Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 35-52 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

DESIGN & DEVELOPMENT OF A CYBER SECURITY CONCEPTUAL FRAMEWORK FOR HIGHER EDUCATION INSTITUTIONS IN THE REPUBLIC OF MOLDOVA

Alexei Arina, Department of Telecommunications and Electronic Systems, Technical University of Moldova

ABSTRACT: This scientific paper reflects the results of research, which aimed to develop a Cyber Security Conceptual Framework for Higher Education Institutions in the Republic of Moldova, to increase cyber security in academic environment. The scientific method Design Science Research was selected for the development of the security framework, due to the practical value it generates, being one of the most used qualitative scientific methods in the field of engineering. The identification of the key processes and stages of implementation of the Cyber Security Conceptual Framework, assessed according to value criteria, supports the way in which cyber security in universities in the Republic of Moldova can be increased. Important contributions are for the academic environment in the Republic of Moldova, where until now, there has been no reference framework to ensure the protection of academic processes.

KEYWORDS*: cyber security, framework, Higher Education Institution, DSR, academic processes.*

1. INTRODUCTION

With the development of information technology, cyber security has become one of the biggest global challenges for organizations implementing new technologies worldwide (Asosheh et al., 2013). Cyber security is defined as a collection of tools, techniques, policies, security measures, security guidelines, risk mitigation strategies, actions, training, good practices, security reinsurance and the latest technologies that can be used to protect cyberspace and user assets (Humayun et al., 2020; von Solms & von Solms, 2018). Common cyber security regulations and requirements would allow a more comprehensive approach to cyber security in organizations with a similar profile. Creating a common cyber security framework, covering core processes, to ensure compliance with the three principles of cyber security: confidentiality, integrity and availability; it would facilitate the implementation of comprehensive security mechanisms and, as a result, increase cyber security. An important role, in this regard, is played by the Government, which has a proactive role in the management of cyber security policies and infrastructure in order to issue standardized recommendations, at state level, especially in the case of public institutions. The harmonization of cyber security strategies developed by the state with international standards ensures compliance and international recognition (Asosheh et al., 2013).

The Republic of Moldova is a developing country, that in recent decades has been trying to align with international practices in the public domain. Information technology plays a very important role in providing public services. According to the annual report on monitoring the evolution of the global information society "Measuring the information society 2017", launched by the International Telecommunication Union, the Republic of Moldova ranks 59th out of 176 countries in the ranking. At the European level, the Republic of Moldova has advanced compared to the global and regional average, being among the top 10 countries with the most dynamic developments in the world (Alexei, 2021).

At the same time, the Information Security Strategy for 2019-2024 (RM Parliament, 2018), adopted by the Parliament of the Republic of Moldova, also identified as a major problem in the field of cyber security, the lack of an integrated cyber security management system that would provide a comprehensive approach to cyber security (points 39 and 40 of the Strategy), solving this problem is identified as a key step in the development of a secure information society in the Republic of Moldova.

There are currently 15 public and 9 private Higher Education Institutions in the Republic of Moldova. Higher Education Institutions are subordinated to the Ministry of Education and Research, so the provisions of the Information Security Strategy must be implemented. However, the results of the survey, conducted by the author between September-November 2020, in which stakeholders from the 9 largest public institutions in the Republic of Moldova participated, show that Higher Education Institutions are not certified with an information security standard and have not implemented an authorized cyber security framework (Alexei Arina, 2021).

Moreover, the diversity of electronic services provided by academia is constantly growing, especially as a result of the pandemic with Covid 19 and the transition to online education. To ensure access to learning platforms, digital libraries, or university management systems, university information systems are open by design (Jang-Jaccard & Nepal, 2014), decentralized and multi-user. Software and network applications have become an integral part of the university environment both in Moldova and internationally. Access to modern technologies is valuable, on the one hand, for the development of

modern learning environments, but on the other hand, it increases the vulnerability of communication networks and the number of threats.

Thus, in the context of the above, the research problem is:" the lack of a cyber security framework focused on academic processes in Higher Education Institutions in the Republic of Moldova, which could be used as a reference framework".

Implementing a security concept that does not take into account the security requirements specific to the academic environment and the activities they carry out, increases the likelihood of a false sense of security.

So, the purpose of this scientific paper is to develop a cyber security conceptual framework (CSCF), focused on the academic processes of Higher Education Institutions in the Republic of Moldova, which complies with the provisions of international standards and best practices in the field, in order to solve the research problem.

The following section presents the results of the literature review, the purpose of which was to identify cyber security strategies for academia, recommended by researchers, internationally. The third section presents the scientific method used to solve the research problem, and the fourth section presents the research results.

2. LITERATURE REVIEW

To achieve the purpose of this research work, the author has carried out a literature review of the last 10 years, using the method proposed by Kitchenham (Barbara Kitchenham 2004), to determine the strategies approached by researchers at the international level and how a cyber security framework can be integrated into academic processes. A comprehensive research paper has already been published (Alexei, 2021).

The implementation of a cyber security framework in HEIs has been recommended by several researchers over time. Cybersecurity frameworks assist in the implementation of Information Security Management Systems, providing a comprehensive approach and comprehensive solution, which includes: policies, tools and procedures needed to increase security (Itradat et al. 2014) and strengthen information systems (Oltramari et al. 2014; Donaldson et al. 2015; Koong and Yunis 2015; Merchan-Lima et al. 2020).

The effectiveness of the proposed solution depends on risk management, which is a mandatory process when conceptualizing the cyber security framework, because identifying assets that assist academic processes, and determining threats and vulnerabilities that influence confidentiality, integrity and availability, have a major impact on the outcome, which will have the security framework (Hommel, Metzger, and Steinke 2015). Risk management can reduce the risks of certain important processes, financial losses or damage to the reputation of higher education institutions (Suroso and Fakhrozi 2018) and can support the creation of security policies (Hommel, Metzger, and Steinke 2015).

These arguments served as a reason for analyzing the recommended strategies for creating the cybersecurity framework, risk management and how to integrate into HEIs, to increase cyber security.

2.1 INTERNATIONAL CYBER SECURITY STANDARDS

Analyzing the literature in the field, we identified 3 international standards recommended in various scientific studies, indexed by the largest databases, such as: Scopus, ScienceDirect, ACM Digital Library, IEEE Xplore, Springer; to be implemented in HEIs. These are: ISO 27001, COBIT AND ITIL.

ISO 27001

The most widely used international standard in the field is ISO 27001 (Rehman, Masood, and Cheema 2013; Itradat et al. 2014), and if we analyze the results of the annual surveys presented by ISO (International Organization for Standardization 2020), the number of organizations certified with ISO 27001 is constantly increasing from 31 910, in 2018, to 44 486 in 2020. The Republic of Moldova is no exception, so the number of organizations certified in 2020 has increased compared to 2018, from 3 to 8.

In the field of Education can be seen a positive trend, at international level, so that if in 2018, the number of institutions certified with ISO 27001 was 137, in 2020 they are 187. Unfortunately, in the field of education, in 2020, there is no institution certified with ISO 27001 in the Republic of Moldova. Although the empirical research conducted by the Rotterdam School of Management, Erasmus University, based on 645 responses from companies, internationally, ISO 27001 certification, had a significant positive effect on increasing information security, estimated by 85% of respondents (Nowak 2015).

ISO 27001 is based on the implementation of an information security management system within organizations and addresses systematic processes, technologies and human resources, for risk assessment and assistance in the information

management process. It is based on the Deming cycle (Haufe et al. 2016), which is a closed action process that assists in information security management processes.

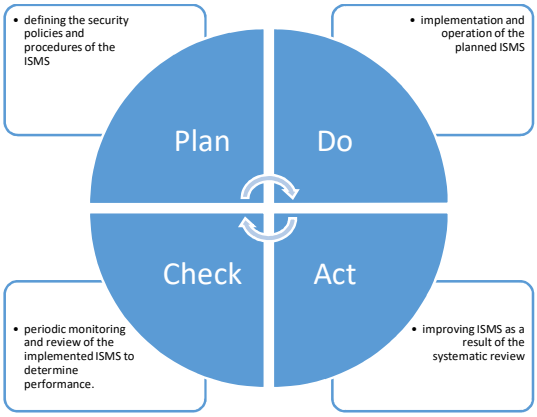

Fig. 1 Deming cycle

With regard to ISMS in HEIs, the Deming cycle represents consecutive actions aimed at achieving the main objective, the implementation of information security within an institution (Szczepaniuk et al. 2020).

The ISO 27001 standard is organized into 14 sections, 35 objectives and 114 security controls, but not all sections of the standard are applicable in HEIs (Rehman, Masood, and Cheema 2013). Researchers recommend the use of at least 8 sections from ISO 27001 in HEIs: asset management, human resource management, physical controls, access control, communications control, operational control, incident management, information system control, and business continuity (Cheung 2014; Esparza et al. 2020).

COBIT

Another standard recommended by researchers to be implemented in HEIs is COBIT. COBIT is a strategy that applies IT Governance and is classified into 4 areas: Planning and Organization, Procurement and Implementation, Delivery and Support, Monitoring and Evaluation (Wolden, Valverde, and Talla 2015).

COBIT's control objectives refer to policies, procedures, practices and organizational structures that ensure the organization's objectives, as well as to prevent or detect any unexpected events (Khther and Othman 2013). COBIT includes 34 IT processes and 13 control objectives. Each process contains a RACI diagram (Khther and Othman 2013), which shows the role of each process in a managerial activity. The activities are identified from the control objectives and have a detailed structure.

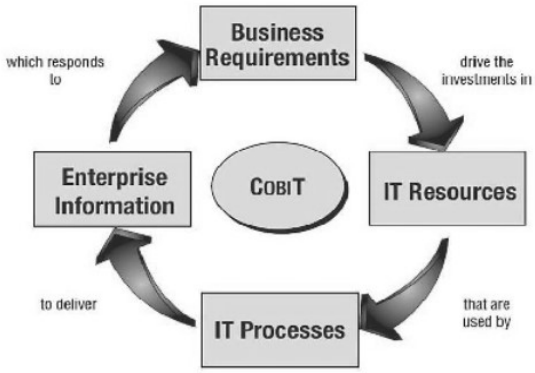

Fig 2. COBIT framework principle (Khther and Othman 2013)

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 cybersecurity. Within the HEIs, it is recommended to use COBIT to verify the maturity level of the model used (Yustanti et al. 2018) and to evaluate IT processes (Khther and Othman 2013).

ITIL

The ITIL framework is presented as an association between different practices and information technology services for better management of IT services (Suwito et al. 2016). Services are characterized as a means of providing value to customers without increasing security risks or cost. ITIL is a bookstore containing a set of 5 books and 34 processes that describe different phases of implementation and provide a systematic approach to IT Governance, operations management and control of IT services (Gërvalla, Preniqi, and Kopacek 2018).

As in the case of COBIT, it is recommended to use the ITIL framework combined with the ISO 27001 standard, in order to integrate the security practices recommended by ISO 27001 in providing the best practical process management services recommended by ITIL. This will reduce the cost of maintaining an acceptable level of security, provide effective risk management and reduce security risks at all levels (Suwito et al. 2016).

Although it would appear that these 3 frameworks contain identical instructions, the implementation requirements are still different, which drastically affects the effect of implementation, especially the required budget. Therefore, before using any of the listed frameworks, it is necessary to clarify the implementation costs, which are usually limited within the HEIs.

ISO 27001 is the most widely used security standard internationally, so it can be concluded that it is the easiest to implement, recognized and implementation costs are lower than ITIL and COBIT, ISO 27001 is like English, has a proven international value.

2.2 RECOMMENDED TECHNIQUES FOR RISK MANAGEMENT IN HEIS

Risk management includes coordinated activities to lead and control an organization in terms of cyber risk (ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary 2018). Cyber risk can be defined as a security event that exploited a vulnerability in the information system and caused the threat (Wangen, Hallstensen, and Snekkenes 2018; Ulven and Wangen 2021). An information security event is an identified occurrence of a system, service, or network condition that indicates a possible breach of information security policy, or failure of controls, or a previously unknown situation that may be relevant to security (ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary 2018) and has a impact and a likelihood (Wangen, Hallstensen, and Snekkenes 2018). At the basis of information risk analysis is the process of identifying threats (Szczepaniuk et al. 2020), threats are defined as "any phenomenon (process, event), undesirable in terms of undisturbed operation of a system" (Szczepaniuk et al. 2020).

A holistic approach to cybersecurity management in HEIs is essential because it provides an overview of all resources that need to be protected. Risk assessment methods should take into account the dependencies between resources that assist university electronic services (Hariyanti, Djunaidy, and Siahaan 2018), so the methods must be able to adapt and be dynamic and appropriate for the university environment. As electronic services are constantly changing, risk factors are changing (Harkins 2016) and affecting the value of university activities (Rojas and Lesmes 2016).

Following the study, it was identified that the main recommended models for risk management in HEIs are: ISO 27005, OCTAVE and OCTAVE Allegro (Alexei, 2021).

ISO 27005

The standard ISO 27005 is part of the ISO 27000 family of security standards. It is the standard underlying risk management, which must be achieved before the creation and implementation of an ISMS, according to ISO 27001.

ISO 27005 addresses security risks from the perspective of information assets, defined as any asset that has value to the organization and requires protection (ISO/IEC 27000:2018, 2018).

According to ISO 27005 (ISO/IEC 27005: Information technology — Security techniques — Information security risk management 2018), all information assets should be classified as primary assets and support assets. The primary assets are all academic processes and information, and the assets: hardware, software, network and communications, personnel and infrastructure, are support assets (Asosheh, Hajinazari, and Khodkari 2013).

OCTAVE

The OCTAVE model is implemented in university activities to reduce the risk of cyber threats, by identifying the causes that make the university system vulnerable (Joshi and Singh 2017). OCTAVE contains specific activities, performed in 3 phases (Joshi and Singh 2017; Das, Mukhopadhyay, and Bhasker 2013). The first phase is to identify the weaknesses of the system, dynamically (for each new technology the risk is assessed). In the second phase, the risk score is calculated,

an important resource in this regard is the Common Vulnerability Scoring System (CVSS) (Singh Umesh Kumar and Joshi C. 2016), to validate the vulnerability that can be exploited. The final step is to create a security risk remediation plan and recursive risk assessment activities (Joshi and Singh 2017).

OCTAVE Allegro

OCTAVE Allegro has been recommended by researchers because it allows for a more comprehensive assessment of the operational risk environment in order to produce better results without the need for extensive knowledge of security risk assessment (Suroso and Fakhrozi 2018). It focuses mainly on information assets in the context of how they are used, where they are stored, processed and transferred, as well as extended to threats, vulnerabilities and any disruption (Hommel, Metzger, and Steinke 2015).

2.3 SECURITY FRAMEWORK IMPLEMENTATION PHASES

Having a security framework focused on university processes, it is necessary to know the stages of its implementation. The security framework can be very well structured, but if implemented incorrectly, it could cause serious harm to organizations instead of benefits.

Following the study, the recommended common steps for the implementation of the security framework within the HEIs can be defined. According to the classification of implementation stages in public organizations, made by Szczepaniuk E and others (Szczepaniuk et al. 2020), there are 6 stages of implementation of security frameworks in public organizations: defining security policies, defining purpose, security risk assessment, risk management, selection of controls and the statement of applicability.

3. RESEARCH METHOD

An essential part of any research paper is the scientific method selected for the study and the tools that facilitate the achievement of relevant scientific results. Without a strong component to produce explicitly applicable research solutions, cyber security research faces the potential to lose influence on the research flows for which such applicability is important (Peffers et al. 2007).

The challenge was to select a method that would allow the creation of a product, a security framework that would contribute to increasing cyber security in HEIs in the Republic of Moldova, to solve the research problem defined above. This premise was the basis for identifying the scientific method of Design Science Research (DSR), which is widely used internationally, and the research results can be models, concepts or frameworks (vom Brocke, Hevner, and Maedche 2020; Hevner et al. 2004; Baskerville et al. 2018). DSR is defined as "a problem-solving paradigm that seeks to improve knowledge by creating innovative artifacts" (vom Brocke, Hevner, and Maedche 2020). The DSR method has been appreciated as one of the main research methods for the engineering field (Dresch, Lacerda, and Antunes Jr 2015).

The literature identifies 6 typical stages of the DSR project: problem identification and motivation, definition of objectives for solution, design and development / design of the artifact, demonstration, evaluation, followed by communication of results (Peffers et al. 2007; Chandra Kruse, Seidel, and vom Brocke 2019; vom Brocke, Hevner, and Maedche 2020). Figure 3 shows the actions performed according to the DSR steps for CSCF development.

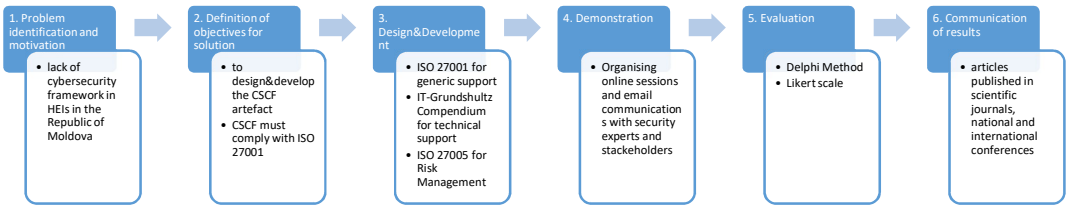

Fig 3. CSCF development on DSR stages

A. Problem identification and motivation

Higher Education Institutions in the Republic of Moldova are not certified with any security standards and have not implemented a comprehensive cybersecurity framework, such as an Information Security Management System, which

is recommended by ISO 27001, or another cyber security framework. Although it provides a variety of digital educational services.

B. Definition of objectives for solution

The result of this type of research, as mentioned above, is an artifact that solves a problem in the field, in this case, it will achieve the purpose of this research paper, also known as the concept of solution, which must be evaluated by criteria of value or utility (Dresch, Lacerda, and Antunes Jr 2015). The value criteria according to which the CSCF artifact can be evaluated are reflected in Table 1.

Table 1. Value criteria of CSCF artifact

Nr	Criterion	Arguments
1	Target group oriented	Contain controls corresponding business processes in academia
2	Implementation phases	The artifact must determine the main steps after which the cybersecurity framework will be implemented within the HEI
3	Predefined roles	The roles of staff involved in the implementation of cybersecurity in HEIs must be clearly defined, in order to know the responsibilities of the post and to designate the owners of critical assets.
4	Risk management	In order to increase the effectiveness of the security framework, it is necessary to identify the real risks, related to the critical assets and the threats that may affect them. To assess the impact of risks.
5	Efficient	The efficiency of the artifact depends directly on how well it is understood by HEI specialists, who are going to implement it. How clearly the objectives, purpose and implementation phases were defined.
6	Scalable	It can be implemented in any institution, regardless of its size and the complexity of the services it provides
7	International importance	To comply with the Bologna Process, which is being implemented in Moldovan universities. Subsequent certification of institutions with an international standard is an appreciable objective.

C. Design and development

The development of the CSCF artifact was based on the knowledge gained from the review of the literature, the result of which showed that researchers recommend for implementation in HEIs the standard ISO 27001, because it has a proven value over time and satisfies the value criteria of point B. The challenge was to determine how ISO 27001 controls could be implemented, being generic. Thus, it was established that the development of the CSCF artifact should be achieved through the synergy of ISO 27001, ISO 27002 which is a guide used to implement information security standards and IT - Grundschutz Kompendium, which is a German technical guide containing the tools necessary for the implementation of security controls. ISO 27005 has been used to achieve risk management, through interdependencies between the university's business processes and supporting assets.

D. Demonstration

Stakeholders from universities and experts in the field of cybersecurity in the Republic of Moldova were contacted via email. Online sessions were held to demonstrate how CSCF artifact can be implemented in HEIs.

E. Evaluation

The qualitative method of evaluating the artifact was used, through several Delphi rounds, which allowed obtaining the evaluation through empirical evidence (feedback from experts and specialists in the field) and evidence proven by applying the international standard ISO 27001. The qualitative approach facilitates a better understanding of the perceptions, beliefs and attitudes of the participants in the philosophical interpretive study of information systems (Myers and Newman 2007). The qualitative method allows to understand the context of a solution, including based on the comments made by HEIs specialists.

Thus, for the initial evaluation, the CSCF artifact was presented to the experts for evaluation, a great value representing the recommendations given by the experts. Subsequently, for empirical evaluation, the CSCF artifact was presented to HEIs stakeholders. The post-implementation feedback will be presented after the CSCF artifact will be implemented for a certain period of time in the HEIs of the Republic of Moldova.

F. Communication of results

The communication of the results took place through the publication of scientific articles and participation with communiqués at national and international conferences. Thus, the criteria according to which the CSCF artifact was developed, the novelty of the product and how it will have an impact on the increase of cybersecurity in the HEIs will be exposed. The CSCF artifact was presented to both the technology-oriented and the management-oriented public.

4. RESULTS

The approach to cybersecurity as a system requires a holistic approach, an overview, not a segmented one (Szczepaniuk et al. 2020), because security is interdisciplinary and does not necessarily refer only to information systems, but involves applicable law, organizational structure and other aspects that may influence this process.

The CSCF artifact is a cybersecurity management system focused on academic activities. The main purpose of the CSCF implementation is to increase cybersecurity in HEIs in the Republic of Moldova.

4.1 CSCF ARTIFACT DESIGN

The conceptual framework takes into account the mission of the organization, the academic institution in this case, and ensures the provision of electronic services respecting the three principles of security: Confidentiality, Integrity and Availability.

The IPO (Input, Process, Output) model (MacCuspie et al. 2014) was used to model the preliminary conceptual framework, the result obtained is reflected in figure 4.

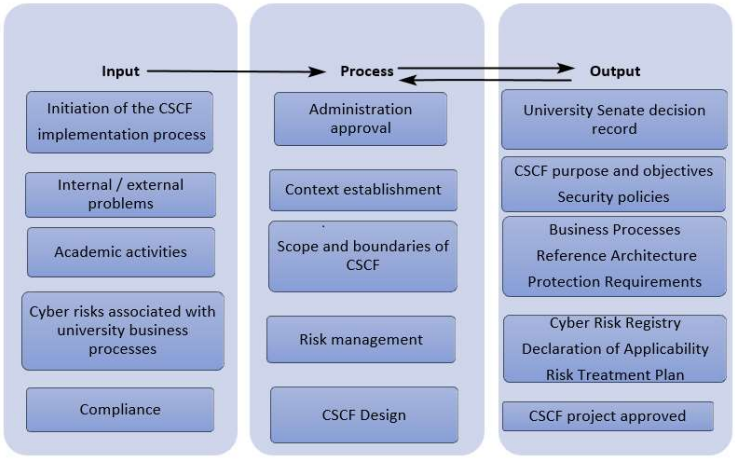

Fig 4. Preliminary conceptual framework

The inputs will influence the processes. The outputs are the goal to be achieved, each stage indicates the life cycle of the proposed conceptual framework.

To operationalize the conceptual framework described above, the Deming cycle will be used to continuously increase the quality of the security framework (Disterer, 2013), due to the dynamic nature of cybersecurity and the mandatory iterative nature of a cybersecurity management system. The application of the Deming cycle emphasizes the need for process guidance, as well as the integration of operations planning and constant verification of implementation in line with planning (Haufe et al. 2016).

As mentioned above, the conceptual framework for cybersecurity will be proposed through the synergy of the following international standards:

- ISO 27001 - which will support the creation of the CSCF;
- ISO 27002 - for the implementation of the CSCF, represents the code of practice for security controls and a good support for ISO 27001;
- ISO 27005 - for the management of security risks in HEIs;

- IT-Grundschutz-Kompendium for technical support.

Conceptual framework processes modeled using the IPO method, the four dimensions of the Deming cycle, and the recommendations of international organizations were applied to determine the design of the CSCF. Framework implementation stages in Moldovan HEIs is reflected in Figure 5.

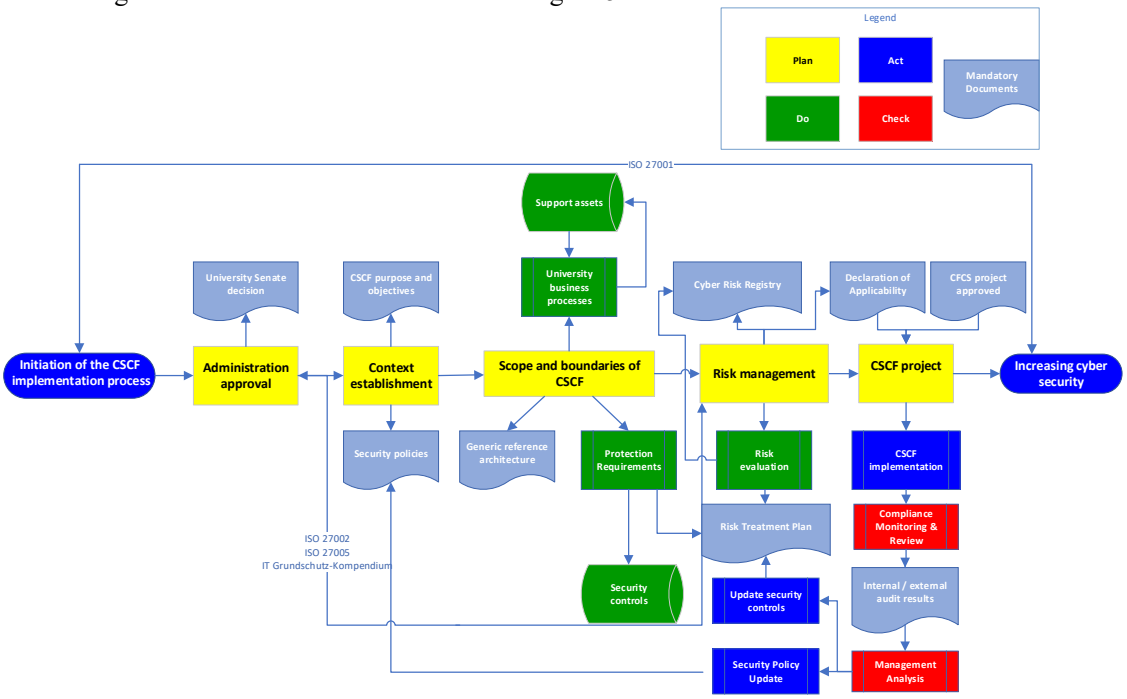

Fig 5. CSCF implementation stages

4.2 CSCF ARTIFACT DEVELOPMENT

CSCF is designed to be a valuable resource and support for Moldovan universities that will implement their own security concept, aligned with the specifics and activities of HEIs, supported by research results, empirical study and international standards. This section will analyze and set out as explicitly as possible these important issues that will result in an increase and a comprehensive approach to cybersecurity, so that the results of this research can be reproduced and put into practice by stakeholders.

4.2.1 Administration approval

The approval of the administration in the university environment of the Republic of Moldova refers to the Senate of the Institution, the supreme governing authority, which consists of the President of the Senate, Secretary and Senators. At this stage, the preliminary goal and organizational priorities are set (Asosheh, Hajinazari, and Khodkari 2013). The main goal for implementing a concept of security in universities is the comprehensive approach to cybersecurity, based on existing reasoning, that it is more cost effective to protect properly than to recover in the event of a disaster, whether it is intentional or not. An additional argument is the provisions of the National Strategy for Information Security of the Republic of Moldova, for the period 2019-2024, which identifies as the main problem for ensuring information security, the lack of information security management systems at the national level (RM Parliament, 2018).

According to ISO 27001, the organization, which aims to implement a cybersecurity framework, must constantly allocate resources "for the establishment, implementation, maintenance and continuous improvement" (ISO/IEC 27001, 2013). The allocation of the necessary resources refers to: human resources, financial resources, information resources, necessary infrastructure.

4.2.2 Context establishment

In order to develop CSCF, the academic institution must define the purpose of implementing the security framework, identify business processes and support assets.

According to ISO 27001, the HEI must identify external and internal issues (Disterer 2013), which are relevant to its purpose (ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT 2013). In order to analyze the internal problems faced by the HEI, it is necessary to take into account: the strategy and objectives of the organization, business processes and support assets, national / international contracts and derivative relations, intellectual property and research results, physical infrastructure and environment, information systems and media used.

This can define the following internal issues: manipulation of personal data, breach of confidentiality, unauthorized access to assets containing sensitive data of the organization, financial losses, interruption of basic activities (courses, exams, inability to enroll in studies), interruption of services, disruption of internal operations and with third parties, financial costs associated with loss of staff, replacement of equipment, value of research, loss of assets, loss of competitive advantage.

External issues cannot be controlled by HEIs, and the following issues need attention: higher-level laws and regulations (state, governmental), socio-cultural and natural environment, financial and macroeconomic, technological.

Depending on the structure and size of the HEI, for the implementation of the CSCF, it is necessary to form a team responsible for the implementation and control of the concept of cybersecurity, consisting of the Information Security Officer and other members. The ISO 27001 standard requires regular and mandatory qualifications of the Information Security Officer, who can be recruited both from university staff and from outside, as long as there are documents attesting the qualification required to hold this position.

Security policies

Security policy reflects the attitude of HEI management towards cybersecurity. The main objective for the implementation of security policies, according to ISO 27002, is to provide management direction and support for information security in accordance with relevant business requirements, laws and regulations (ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security controls 2013).

The analysis of university websites in the Republic of Moldova revealed that academic institutions have published the GDPR Policy, but there are no general or specific security policies, as confirmed by the results of the author's survey involving 9 stakeholders from the most large higher education institutions in the Republic of Moldova, of which only 22.2% stated that they have internal security policies.

According to several researchers (Ghazvini, Shukur, and Hood 2018; Flowerday and Tuyikeze 2016) the way in which security policies are developed and implemented remains uncertain, which is a shortcoming of this stage. The content of security policies also differs, creating uncertainty about the content.

It is recommended for the development of security policies in academic institutions in Moldova to follow the following steps, reflected in Figure 6.

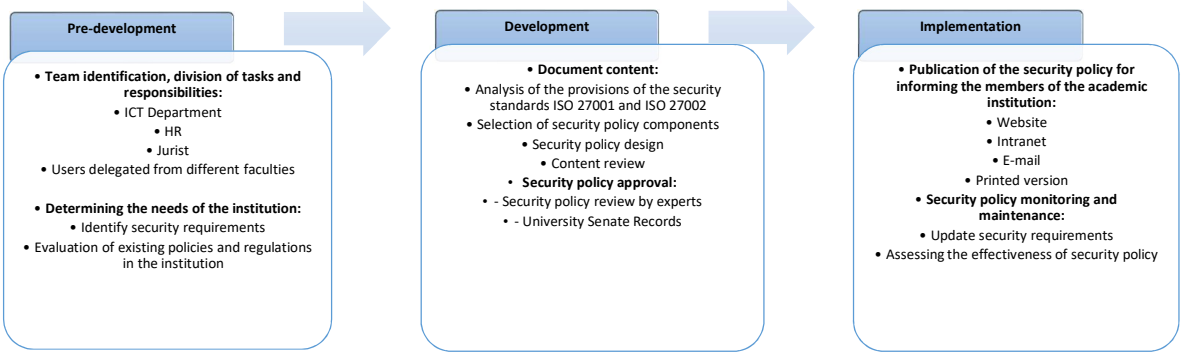

Fig 6. Generic framework for security policies development in HEIs

It is recommended that the security policy as well as the specific security policies be established in accordance with the structure reflected in Table 2.

Table 2. The structure of security policy

Key items	**Justification** (According to the provisions of the ISO 27002 standard)
Title	General or specific: control access, backups, BYOD, etc.
Version and authors	It will include all existing versions of the respective security policy, the date of the changes, the responsible person

Goal	Describes the expectations of the administration of the institution as a result of the implementation of the policy and the problems that will be solved
Scope and boundaries	Describe the area to be covered by the policy, such as: access control, security of communication, acceptable use, etc .; to whom that security policy is addressed
Presentation	A brief description of cybersecurity issues, which may include threats, vulnerabilities and risks specific to the field of education
Security policy requirements	Describe in detail, as clearly and explicitly as possible, the requirements of the institution
Roles and responsibilities	Defines who is responsible for violating security policy requirements and where security incidents can be reported
Related documents	Describe other relevant policies (if any) that may help minimize security issues and incidents, or links to additional support

4.2.3 Scope and boundaries of CSCF

The need to reflect a generic reference architecture specific to the university environment on the one hand provides an overview of the typical functionality (Pääkkönen and Pakkala 2015) of academic activities, and on the other hand supports the creation of architectures for each institution (Angelov, Grefen, and Greefhorst 2012), which aims to implement a security concept.

The empirical study facilitated the creation of a generic reference architecture specific to the university environment in Moldova, obtained from semi-structured interviews with university network administrators reflected in Figure 7.

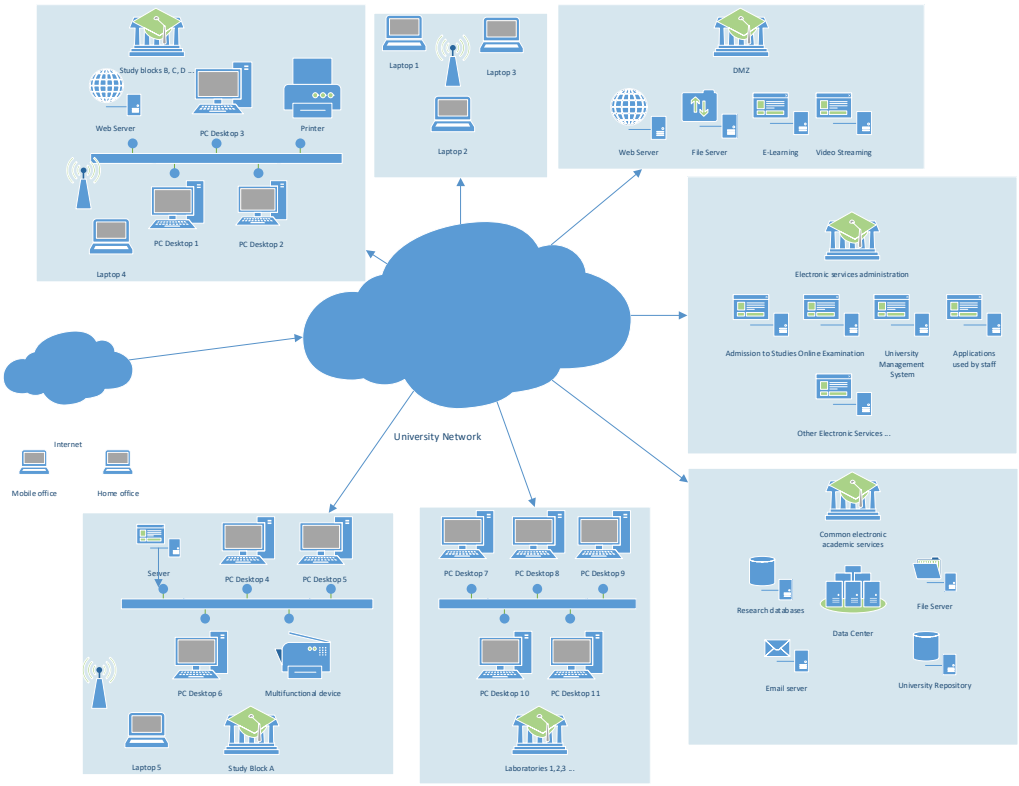

Fig 7. The reference architecture of HEIs in Moldova

The identification of the academic business processes allowed the development of the CSCF artifact oriented towards the university environment, in order to satisfy the Target Group Oriented criterion. Business processes can be defined as "sets of interconnected tasks that lead to the creation of a product or service" (Ivanov et al. 2011). Basic university business processes are education and research. The CSCF will only consider the components of the education process, as it also includes the research aspects, the results are exposed in the table 3.

Table 3. Academic business processes

Academic business processes	Description

Common academic services	Network infrastructure Stationary workstations (Laboratories) Mobile workstations or BSOD Remote work (VPN, WLAN) Centralized services: - website - virtual servers - centralized access control, - user identification and authentication - email services - file services
Admission to Studies	- application process - preliminary examination - the approval processes - generate notifications - final approval - deletion of the applicant's data
IT infrastructure for students	- laboratories with specialized equipment - video conferencing applications - online learning platforms
Online examination	- creating exam questions - creating the evaluation test - attendance control - exam evaluation - notation in the dean's office system - publishing / announcing test results, archiving the results - creating backups - creating the archive - creating the paper archive - verification of information
University Management System	- administration of the student's entire academic career, - results of examination sessions, - contract and study agreement - electronic register - anti-plagiarism system for students, - additional fees, - holiday order, - employee pay slips, - orders and regulations, university news

This list is not exhaustive, other university activities can be excluded / included, depending on the spectrum of electronic services provided by HEI, thus supporting the scalability criterion of CSCF.

Depending on the protection requirements, the recommended security controls are proposed to be classified into:

- Basic (mandatory) security controls required to be mandatorily implemented by any HEI that creates a security concept;
- Standard security controls for institutions aimed at certification with ISO 27001 or another security standard.

4.2.4 Risk management

In order to support the criteria of International Importance and Risk Management, it is recommended to use the ISO 27005 standard, due to its international importance and because it is a direct support for the implementation of ISO 27001, a standard selected as a reference for creating the CSCF artifact. Risk management includes coordinated activities to manage and control an organization in terms of risk (ISO/IEC 27000:2018, 2018.).

Cyber risk can be defined as a security event that exploited a vulnerability in the information system and caused the threat (Wangen, Hallstensen, and Snekkenes 2018; Ulven and Wangen 2021). An information security event is an identified occurrence of a system, service, or network state that indicates a possible breach of information security policy, or a failure of controls, or a previously unknown situation that may be relevant to security (ISO/IEC 27000:2018, 2018) and has a impact and a likelihood (Wangen, Hallstensen, and Snekkenes 2018; ISO/IEC 27005: Information technology — Security techniques — Information security risk management 2018). The basis of information risk analysis is the process of identifying threats (Szczepaniuk et al. 2020), which are defined as "any phenomenon (process, event), undesirable in terms of undisturbed operation of a system" (Szczepaniuk et al. 2020).

As previously stated in this research paper, a holistic approach to cybersecurity management in HEIs is essential because it provides an overview of all resources that need to be protected. Risk assessment methods should take into account the dependencies between the resources that assist university electronic services (Hariyanti, Djunaidy, and Siahaan 2018), so the methods must be able to adapt and be dynamic and appropriate for the university environment. As electronic services are constantly changing, risk factors are changing (Harkins 2016) and affecting the value of university activities (Rojas and Lesmes 2016).

From the considerations presented above, a new approach to risk management is proposed in terms of university business processes, because they are limited in number, versus the impressive number of support assets, and the assessment of security risks in terms of business processes supports the holistic approach to cybersecurity in academia. Thus, when designing a new business process, security risks are taken into account, this new concept is called "risk conscious business process management" (Ahmed and Matulevičius 2014; Khanmohammadi and Houmb 2010; Jakoubi et al. 2010).

Another problem that can be solved by addressing the security risks associated with business processes are the information assets in the Cloud and the services provided by third parties, which make the identification of information assets a very difficult process (Hariyanti, Djunaidy, and Siahaan 2018).

The ISO 27001 standard does not stipulate the obligation to implement a risk register, but such an approach will allow to comprehensively address the security risks, in which all the data related to the risks, impact, likelihood and controls that are already in place will be systematized implemented to change the risk. This hypothesis has been confirmed by other researchers (Haji, Tan, and Costa 2019) and international best practices (ISACA Germany Chapter, 2017). The risk register can serve in the case of certification as a mandatory document, namely the Risk Assessment Report. The model proposed by me, which can be used for the holistic approach in the risk assessment process is presented in figure 8.

SECURITY RISKS REGISTER											
Department:		Risk Assessment Manager:					Approved by:			Reference No.	
Business process:		Member RA 1:									
BP location:		Member RA 2:					Signature				
Date:		Member RA 3:					Name:				
Version:		Member RA 4:					Position:				
Scheduled review:		Member RA 5:					Date:				
Identifying threats / vulnerabilities				Risk assessment			Risk control				
Asset category	Support assets	Threats / Vulnerabilities	Risk ID	Impact	Likelihood	Risk value	Risk options	Implemented controls	Asset owner	Comments	
Hardware											
Software											
Network and communications											
Personell											
Infrastructure											

Fig 8. Risk Register

A very important document for HEIs, which aims to be certified with ISO 27001, or which want to verify the level of compliance of the security controls implemented with Annex A of the ISO 27001 standard, is the Statement of Applicability, which identifies the applicable controls. A recommended pattern is shown in Figure 9.

Clause Annex A ISO 27001	Anexa A ISO 27001 Control	Control Description	Applicable	Justification	Reference Control	Status
A.5 Information Security Policies						
A.5.1 Management direction for information security	A.5.1.1Policies for Information Security	A set of information security policies must be defined, approved by management, published and communicated to employees and relevant third parties.	Yes	Security policy is required to inform employees / students and third parties about HEI's attitude towards information security	General security policy	Done
	A.5.1.2 Review of the policies for information security	Information security policies need to be reviewed at planned intervals or when changes occur to ensure their continued compliance, compatibility and effectiveness.	Yes	Updating security policy objectives and requirements is necessary due to the dynamic environment specific to university services	Information about the date and person responsible for reviewing the security policy	In process

Fig 9. Statement of Applicability

The final step is to implement the Risk Treatment Plan (RTP). Security controls for risk management, according to ISO 27005, can be taken from any source [37], the only condition is that they align with Annex A of ISO 27001 [4] and the Statement of Applicability of the academic institution. CSCF security checks are recommended to be retrieved from the IT Grundschutz Kompendium, which is a German-German guide, updated annually with recommended technical checks. The proposed model for the Risk Treatment Plan is reflected in Figure 10.

Risk Treatment Plan																
Department:			Responsabil RT:									Approved by:				
Business process:			Member RT 1:													
BP location:			Member RT 2:									Signature				
Date:			Member RT 3:									Name:				
Version:			Member RT 4:									Position:				
Scheduled review:			Member RT 5:									Date:				
Asset category	Support assets	Common Threats / Vulnerabilities	Specific Threats / Vulnerabilities			Security Controls						Compliance with ISO 27001	Comments			
							Implemented			Implemented						
						Basic Controls	Yes	No	Standard Controls	Yes	No					
Hardware																
Software																
Network and Communication																
Personnel																
Infrastructure																

Fig 10. Risk Treatment Plan

An important role is played by the owners of university business processes, in order to identify an effective and real risk-oriented Risk Management Plan, because they know best the business process support assets, which was the basis of the decision to interview HEIs stakeholders.

4.2.5 CSCF project

According to ISO 27003 (ISO&IEC, 2010), which provides clear guidance for implementing the security management system in an organization based on ISO 27001; the whole procedure by which the organization adopts a concept of cybersecurity must be carried out as a project.

The project represents the CSCF plan, which will include the organizational structure of the HEI and the required documentation, which demonstrates the concept's compliance with the reference standard (Asosheh, Hajinazari, and Khodkari 2013).

Once the CSCF has been implemented, it is necessary to regularly monitor all processes in order to ensure the compliance, compatibility and efficiency (ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT 2013) of

security controls. An important role is played by the internal audit, which aims to identify the CSCF's compliance (Cheung 2014) with the organization's requirements for cyber security and with the requirements of the international standard.

The results of the internal audit can be finalized by updating the security controls that have proven to be ineffective or by updating the security policies for those areas that are not covered.

The involvement of university top management in the design and implementation of the concept of cybersecurity is the key to successful IT governance.

5. DISCUSSION

Increasing cybersecurity in Higher Education Institutions by implementing a conceptual framework that represents the synergy between international standards in the field, such as: ISO 27001, ISO 27002, ISO 27005; and best practices developed by the Information Systems Audit and Control Association (ISACA) (ISACA Germany Chapter, 2017), will ensure the success of the implementation and the effectiveness of the security framework focused on the academic processes of HEIs in the Republic of Moldova.

The identification of university business processes, specific to Moldovan universities and the author's recommendations related to the stages of implementation of the conceptual framework, will be an important resource for any Moldovan university that wants to implement a security concept. The resulting CSCF artifact is a practical guide according to which Higher Educational Institutions that have already implemented certain provisions of ISO 27001 will be able to assess their level of compliance, and those institutions that have not yet implemented, will be able to use it as a guide to secure their assets.

6. CONCLUSION

The current trends of HEIs in the Republic of Moldova are to provide quality studies that meet the standards of academic institutions around the world. Thus, in recent years a revolutionary evolution can be attested, through the implementation and use of learning platforms, university management systems or platforms for online examination. Migration from the traditional to the electronic environment has added value to academic processes on the one hand, and on the other hand has significantly increased cyber risks.

Thus, the need to implement a cybersecurity framework that reduces information risks increases over time. This scientific paper identified as a research problem: "the lack of a cybersecurity framework focused on academic processes in HEIs in the Republic of Moldova, which could be used as a reference framework", problem also defined in the Information Security Strategy for 2019-2024 (RM Parliament, 2018), adopted by the Parliament of the Republic of Moldova. So, the aim was to develop a Cyber Security Conceptual Framework, which can be used to implement a security concept.

The DSR scientific method was selected to develop the conceptual framework due to its potential to contribute to encouraging the innovation capacities of organizations, as well as to contribute to the sustainable transformation of society (vom Brocke, Hevner, and Maedche 2020; Watson, Boudreau, and Chen 2010), but especially because the finality of the processes DSR is an artifact that solves a problem in the field. DSR projects must offer both intellectual merit in creative design and extended impact in the field of application through original solutions to the research problem (Hevner et al. 2004; Baskerville et al. 2018). The analysis of the business environment and the derivation of the specific needs to be solved build the starting point of a DSR project.

Based on the above, CSCF was created by analyzing the academic processes of HEIs in the Republic of Moldova, the specific needs, which were identified by empirical study, conducted by a survey completed by HEIs stakeholders and by semi-structured interviews to identify support assets of university business processes.

The selection of the ISO 27001 standard, as a reference standard, is argued by the international importance it demonstrates, but also as a result of the review of scientific articles from the last 10 years. The Bologna Process, implemented by all HEIs in the Republic of Moldova, also recommends the implementation in academic institutions of standardized practices or those with recognized international value.

Identifying the key processes and phases of CSFC implementation in the university environment would increase the cybersecurity of HEIs. Patterns for mandatory documents, according to the ISO 27001 standard, which must be held by the institution, have been proposed.

However, the author does not state the completeness of the proposed framework, and future research directions will focus on the completeness and refinement of the processes of the Cyber Security Conceptual Framework.

The results of the research presented in this paper have significant practical and research contributions.

The practical contribution refers to the Cyber Security Conceptual Framework, oriented on the academic processes of the universities of the Republic of Moldova, in which concrete actions are proposed, focused on the needs of the

researched environment. The practical contribution also solves a national problem, defined in the Information Security Strategy for 2019-2024 of the Republic of Moldova.

Being a pioneer in this field in the Republic of Moldova, I dare to hope that the results of this project will increase the cybersecurity of HEIs in Moldova. With the growth of academic electronic services, the need to implement the concept of security will be growing, and the CSCF artifact will be a valuable guide.

Due to the international standards, used as a reference for the proposed framework, CSCF will be able to be implemented by other academic institutions, outside the country, the academic processes are similar.

There are not many studies in the field of research that reflect how cybersecurity can be enhanced by HEIs, so this paper will add value. The analysis of scientific papers published by researchers in the Republic of Moldova, focusing on the cybersecurity of universities, apart from the articles previously published by the author, showed, that there are no other studies, so important contributions are made to the knowledge base.

7. REFERENCES

1. Ahmed, Naved, and Raimundas Matulevičius. 2014. "Securing Business Processes Using Security Risk-Oriented Patterns." *Computer Standards & Interfaces* 36 (4): 723–33. https://doi.org/10.1016/j.csi.2013.12.007.
2. Alexei, Arina. 2021. "Ensuring Information Security in Public Organizations in The Republic of Moldova through the ISO 27001 Standard." *Journal of Social Sciences* IV (1) (March). https://doi.org/10.52326/jss.utm.2021.4(1).11.
3. Alexei, Arina. 2021. "Network Security Threats to Higher Education Institutions." In *CEE E|Dem and E|Gov Days*, 323–33. Budapest. https://doi.org/10.24989/ocg.v341.24.
4. Alexei, Arina. 2021. "Using Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova." In *The 12th International Conference on Electronics, Communications and Computing*. Chișinău: Technical University of Moldova.
5. Alexei, Arina. 2021. "Cyber Security Strategies for Higher Education Institutions." *Journal of Engineering Science* XXVIII (4): 74–92. https://doi.org/10.52326/jes.utm.2021.28(4).07.
6. Alexei, Arina, and Alexei Anatolie. 2021. "Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning." *International Journal of Scientific & Technology Research* 10 (3).
7. Alexei, Arina, Nistiriuc Pavel, and Alexei Anatolie. 2021. "Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions." In *The 12th International Conference on Electronics, Communications and Computing*. Chișinău: Technical University of Moldova.
8. Angelov, Samuil, Paul Grefen, and Danny Greefhorst. 2012. "A Framework for Analysis and Design of Software Reference Architectures." *Information and Software Technology* 54 (4): 417–31. https://doi.org/10.1016/j.infsof.2011.11.009.
9. Asosheh, Abbass, Parvaneh Hajinazari, and Hourieh Khodkari. 2013. "A Practical Implementation of ISMS." In *7th International Conference on E-Commerce in Developing Countries:With Focus on e-Security*. IEEE. https://doi.org/10.1109/ECDC.2013.6556730.
10. Barbara Kitchenham. 2004. "Procedures for Performing Systematic Reviews." *Eversleigh NSW 1430*, Australia.
11. Baskerville, Richard, Abayomi Baiyere, Shirley Gergor, Alan Hevner, and Matti Rossi. 2018. "Design Science Research Contributions: Finding a Balance between Artifact and Theory." *Journal of the Association for Information Systems* 19 (5). https://doi.org/10.17705/1jais.00495.
12. Brocke, Jan vom, Alan Hevner, and Alexander Maedche. 2020. "Introduction to Design Science Research." In: vom Brocke J., Hevner A., Maedche A. (eds) Design Science Research. Cases. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-030-46781-4_1.
13. Chandra Kruse, Leona, Stefan Seidel, and Jan vom Brocke. 2019. "Design Archaeology: Generating Design Knowledge from Real-World Artifact Design." In: Tulu B., Djamasbi S., Leroy G. (eds) *Extending the Boundaries of Design Science Theory and Practice*. DESRIST 2019. Lecture Notes in Computer Science, vol 11491. Springer, Cham. https://doi.org/10.1007/978-3-030-19504-5_3.
14. Cheung, Simon K. S. 2014. "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

15. Das, Saini, Arunabha Mukhopadhyay, and Bharat Bhasker. 2013. "Today's Action Is Better than Tomorrow's Cure - Evaluating Information Security at a Premier Indian Business School." *Journal of Cases on Information Technology* 15 (3). https://doi.org/10.4018/jcit.2013070101.
16. Disterer, Georg. 2013. "ISO/IEC 27000, 27001 and 27002 for Information Security Management." *Journal of Information Security* 04 (02). https://doi.org/10.4236/jis.2013.42011.
17. Donaldson, Scott E., Stanley G. Siegel, Chris K. Williams, and Abdul Aslam. 2015. "Cybersecurity Frameworks." In *Enterprise Cybersecurity*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4302-6083-7_17.
18. Dresch, Aline, Daniel Pacheco Lacerda, and José Antônio Valle Antunes Jr. 2015. *Design Science Research*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-07374-3.
19. Esparza, Daisy Elizabeth Imbaquingo, Francisco Javier Diaz, Tatyana Katherine Saltos Echeverria, Silvia Rosario Arciniega Hidrobo, Diego Andres Leon Villavicencio, and Adrian Robayo Ordonez. 2020. "Information Security Issues in Educational Institutions." In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE. https://doi.org/10.23919/CISTI49556.2020.9141014.
20. Flowerday, Stephen v., and Tite Tuyikeze. 2016. "Information Security Policy Development and Implementation: The What, How and Who." *Computers & Security* 61 (August). https://doi.org/10.1016/j.cose.2016.06.002.
21. Gërvalla, Muhamet, Naim Preniqi, and Peter Kopacek. 2018. "IT Infrastructure Library (ITIL) Framework Approach to IT Governance." In *IFAC-PapersOnLine*, 51:181–85. Elsevier B.V. https://doi.org/10.1016/j.ifacol.2018.11.283.
22. Ghazvini, Arash, Zarina Shukur, and Zaihosnita Hood. 2018. "Review of Information Security Policy Based on Content Coverage and Online Presentation in Higher Education." *International Journal of Advanced Computer Science and Applications* 9 (8). https://doi.org/10.14569/IJACSA.2018.090853.
23. Haji, Sami, Qing Tan, and Rebeca Soler Costa. 2019. "A Hybrid Model for Information Security Risk Assessment." *International Journal of Advanced Trends in Computer Science and Engineering*, February, 100–106. https://doi.org/10.30534/ijatcse/2019/1981.12019.
24. Hariyanti, Eva, Arif Djunaidy, and Daniel Oranova Siahaan. 2018. "A Conceptual Model for Information Security Risk Considering Business Process Perspective." In *2018 4th International Conference on Science and Technology (ICST)*. IEEE. https://doi.org/10.1109/ICSTC.2018.8528678.
25. Harkins, Malcolm W. 2016. *Managing Risk and Information Security*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-1455-8.
26. Haufe, Knut, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis, and Vladimir Stantchev. 2016. "ISMS Core Processes: A Study." *Procedia Computer Science* 100 (January): 339–46. https://doi.org/10.1016/J.PROCS.2016.09.167.
27. Hevner, March, Park, and Ram. 2004. "Design Science in Information Systems Research." *MIS Quarterly* 28 (1). https://doi.org/10.2307/25148625.
28. Hommel, Wolfgang, Stefan Metzger, and Michael Steinke. 2015. "Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization." *EUNIS Journal of Higher Education IT*.
29. Humayun, Mamoona, Mahmood Niazi, NZ Jhanjhi, Mohammad Alshayeb, and Sajjad Mahmood. 2020. "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study." *Arabian Journal for Science and Engineering* 45 (4). https://doi.org/10.1007/s13369-019-04319-2.
30. ISO/IEC 27003: Information technology — Security techniques — Information security management systems — Guidance. 2017. "International Organization for Standardization." Geneva. https://www.iso.org/standard/63417.html.
31. ISACA Germany Chapter e.V. Oberwallstr. 24 10117 Berlin, Germany. 2017. "Implementation Guideline ISO/IEC 27001:2013." Berlin.
32. ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security controls. 2013. "International Organization for Standardization." *Switzerland*.
33. ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. 2013. "International Organization for Standardization." Geneva, Switzerland. https://www.iso.org/isoiec-27001-information-security.html.
34. ISO/IEC 27005: Information technology — Security techniques — Information security risk management. 2018. "International Organization for Standardization." Geneva, Switzerland.

35. ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2018. "International Organization for Standardization." Geneva, Switzerland. 2018. https://www.iso.org/standard/73906.html.
36. Itradat, Awni, Sari; Sultan, Maram; Al-Junaidi, Rawa'a; Qaffaf, Feda'a; Mashal, and Fatima Daas. 2014. "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study." *Jordan Journal of Mechanical & Industrial Engineering* 8 (2): 102–18.
37. Ivanov V., Tzaneva M., Murdjeva A., Kisimov V. 2011. "Securing the Core University Business Processes." In: Camenisch J., Kisimov V., Dubovitskaya M. (eds) Open Research Problems in Network Security. iNetSec 2010. Lecture Notes in Computer Science, vol 6555. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19228-9_9
38. Jakoubi, Stefan, Simon Tjoa, Sigrun Goluch, and Gerhard Kitzler. 2010. "Risk-Aware Business Process Management—Establishing the Link Between Business and Security." In: Xhafa F., Barolli L., Papajorgji P. (eds) Complex Intelligent Systems and Their Applications. Springer Optimization and Its Applications, vol 41. Springer, New York, NY. https://doi.org/10.1007/978-1-4419-1636-5_6.
39. Jang-Jaccard, Julian, and Surya Nepal. 2014. "A Survey of Emerging Threats in Cybersecurity." In *Journal of Computer and System Sciences*, 80:973–93. Academic Press Inc. https://doi.org/10.1016/j.jcss.2014.02.005.
40. Joshi, Chanchala, and Umesh Kumar Singh. 2017. "Information Security Risks Management Framework – A Step towards Mitigating Security Risks in University Network." *Journal of Information Security and Applications* 35 (August). https://doi.org/10.1016/j.jisa.2017.06.006.
41. Khanmohammadi, Kobra, and Siv Hilde Houmb. 2010. "Business Process-Based Information Security Risk Assessment." In *2010 Fourth International Conference on Network and System Security*, 199–206. IEEE. https://doi.org/10.1109/NSS.2010.37.
42. Khther, Rasha Adnan, and Marini Othman. 2013. "Cobit Framework as a Guideline of Effective It Governance in Higher Education: A Review." *International Journal of Information Technology Convergence and Services* 3 (1). https://doi.org/10.5121/ijitcs.2013.3102.
43. Koong, K., and M Yunis. 2015. "Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework." In *AMCIS 2015 Proceedings*.
44. MacCuspie, Robert I., Harvey Hyman, Chris Yakymyshyn, Sesha S. Srinivasan, Jaspreet Dhau, and Christina Drake. 2014. "A Framework for Identifying Performance Targets for Sustainable Nanomaterials." *Sustainable Materials and Technologies* 1–2 (December): 17–25. https://doi.org/10.1016/J.SUSMAT.2014.11.003.
45. Merchan-Lima, Jorge, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca, and Dorys Quiroz. 2020. "Information Security Management Frameworks and Strategies in Higher Education Institutions: A Systematic Review." *Annals of Telecommunications*, July. https://doi.org/10.1007/s12243-020-00783-2.
46. Myers, Michael D., and Michael Newman. 2007. "The Qualitative Interview in IS Research: Examining the Craft." *Information and Organization* 17 (1). https://doi.org/10.1016/j.infoandorg.2006.11.001.
47. Nowak, G. J. 2015. "Information Security Management with Accordance to ISO27000 Standards: Characteristics, Implementations, Benefits in Global Supply Chains." In *Logistyka*, 639–54.
48. Oltramari, Alessandro, Noam Ben-Asher, Lorrie Cranor, Lujo Bauer, and Nicolas Christin. 2014. "General Requirements of a Hybrid-Modeling Framework for Cyber Security." In *2014 IEEE Military Communications Conference*. IEEE. https://doi.org/10.1109/MILCOM.2014.28.
49. Pääkkönen, Pekka, and Daniel Pakkala. 2015. "Reference Architecture and Classification of Technologies, Products and Services for Big Data Systems." *Big Data Research* 2 (4): 166–86. https://doi.org/10.1016/J.BDR.2015.01.001.
50. Parlamentul RM. 2018. "Strategia Securității Informaționale a RM Pentru Perioada 2019-2024." November 22, 2018. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fgov.md%2Fsites%2Fdefault%2Ffiles%2Fdocument%2Fattachments%2Fintr23_86.pdf.
51. Peffers, Ken, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. 2007. "A Design Science Research Methodology for Information Systems Research." *Journal of Management Information Systems* 24 (3). https://doi.org/10.2753/MIS0742-1222240302.

52. Rehman, Huma, Ashraf Masood, and Ahmad Raza Cheema. 2013. "Information Security Management in Academic Institutes of Pakistan." In *2013 2nd National Conference on Information Assurance (NCIA)*. IEEE. https://doi.org/10.1109/NCIA.2013.6725323.
53. Rojas, Oscar González, and Sebastián Lesmes. 2016. "Value at Risk Within Business Processes: An Automated IT Risk Governance Approach." In *BPM*.
54. Singh Umesh Kumar, and Joshi C. 2016. "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*. San Francisco.
55. Solms, Basie von, and Rossouw von Solms. 2018. "Cybersecurity and Information Security – What Goes Where?" *Information & Computer Security* 26 (1). https://doi.org/10.1108/ICS-04-2017-0025.
56. Suroso, Jarot S., and Muhammad A. Fakhrozi. 2018. "Assessment of Information System Risk Management with Octave Allegro at Education Institution." *Procedia Computer Science* 135. https://doi.org/10.1016/j.procs.2018.08.167.
57. Suwito, Misni Harjo, Shinchi Matsumoto, Junpei Kawamoto, Dieter Gollmann, and Kouichi Sakurai. 2016. "An Analysis of IT Assessment Security Maturity in Higher Education Institution." In: Kim K., Joukov N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, vol 376. Springer, Singapore. https://doi.org/10.1007/978-981-10-0557-2_69.
58. Szczepaniuk, Edyta Karolina, Hubert Szczepaniuk, Tomasz Rokicki, and Bogdan Klepacki. 2020. "Information Security Assessment in Public Administration." *Computers and Security* 90 (March): 101709. https://doi.org/10.1016/j.cose.2019.101709.
59. Ulven, Joachim Bjørge, and Gaute Wangen. 2021. "A Systematic Review of Cybersecurity Risks in Higher Education." *Future Internet* 13 (2): 39. https://doi.org/10.3390/fi13020039.
60. Wangen, Gaute, Christoffer Hallstensen, and Einar Snekkenes. 2018. "A Framework for Estimating Information Security Risk Assessment Method Completeness." *International Journal of Information Security* 17 (6). https://doi.org/10.1007/s10207-017-0382-0.
61. Watson, Boudreau, and Chen. 2010. "Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community." *MIS Quarterly* 34 (1). https://doi.org/10.2307/20721413.
62. Wolden, Mark, Raul Valverde, and Malleswara Talla. 2015. "The Effectiveness of COBIT 5 Information Security Framework for Reducing Cyber Attacks on Supply Chain Management System." In *IFAC-PapersOnLine*, 28:1846–52. Elsevier. https://doi.org/10.1016/j.ifacol.2015.06.355.
63. Yustanti, W, A Qoiriah, R Bisma, and A Prihanto. 2018. "An Analysis of Indonesia's Information Security Index: A Case Study in a Public University." *IOP Conference Series: Materials Science and Engineering* 296 (January). https://doi.org/10.1088/1757-899X/296/1/012038.