INFORMATION AND WEB TECHNOLOGIES

DOI 10.51582/interconf.7-8.06.2021.036

Alexei Arina
PhD student, lecturer, Department of Telecommunications and Electronic Systems,
Technical University of Moldova, Republic of Moldova

Nistiriuc Pavel
Associate professor, Department of Telecommunications and Electronic Systems,
Technical University of Moldova, Republic of Moldova

Alexei Anatolie
PhD student, lecturer, Department of Telecommunications and Electronic Systems,
Technical University of Moldova, Republic of Moldova

ANALYSIS OF SECURITY FRAMEWORKS IMPLEMENTED IN HEI's

Abstract*. With the increasing use of new information technologies in the activity of HEIs, the need to protect information has emerged. Information security addresses several issues, not just IT. Therefore, in the meantime, it has become mandatory to implement security frameworks that address cyber security as a complex process. Internationally, there are several standardized security frameworks, such as: ISO27001, NIST, COBIT, ITIL, PCI DSS. The purpose of this scientific article was to use grounded-theory method to review scientific journal publications and conference proceedings to identify those security frameworks that are recommended by researchers.*

Keywords*: cyber security, HEIs, security framework, information*.

Introduction

Information security in HEIs (Higher Education Institutions) has been increasingly affected in recent years [1]–[3]. Thus, the latest reports prepared by large companies in the field, such as: Microsoft, Kaspersky [4], Barracuda Networks [5], IBM & Ponemon Institute [6], attest to a considerable increase in cyber threats

to university networks. Analyzing the data of the security reports, it can be stated that the biggest threats to the cyber security of the university networks are: malicious programs, DoS/DDoS attacks and phishing attacks [7]. Due to the fact that university networks are designed to offer a wide range of services, simultaneously for different groups of users, such as: students, staff, partners or outsiders, the vulnerabilities to which they are exposed, increase depending on the volume and quality of information which it manages [8]. As confirmation, serves growing interest of hackers for HEIs who in 2020, conducted research to identify a vaccine against Covid-19, so that European supercomputers working on Covid-19 research in the spring of 2020, and the affected academic institutions were forced to temporarily take their systems offline. Data centres in the UK, Spain, Germany and Switzerland have confirmed the intrusions. The University of California San Francisco (UCSF), in June 2020, paid $ 1.14 million in Bitcoin to recover data from their medical school.

HEIs manage with data of big interest for cyber attackers, such as:

– Intellectual property, especially in academic institutions conducting various health research, such as those that, in 2020, conducted extensive studies to identify a Covid-19 vaccine.

– Personal data of students, which include various educational materials and results of examination sessions, but also the identification code or records of bank accounts.

According to the report by IBM & Ponemon Institute [6], the main types of compromised registrations in 2020 are personal information (80%), which averaged a loss of $ 150 per record and intellectual property (32%) with a loss of $ 147 per record. If we analyse the percentage change in the average total cost for compromised data, in Europe, the Scandinavian countries recorded the highest increase (12.8%) in 2020 compared to 2019, followed by the United Kingdom (4.4%). Negative trends are recorded in Germany (-4.7%) and France (-5.2%).

All of the above were to demonstrate how affected HEIs are by cyber-attacks and to emphasize the need to implement an information security management system (ISMS), that would focus on increasing cyber security in HEIs.

Thus, in the following sections, an analysis of scientific articles will be performed, indexed by such databases as: Scopus, ScienceDirect, ACM Digital Library, IEEE and Springer, which recommend a security model that can be implemented in HEIs, to increase cyber security.

1. Literature review

For literature review, will be used grounded-theory method recommended by Joost F. Wolfswinkel, Elfi Furtmueller and Celeste P.M. Wilderom [9]. The authors state that: "... this method is designed as a guide to help systematize the review process for a more optimal outcome that contributes to theoretical progress". The method recommends five steps for a rigorous literature review: define, search, select, analyse and present.

It needs to define, at first, a research questions, in this case the research question is:" What kind of security frameworks are recommended to improving cyber security in HEIs?"

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; based on the keywords set out in Table 1.

Table 1

Keywords

No	Keywords
1	[Information Security] or [Information Security Management System] or [Cyber Security] 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 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

Thus, as a result of the search, 30 scientific articles were selected from the previously announced databases. The selected items meet the inclusion criteria.

Table 2

Search results

Source	**Applied filters**	**Notes**	**Nr. of selected articles**
ScienceDirect	Title, Abstract, Keywords	Abstract and citation database of peer-reviewed literature	9
Scopus	Title, Abstract, Keywords	Abstract and citation database of peer-reviewed literature	7
IEEE Xplore	Title, Abstract, Keywords	Abstract and citation database of peer-reviewed literature	6
ACM Digital Library	Title, Abstract, Keywords	Abstract and citation database of peer-reviewed literature	2
Springer	Title, Abstract, Keywords	Abstract and citation database of peer-reviewed literature	6

To answer the research question, analyzing the results obtained, it can be concluded that the standardized security frameworks recommended by researchers are: ISO27001, COBIT and ITIL or their combination.

The following section will describe the recommended security frameworks, from the perspective of implementation in HEIs.

2. Discussion

Out of 30 scientific articles relevant to cyber security in HEIs, 5 researchers recommend the use of ISO27001, 2 scientific articles recommend COBIT, ITIL is recommended as a cyber security framework by one article and another article recommends the hybrid version, which combines the 3 standards. Otherwise, most researchers recommend their own strategies or do not analyse any framework for increasing cyber security in HEIs.

Table 3

Recommended security frameworks

Criterion	Framework	Scientific Paper	%
Security framework/standard for Information Security Management	ISO 27001	5	16,67
	COBIT	2	3,33
	ITIL	1	3,33
	Hybrid	1	3,33
	Not including	7	26,67
	Own framework	14	46,67

3. Analysis of security frameworks

3.1 ISO27001

The ISO27001 standard is the most widely used standard for ensuring information security, at international level [10]–[12]. According to annual reports submitted by ISO, in education, there is a steady increase in the number of institutions certified to ISO 27001, so that in 2018 internationally certified were 137 institutions and in 2019, 176 certified institutions [13]. Most ISO27001 certified institutions are in Japan (26), Greece (30), Italy (11), Poland (12), the Czech Republic (11).

The ISO27001 standard involves the creation of an information security management system (SMSI) within institutions. For the implementation of SMSI, ISO27001, uses the PDCA model (Planning, Implementation, Verification, Action) [14], reflected in figure 1.

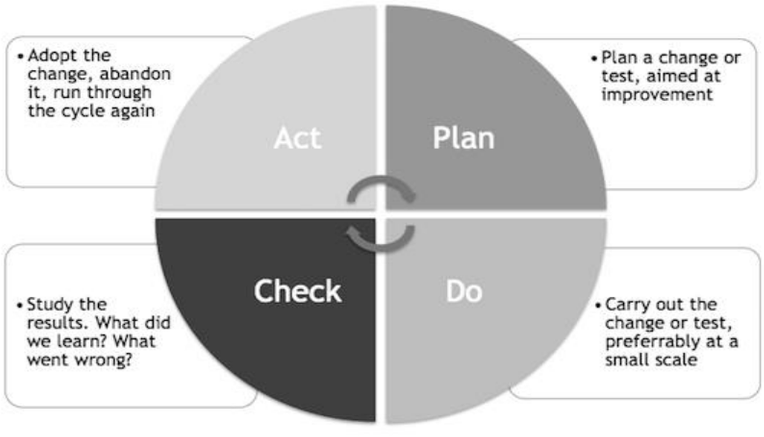

Fig. 1. **Plan-Do-Check-Act**

Protection of corporate assets is achieved by implementing ISMS, which is based on security risk assessment and based on CIA triad [11], [12], [15]–[17]. The CIA triad includes: confidentiality of information, integrity of information and availability of services [17]. As information security is not just about IT, the ISO27001 standard also contains specific controls for human resource management, legal constraints and organizational management [11]. This is also due to the fact that cyber security depends more on the human factor than on the technology used [12], and the security threats coming from the employees of an organization are far superior to external threats [12].

The ISO27001 standard is organized into 14 sections, 35 objectives and 114 security controls [11]. 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 [1], [18]. Not all sections of the standard are applicable in HEIs, as the ISO27001 standard is aimed at non-academic and commercial organizations [10].

Namely due to the generality of ISO27001 standard, it is difficult to identify specific targeted strategy for HEIs, so empirical research could elucidate new variables not listed by standards.

3.2 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 [19]. COBIT focuses on generating a structured set of principles, such as organizational requirements, IT resources, IT processes and the provision of information [19]. 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 [20].

COBIT is focused on risk management, as is ISO27001, 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 [21].

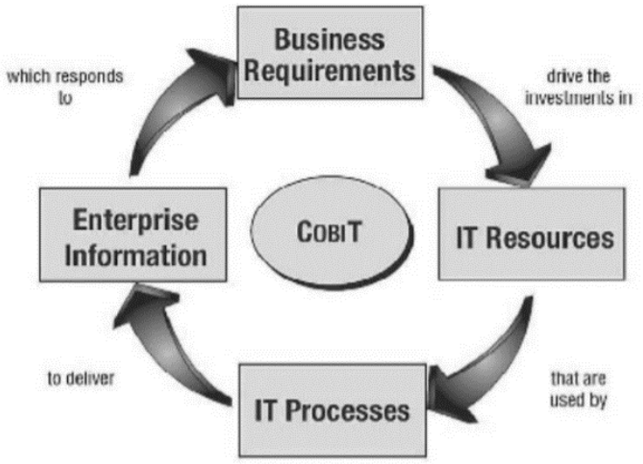

Fig. 2. **COBIT framework principle** [19]

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 [19]. COBIT includes 34 IT processes and 13 control objectives. Each process contains a RACI diagram [19], 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 ISO27001 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 [16] and to evaluate IT processes [19].

3.3 ITIL

The ITIL standard is an association between different practices and information technology services for better management of IT services [20]. 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 [22].

Fig. 3. **ITIL Framework** [22]

The service design phase includes 8 processes: design, coordination, service catalog management, service management, provider management, IT service continuity, information security management, availability management and capacity management [23]. At this stage, it is ensured that all IT units can provide quality services, meet all the requirements of the company by aligning IT and business needs, improving IT governance, improving service quality, improving coherence between IT units and easier implementation of new services. There are five key aspects of the design service [24]:

1. Designing each IT service offered;

2. Design of service management systems and tools;

3. IT design of architecture and management system;

4. Designing the necessary processes for the installation, operation and improvement of IT services;

5. Design of measurement and metric methods.

The operation of the service helps to control and manage the risk of IT services by using contingency plans for risk management. It ensures compliance with the requirements of the institution and includes 7 processes: change management, implementation management, service validation and testing, change evaluation,

service assets and configuration management, knowledge management and transition, planning and assistance [22], [24]. This phase contributes to the management of changes in IT systems and aims primarily to minimize the impact of changes in the quality of service delivery [24].

The last phase contributes to the everyday functioning of managing IT services. It includes 5 processes: event management, incident management, problem management and task accomplishment [21], [22]. At this stage, the performance of the implemented services is performed and calculated. The service operation stage can also be divided into the following categories [24]: service operation, incident management and problem management service [22], [24].

As in the case of COBIT, it is recommended to use the ITIL standard combined with the ISO27001 standard, to integrate the security practices recommended by ISO27001 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 [20].

3.4 Hybrid strategy

The hybrid strategy is supported by several studies [20], [25], as standards evolve, the alignment of ITIL, COBIT and ISO27001 standards, allows the implementation of a more comprehensive information security management system. The researchers agreed that ITIL, COBIT and ISO27001 are the most popular standards that can be merged and adapted to the requirements of the organization [26]. ISO27001 focuses on information security management, while ITIL and COBIT focus on information security and the relationship between project management and IT Governance [23]. One of the arguments used to combine the announced standards is that in order to provide IT services, monitoring is the key process. Thus, it is recommended to use COBIT, at the highest level, by establishing a general control framework that is based on IT processes, applicable to any type of organization. By associating [20] the processes recommended by ITIL with the ISO27001 controls and the general COBIT framework, specific practices covering certain dedicated areas can be defined, the recommended association can be seen in Table 4.

Table 4

Combining security standards

COBIT 4.1	**ITIL V3**	**ISO27001**
Service support DSS02 Service and incident demand management AP011 Quality management	Service Office	6.3.2 Reporting security vulnerabilities
DSS02 Problem and Incident Management	Incident Management	13.2.1 Establishing Liability for Incidents and Procedures
DSS04 Problem management	Problem management	13.2.1 Establish responsibility in case of incidents and procedures
BAI010 Configuration management	Configuration management	
BAI106 Change management	Change management	10.5.1 Modification of control procedures 8.2.1 Control of operational changes
BAI106 Change Management	Launch Management	10.4.1 Operational Software Control 10.5.2 Technical review of operating system changes
Service delivery APO09 Management of service agreements	Service level agreements	4.2.2 Security requirements for third parties 10.2.1 Management of agreements for services provided by third parties
APO006 Budget and cost management	Financial management	
DSS04 Continuity Management	Continuity Management	14 Business Continuity Management
BAI04 Availability and capacity management	Capacity management	8.2.1 Capacity planning
BAI04 Availability and capacity management	Availability management	8.5.1 Network control 9.5.5 Use of system utilities

Although it would seem that these 3 standards contain identical instructions, the implementation requirements are different, which drastically affects the implementation process, especially the budget. Therefore, before using any of the listed standards, it is necessary to clarify the implementation costs, which are usually limited within the HEI.

ISO27001 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, ISO27001 is like English, has a proven international value.

Conclusions

Own security models are recommended for implementation in HEIs, in 46% of the scientific papers analyzed, because they can be performed in strict accordance with institutional requirements and modeled in dependence of the budget. International security standards, such as ISO27001, COBIT or ITIL, are aimed at non-academic organizations and do not contain specific HEI recommendations, and as a result are more difficult to implement. Certification costs are also high and HEI budgets are limited. However, when developing the security model for HEIs, it is advisable to take into account the controls proposed by international standards, as they have excellent controls, which have proven effective over time and are internationally appreciated.

References:

1. D. E. I. Esparza, F. J. Diaz, T. K. S. Echeverria, S. R. A. Hidrobo, D. A. L. Villavicencio, and A. R. Ordonez, “Information security issues in educational institutions,” Jun. 2020, doi: 10.23919/CISTI49556.2020.9141014.
2. E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, “Information security assessment in public administration,” *Computers and Security*, vol. 90, p. 101709, Mar. 2020, doi: 10.1016/j.cose.2019.101709.
3. N. Mumtaz, “Analysis of information security through asset management in academic institutes of Pakistan,” Dec. 2015, doi: 10.1109/ICICT.2015.7469581.
4. Kaspersky, “Education Report,” 2020. Accessed: Dec. 09, 2020. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_04092020_2.pdf.
5. Barracuda, “Threat Spotlight Spear Phishing Education,” 2020. Accessed: Dec. 12, 2020. [Online]. Available: https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5-2020L.pdf?mkt_tok=eyJpIjoiTVdNellXVmlOREExTURoaSIsInQiOiJJM1ErR0FRaHFsc2YyU2dMdEhmUVFSVW1XYkxBYzB3T1JqSzgrZlVZZ25paGx4c25sRWN0S0pWSW5wa3RqTEFMRm83cFJmazlcL2dhK3FHZFZWMVQyXC9KOVpzVjdXb3VEMWlUVXg0blp2cjFaend1NGRZaU5VZkNsK2NhaDhzUFFIIn0%3D.
6. Ponemon Institute, “Cost of a Data Breach Report,” 2020. Accessed: Dec. 01, 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

7. A. Alexei, “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.
8. C. Joshi and U. K. Singh, “Information security risks management framework – A step towards mitigating security risks in university network,” *Journal of Information Security and Applications*, vol. 35, Aug. 2017, doi: 10.1016/j.jisa.2017.06.006.
9. J. F. Wolfswinkel, E. Furtmueller, and C. P. M. Wilderom, “Using grounded theory as a method for rigorously reviewing literature,” *European Journal of Information Systems*, vol. 22, no. 1, Jan. 2013, doi: 10.1057/ejis.2011.51.
10. H. Rehman, A. Masood, and A. R. Cheema, “Information Security Management in academic institutes of Pakistan,” Dec. 2013, doi: 10.1109/NCIA.2013.6725323.
11. A. Alexei, “ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE REPUBLIC OF MOLDOVA THROUGH THE ISO 27001 STANDARD,” *Journal of Social Sciences*, vol. IV(1), Mar. 2021, doi: 10.52326/jss.utm.2021.4(1).11.
12. A. Itradat, S. Sultan, M. Al-Junaidi, R. Qaffaf, F. Mashal, and F. Daas, “Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study,” *Jordan Journal of Mechanical & Industrial Engineering*, vol. 8, no. 2, pp. 102–118, 2014.
13. Alexei Arina and Alexei Anatolie, “Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning,” *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 10, no. 3, Mar. 2021.
14. F. STEFAN, G. GERNOT, E. ANDREAS, R. BERNHARD, and W. EDGAR, “Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard,” in *13th Pacific Rim International Symposium on Dependable Computing* , 2007, pp. 381–388.
15. A. Asosheh, P. Hajinazari, and H. Khodkari, “A practical implementation of ISMS,” Apr. 2013, doi: 10.1109/ECDC.2013.6556730.
16. W. Yustanti, A. Qoiriah, R. Bisma, and A. Prihanto, “An analysis of Indonesia’s information security index: a case study in a public university,” *IOP Conference Series: Materials Science and Engineering*, vol. 296, Jan. 2018, doi: 10.1088/1757-899X/296/1/012038.
17. G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” *Journal of Information Security*, vol. 04, no. 02, 2013, doi: 10.4236/jis.2013.42011.
18. S. K. S. Cheung, “Information Security Management for Higher Education Institutions,” 2014.
19. R. A. Khther and M. Othman, “Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review,” *International Journal of Information Technology Convergence and Services*, vol. 3, no. 1, Feb. 2013, doi: 10.5121/ijitcs.2013.3102.

20. M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann, and K. Sakurai, “An Analysis of IT Assessment Security Maturity in Higher Education Institution,” 2016.
21. M. Wolden, R. Valverde, and M. Talla, “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.
22. M. Gërvalla, N. Preniqi, and P. Kopacek, “IT infrastructure library (ITIL) framework approach to IT governance,” in *IFAC-PapersOnLine*, Oct. 2018, vol. 51, no. 30, pp. 181–185, doi: 10.1016/j.ifacol.2018.11.283.
23. Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan, “Information Security Management System Standards: A Comparative Study of the Big Five,” *International Journal of Electrical & Computer Sciences IJECS-IJENS*, 2011.
24. R. R. Moeller, *Executive’s Guide to IT Governance*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2013.
25. S. Haji, Q. Tan, and R. S. Costa, “A Hybrid Model for Information Security Risk Assessment,” *International Journal of Advanced Trends in Computer Science and Engineering*, Feb. 2019, doi: 10.30534/ijatcse/2019/1981.12019.
26. R. Almeida, R. Lourinho, M. Mira da Silva, and R. Pereira, “A Model for Assessing COBIT 5 and ISO 27001 Simultaneously,” Jul. 2018, doi: 10.1109/CBI.2018.00016.