide, it was easier to apply it, requiring only small adjustments along the way.

So, it possible now to answer the research question: "What is the cyber security strategy recommended within HEIs, how comprehensive are these researches?", by the following statements, that include also the answers to complementary questions, for a more comprehensive analysis and results:

- Researchers recommend the creation of a cyber security framework that supports ISO 27001 certification, in order to have international value. At the same time, it is necessary to identify the security framework that contains technical controls, focused on university assets, because the ISO 27001 standard specifies the objectives that the organization should achieve, but does not define how to do it.
- Risk management is identified as a key activity to implement an effective cyber security strategy. By estimating the impact that security risks may have, risk management plans will be identified to increase cyber security in HEIs. In this regard, scientific papers that included risk management strategies recommended the use of the ISO 27005 standard.
- The implementation phases of the security frameworks were described only in 14 out of 30 selected articles, but no article contains all the recommended phases for the implementation of ISMS in public organizations [57].
- The researchers consider relevant the following functions that the HEIs-oriented security framework should perform: Identification (29.17%), Protection (31.25%), Detection (22.92%).
- The finality is to build a cyber security framework that will support IT Governance and security policies creation.
- The validation methods used are: case studies, network penetration tests and surveys. This process makes it possible to identify the strengths and weaknesses of a security framework. It is a very important step in evaluating a cyber security framework.

The laborious review of the literature in this scientific paper is the knowledge base needed to create a cyber security framework, with the aim of increasing security in university networks. Thus, it was possible to identify the current state of scientific research in this field.

References

1. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity. In: *Journal of Computer and System Sciences*, Aug. 2014, 80(5), pp. 973–993, doi: 10.1016/j.jcss.2014.02.005.
2. Joshi C., Singh U. K. Information security risks management framework – A step towards mitigating security risks in university network. In: *Journal of Information Security and Applications*, Aug.2017, vol.35, doi: 10.1016/j.jisa.2017.06.006.
3. Cost of a Data Breach Report. Ponemon Institute and IBM, 2020. Accessed: 2.07.2021. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report.
4. Cyber Security Report. Check Point Research, 2020. Accessed: May 30, 2021. [Online]. Available: https://www.checkpoint.com.
5. Alexei A. Network security threats to higher education institutions. In: *CEE e|Dem and e|Gov Days*, May 2021, pp. 323–333, doi: 10.24989/ocg.v341.24.
6. Bianchi I. S., Sousa R. D. IT Governance Mechanisms in Higher Education. In: *Procedia Computer Science*, 2016, vol.100, doi: 10.1016/j.procs.2016.09.253.
7. Bianchi I.S., Sousa R.D., Pereira R.F. IT governance Mechanisms at Universities: An Exploratory Study. In: *AMCIS, Business, Computer Science*, 2017.
8. Hina S., Panneer Selvam D. D. D., Lowry P. B. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. In: *Computers and Security*, Nov.2019, vol.87, p.101594, doi: 10.1016/j.cose.2019.101594.
9. Donaldson S. E., Siegel S. G., Williams C. K., Aslam A. Cybersecurity Frameworks. In: *Enterprise Cybersecurity*, Berkeley, CA: Apress, 2015.
10. Koong K., Yunis M. Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework. In: *AMCIS, Business, Computer Science, Engineering*. 2015.
11. Oltramari A., Ben-Asher N., Cranor L., Bauer L., Christin N. General Requirements of a Hybrid-Modeling Framework for Cyber Security. In: *IEEE Military Communications Conference*, 2014, pp. 129 - 135, doi: 10.1109/MILCOM.2014.28.
12. Merchan-Lima J., Astudillo-Salinas F., Tello-Oquendo L., Sanchez F., Lopez - Fonseca G., Quiroz D. Information security management frameworks and strategies in higher education institutions: a systematic review. In: *Annals of Telecommunications*, Jul. 2020, doi: 10.1007/s12243-020-00783-2.
13. Kitchenham B. Procedures for Performing Systematic Reviews. In: *Eversleigh NSW* 1430, Australia, Jul. 2004.
14. Disterer G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. In: *Journal of Information Security*, 4(2), 2013, doi: 10.4236/jis.2013.42011.
15. Hutchins M. J., Bhinge R., Micali M. K., Robinson S. L., Sutherland J. W., Dornfeld D. Framework for Identifying Cybersecurity Risks in Manufacturing. In: *Procedia Manufacturing*, Jan. 2015, vol. 1, pp. 47–63, doi: 10.1016/j.promfg.2015.09.060.
16. Khther R. A., Othman M. Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review. In: *International Journal of Information Technology Convergence and Services*, 2013, 3(1), doi: 10.5121/ijitcs.2013.3102.
17. Gërvalla M., Preniqi N., Kopacek P. IT infrastructure library (ITIL) framework approach to IT governance. In: *IFAC-PapersOnLine*, 2018, 51(30), pp. 181–185, doi: 10.1016/j.ifacol.2018.11.283.
18. Rehman H., Masood A., Cheema A. R. Information Security Management in academic institutes of Pakistan. 2013, doi: 10.1109/NCIA.2013.6725323.
19. Cheng S. W. Reference Manager Mendeley. 2014. https://www.elsevier.com/connect/exporting-to-mendeley - from-scopus-and-sciencedirect (accessed Apr. 01, 2021).
20. Yustanti W., Qoiriah A., Bisma R., Prihanto A. An analysis of Indonesia's information security index: a case study in a public university. In: *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 296, doi: 10.1088/1757-899X/296/1/012038.
21. Itradat A., Sultan S., Al-Junaidi M., Qaffaf R., Mashal F., Daas F. Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study.

In: *Jordan Journal of Mechanical & Industrial Engineering*, 2014, vol. 8, no. 2, pp. 102–118.
22. Hommel W., Metzger S., Steinke M. Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization. In: *EUNIS Journal of Higher Education IT*, 2015.
23. Das S., Mukhopadhyay A., Bhasker B. Today's Action is Better than Tomorrow's Cure - Evaluating Information Security at a Premier Indian Business School. In: *Journal of Cases on Information Technology*, 2013, vol. 15, no. 3, doi: 10.4018/jcit.2013070101.
24. Arafat J., Daiyan G. M., Waliullah Md. Emergence of Robust Information Security Management Emergence of Robust Information Security Management emergence of Robust Information Security Management Structure around the world wide Higher Education Structure around the world wide Higher Education Institutions: Institutions: a Multifaceted Security Solution. In: *International Journal of Computer Science Issues*, 2012.
25. Liu C.-W. Huang P., Lucas H. C. IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. In: *SSRN Electronic Journal*, 2016, doi: 10.2139/ssrn.2850178.
26. Kang C. M., Joseph P. S., Issa K. A study on integrating penetration testing into the information security framework for Malaysian higher education institutions, May 2015, doi: 10.1109/ISMSC.2015.7594045.
27. Naagas M. A., Mique JR E. L., Palaoag T. D., Dela Cruz J. S. Defense-through-Deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack. In: *Bulletin of Electrical Engineering and Informatics*, Dec. 2018, vol. 7, no. 4, doi: 10.11591/eei.v7i4.1349.
28. Suroso J. S., Fakhrozi M. A. Assessment of Information System Risk Management with Octave Allegro at Education Institution. In: *Procedia Computer Science*, vol. 135, 2018, doi: 10.1016/j.procs.2018.08.167.
29. Ismail W. B. W., Widyarto S., Ahmad R. A. T. R., Ghani K. A. A generic framework for information security policy development. In: *4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI*), 2017, pp. 1 - 6, doi: 10.1109/EECSI.2017.8239132.
30. Ghazvini A., Shukur Z., Hood Z. Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. In: *International Journal of Advanced Computer Science and Applications*, 2018, vol. 9, no. 8, doi: 10.14569/IJACSA.2018.090853.
31. Suwito M. H., Matsumoto S., Kawamoto J., Gollmann D., Sakurai K. An Analysis of IT Assessment Security Maturity in Higher Education Institution. In: *K. J. Kim, & N. Joukov (Eds.), Information Science and Applications*, ICISA 2016 (pp. 701-713). (Lecture Notes in Electrical Engineering; Vol. 376). Springer Verlag. https://doi.org/10.1007/978-981-10-0557-2_69.
32. Cheung S. K. S. Information Security Management for Higher Education Institutions. In: *Pan JS., Snasel V., Corchado E., Abraham A., Wang SL. (eds) Intelligent Data analysis and its Applications*, Volume I. Advances in Intelligent Systems and Computing, vol 297. Springer, Cham. https://doi.org/10.1007/978-3-319-07776-5_2.
33. Zeng Y., Zhang H., Liu X., Fu Y., Deng Q., Ye R. Information system and management for campus Safety. In: *Proceedings of the 5th ACM SIGSPATIAL International Workshop on the Use of GIS in Emergency Management,* November 2019 Article No.: 1Pages 1–6, https://doi.org/10.1145/3356998.3365760.
34. Sanchez-Puchol F., Pastor-Collado J. A., Borrell B. Towards an Unified Information Systems Reference Model for Higher Education Institutions. In: *Procedia Computer Science*, Jan. 2017, vol. 121, pp. 542–553, doi: 10.1016/j.procs.2017.11.072.
35. Mantra I. G. N., Hartawan M. S., Saragih H., Rahman A. A. Web vulnerability assessment and maturity model analysis on Indonesia higher education. In: *Procedia Computer Science*, Jan. 2019, vol. 161, pp. 1165–1172, doi: 10.1016/j.procs.2019.11.229.
36. Sahri Z., Aziz M.E.S.A., Zolkefley K. I., Sadjirin R., Raus M. I. M. Implementing IT Security Penetration Testing in Higher Education Institute. In: *Australian Journal of Basic and Applied Sciences*, pp. 67 – 72, 2014.
37. Agrawal B., Jain A. Missing Values Prediction for Cyber Vulnerability Analysis in Academic Institutions. In: *International Journal of Computer Applications*, vol. 180, no. 43, May 2018, doi: 10.5120/ijca2018917129.
38. Ananthi C. M.T., Arul L. R.P.J. Implications, Risks and Challenges Of Cloud Computing In Academic Field – A State-Of-Art. In: *International journal of scientific & technology research*, Dec. 2019vol. 8, no. 12, pp. 3268–3278.
39. Liu C.-W., Huang P., Lucas H. C. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. In: *Journal of Management Information Systems*, vol. 37, no. 3, Jul. 2020, doi: 10.1080/07421222.2020.1790190.
40. Lucas R. A. G. G., Wadjdi A. F., Poniman A., Martha S. Sixware Cybersecurity Framework Development To Protect Defense Critical Infrastructure And Military Information Systems. In: *International Journal of Scientific & Technology Research*, 2021.

41. Li X. The Design of Information Security Management System in College. In: *Social science, education and human science,* 2016.
42. Gunawan I. G. Analysis and Implementation of Operational Security Management on Computer Center At The University X. In: CCE, 2014.
43. Pereira C., Ferreira C., Amaral L. An IT value management capability model for Portuguese universities: A Delphi study. In: *Procedia Computer Science*, Jan. 2018, vol. 138, pp. 612–620, doi: 10.1016/j.procs.2018.10.082.
44. Elgelany A., Gaoud W. Cloud Computing: Empirical Studies in Higher Education A Literature Review. In: *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 10, pp. 121–127, 2017, doi: 10.14569/IJACSA.2017.081017.
45. Ho S. Y. *et al*. What can Venn diagrams teach us about doing data science better? In: *International Journal of Data Science and Analytics*, vol. 11, no. 3, pp. 1–10, 2021, doi: 10.1007/s41060-020-00230-4.
46. Alexei A., Alexei A. Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. In: *International Journal of Scientific & Technology Research*, Mar. 2021, vol. 10, no. 3.
47. Alexei A. Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standards. In: *Journal of Social Sciences*, vol. IV(1), Mar. 2021, doi: 10.52326/jss.utm.2021.4(1).11.
48. Asosheh A., Hajinazari P., Khodkari H. A practical implementation of ISMS. In: 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, Apr.2013, doi: 10.1109/ECDC.2013.6556730.
49. Esparza D. E. I., Diaz F. J., Echeverria T. K. S., Hidrobo S. R. A., Villavicencio D. A. L., Ordonez A. R. Information security issues in educational institutions. In: *15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020, pp. 1-7, doi: 10.23919/CISTI49556.2020.9141014., doi: 10.23919/CISTI49556.2020.9141014.
50. Wolden M., Valverde R., Talla M. The effectiveness of COBIT 5 information security framework for reducing cyber-attacks on supply chain management system. In: *IFAC-PapersOnLine*, May 2015, vol. 28, no. 3, pp. 1846–1852, doi: 10.1016/j.ifacol.2015.06.355.
51. Johnson L. Security Controls Evaluation, Testing, and Assessment Handbook. Elsevier, 2020.
52. Mishima K., Sakurada T., Hagiwara Y., Tsujisawa T. Secure Campus Network System with Automatic Isolation of High Security Risk Device. In: *Proceedings of the 2018 ACM SIGUCCS Annual Conference,* September 2018, Pages 107–110, https://doi.org/10.1145/3235715.3235738.
53. Tsunoda H., Keeni G. M. Security by simple network traffic monitoring. In: *Proceedings of the Fifth International Conference on Security of Information and Networks*, October 2012, Pages 201–204. https://doi.org/10.1145/2388576.2388608
54. Mumtaz N. Analysis of information security through asset management in academic institutes of Pakistan. In: *2015 International Conference on Information and Communication Technologies (ICICT)*, 2015, pp. 1-4, doi: 10.1109/ICICT.2015.7469581.
55. Naagas M. A., Palaoag T. D. A Threat-Driven Approach to Modeling a Campus Network Security. In: *Proceedings of the 6th International Conference on Communications and Broadband Networking*, February 2018 Pages 6 – 12, https://doi.org/10.1145/3193092.3193096.
56. Singh U. K., Joshi C. Quantitative Security Risk Evaluation using CVSS Metrics by Estimation of Frequency and Maturity of Exploit. In: *Proceedings of the World Congress on Engineering and Computer Science*, 2016, Vol I, WCECS 2016, San Francisco, USA 2016.
57. Szczepaniuk E. K., Szczepaniuk H., Rokicki T., Klepacki B. Information security assessment in public administration. In: *Computers and Security*, Mar. 2020, vol. 90, p. 101709, doi: 10.1016/j.cose.2019.101709.
58. Alghamdi S., Win K. T., Vlahu-Gjorgievska E. Information security governance challenges and critical success factors: Systematic review. In: *Computers and Security*, vol. 99, Dec. 2020, doi: 10.1016/j.cose.2020.102030.
59. Wilmore A. IT strategy and decision-making: a comparison of four universities. In: *Journal of Higher Education Policy and Management*, vol. 36, no. 3, May 2014, doi: 10.1080/01587919.2014.899056.
60. Hina S., Dominic D. D. Information security policies: Investigation of compliance in universities. In: *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, 2016, pp. 564-569, doi: 10.1109/ICCOINS.2016.7783277.
61. Skinner R., Nelson R. R., Chin W. W., Land L. The Delphi Method Research Strategy in Studies of Information Systems. In: *Communications of the Association for Information Systems*, vol. 37, 2015, doi: 10.17705/1CAIS.03702.