TEM Journal. Volume 11, Issue 3, pages 1093-1102, ISSN 2217-8309, DOI: 10.18421/TEM113-14, August 2022.

Digitalization of Educational Services with Regard to Policy for Information Security

Pavel Petrov [1], Ivan Kuyumdzhiev [1], Rami Malkawi [2],
Georgi Dimitrov [3], Jordan Jordanov [1]

[1] University of Economics - Varna, Varna, Bulgaria
[2] Yarmouk University, Irbid, Jordan
[3] University of Library Studies and Information Technologies, Sofia, Bulgaria

***Abstract* – Faced with the widespread digitalization in educational services, every educational organization has to strive to meet modern-day quality and security standards for both information and other assets. The education organizations should invest in a methodology that identifies system flaws and, as a result, opportunities for improvement. To protect the educational organization's information assets from internal, external, intentional, or unintentional threats, an "Information Security Policy" should be developed. Effective data management necessitates not only the identification of data requirements but also security issues. Educators and students should be subject to policies that define and impose conditions in a variety of sensitive areas.**

***Keywords* – education organizations, information security policy, data management.**

1. Introduction

The digitalization of educational services, as well as the growing number of educational services available through the Internet, increases the role and importance of information systems.

With this regard educational organizations have a need of a methodology that identifies system flaws and, as a result, opportunities to improve their effectiveness. As a result of these trends, there has been a growing interest in developing information security policies in recent years. This is due to various of factors, together with regulations requiring internal rules for information system management, as well as a positive shift in the thinking of educational leadership [14], [16], [18] and the recognition that one of the key accompanying activities, such as the use of digitalization, necessarily requires professional management and reliable control [11], [12]. Several stages have to be completed before a policy can be successfully implemented in educational institutions. In the beginning, an observation is required to assess the state of information security and its adequacy to the requirements set by educational services. At this point, an analysis of the following information is needed:

- The educational organization's structure;
- The information technology used to collect, process, transmit, and store data;
- Key educational processes and their reliance on technology;
- The normative and organizational documents, as well as their conformity with other policies.

After analyzing the results, it is necessary to form a working group in charge of developing the policy and clearly defining the boundaries of the digitalization process. It should be noted that expanding the scope of digitization and incorporating more educational processes significantly increases project's complexity and reduces chances of its successful completion.

In the final stage of the analysis, an "Information Security Policy" has to be developed to protect the educational organization's information assets from internal, external, intentional, or unintentional threats by ensuring:

DOI: 10.18421/TEM113-14
https://doi.org/10.18421/TEM113-14

Corresponding author: Pavel Petrov,
University of Economics - Varna, Varna, Bulgaria.
Email: petrov@ue-varna.bg

Received: 04 June 2022.
Revised: 21 July 2022.
Accepted: 29 July 2022.
Published: 29 August 2022.

- information confidentiality;
- information's integrity;
- ease of access to information concerning work processes;
- adherence to legislative and regulatory requirements;
- creation, maintenance, and testing of plans for educational service continuity;
- all employees have to be trained on the digitalization requirements;
- reporting and thorough investigation of information security incidents that have been identified or are suspected;
- keeping a manual, procedures, and instructions in line with digitalization goals.

Information security policies should be consistent with other existing policies in the organization (e.g., those related to human resources, accounting, labor protection, and so on) and disseminated to anyone who has access to the organization's information system, whether they are employees or outsiders. Everyone who is subjected to the information security policy has to be aware of the consequences of breaking it.

The policy should be reviewed on a regular basis, either in the event of changes in the IT infrastructure or in response to a change in a pre-defined process, and, if necessary, changed, in order to maintain its relevance and effectiveness. This, in our opinion, necessitates the automation of processes for analyzing existing IT infrastructure and disseminating new rules to the organization's employees. Slowing or ignoring any of these processes renders imposed policies ineffective, if not harmful. Developing new services and installing new software and hardware, for example, is frequently done without the necessary analysis and evaluation. This, in turn, leads to an unintentional increase in risk due to noncompliance with the imposed rules. Another common issue is the adoption of policies and standards that are not communicated to employees. In this case, they are only desirable and thus ineffective.

The following generally accepted principles have to be considered:

1. Information security is a process, not a state, with a beginning but no end. Control over this process is lost if certain rules are not followed.
2. The analysis of the organization's security policy as a subject and an important part of the monitoring of information systems demonstrates that it is necessary and possible to develop an automated information system that supports the stages of the information security lifecycle and end-user access to information. This would aid in the conduct of quality monitoring and, as a result, the organization's information security system.
3. Organizational policy requirements are supported by rules. They are intended to define methods of operation for achieving the organization's objectives. Large educational organizations with significant resources can create and enforce their own peer-reviewed standards. Medium and small educational organizations, on the other hand, lack the necessary potential. Many organizations, however, do not, but standards for the system development process, software configuration, data structures, applied control mechanisms, and supported documentation have to be adopted.

2. Policy for Data Management and Data Processing

Identification of data requirements is necessary for effective data management. The establishment of effective procedures for the management of the infrastructure [17], [21], [28] for their storage, the creation of archives and their restoration, if necessary, as well as the appropriate destruction of data carriers are all part of the data management process. In a broader sense, data management encompasses database management, modeling, development, implementation, and use; metadata management in the organization - related to users, standards, integration, and the creation of queries and reports; and database management, modeling, development, implementation, and use. Data quality management is an important part of the overall process. It manifests itself in the creation of data quality specifications, quality analysis, and quality improvement proposals. As part of data management, data security management and electronic document management can be mentioned.

2.1. Quality of Data Management and Organizational Maturity

There are several methods for evaluating the quality of data management that has been achieved. The percentage of user satisfaction with data availability and the rate of successful disaster recovery can be used to assess data management. To increase this share, a policy for archiving, restoration, and maintenance of media containing archival copies should be established. The number of incidents in which personal data was leaked after the destruction of the media containing it is also critical, as this can result in significant losses for the organization.

The fulfillment of the aforementioned conditions provides justification for assessing the level of maturity of the data management system in accordance with the COBIT Maturity Model [8], [24], [25] as:

- non-existent data management system;
- the initial state;
- natural;
- clarified;
- controllable and evaluable;
- improved.

Data is not considered an asset and a vital resource in some small or relatively new and inexperienced organizations. In this regard, there is no standardized system for data ownership and management responsibilities. Data quality and security are extremely low or non-existent in these cases.

When an organization recognizes the need for data management (for example, when changing management, enforcing regulations, or a series of incidents related to poor data management), data security requirements are developed but not formalized and disseminated to employees. Data archiving procedures are carried out on a regular basis, and precautions are taken to ensure their safe destruction. There is no clear division of responsibilities for data management and staff training in this initial state.

Organizations at the third level of maturity have recognized the need for effective data management and are developing a high-level data ownership system. Data security requirements are documented in such organizations, and key activities such as data archiving, recovery, and destruction are monitored. Typically, key IT staff are assigned responsibilities related to the data management process [15], [23].

When the need for data management is understood and accepted throughout the organization, it is considered defined. Data management responsibilities have been defined, and ownership has been transferred to a group in charge of integrity and security. Data management procedures have been formalized, and tools for archiving, restoring, and destroying data have been implemented. There are also practices for staff training, data management monitoring, and the use of basic metrics in such organizations. Ownership and management of information responsibilities are clearly defined, distributed, and disseminated across the organization. To carry out the procedures, modern tools are beginning to be used. The indicators for meeting goals and achieving good performance are defined in collaboration with students and monitored using a well-defined process. Data management training is provided on a formal basis.

The highest level of organizational maturity in terms of data management policy includes organizations that have understood and accepted the need for all necessary measures to achieve quality data management. Future requirements and needs have been investigated. Responsibilities for data ownership and management are clearly defined, widely distributed throughout the organization, and regularly updated. Procedures have been formalized and sharing experiences has become commonplace. For maximum automation of the management process, advanced tools and instruments are used. Indicators of objectives and their implementation are created with the assistance of students and are fully monitored through a well-defined process. Opportunities for advancement are constantly being sought. There are now training programs in place for data management personnel.

Most organizations are between the third and fourth levels of maturity, which means they recognize the importance of data management across the organization but lack established methods for training and involving every employee in the concept of corporate data management. As a result, while some employees recognize the importance of adhering to established policies and are willing to do so, they lack a precise and clear understanding of how to do so. On the other hand, there is a subset of employees who are aware of the issue but lack the motivation, desire, or knowledge to carry out the procedures prescribed by operational management. As a result, there is a clear need for a software solution to meet the needs of the organization's data management process. Among these are:

- Quick and clear division of responsibilities;
- Providing instruction;
- Look for areas for improvement.

2.2. Processing Integrity and the Involved Risks

According to the American Institute of Certified Public Accountants (AICPA) [1] processing integrity exists when "system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives". The following should be considered in this regard:

- Completion typically means that all transactions and services have been processed or completed without exception or repeat.
- Accuracy entails ensuring that important information about completed transactions is correct throughout the process, and that transactions and services are conducted and processed according to plan.
- In the framework of the confirmation of such supply, the timeliness of the provision of services or the delivery of goods is included.
- Authorization entails ensuring that the processing is carried out in compliance with the information processing rules' appropriate approvals and privileges.

The treatment's integrity has to consider the risks involved [26]. The main ones concern the fact that the party initiating the transaction will be unable to complete it or provide the service correctly or in accordance with the needs. Without the necessary control mechanisms in place, the buyer may not receive the ordered goods or services, may receive more than is required, or may receive the incorrect goods or services. The processing integrity affects all system components, including the procedures for initiating, recording, processing, and reporting information, product, or service, which are subject to the obligation of the party providing them. The nature of educational services necessitates the entry of data via specially designed web forms, whereas data entry methods in other software systems can vary significantly. As a result, the data entry control mechanisms in educational services systems may differ from those in other systems.

The integrity of processing differs from the integrity of data in that it does not imply that the information stored in the system is complete, accurate, timely, and authorized. If the system, on the other hand, processes information outside its borders, the organization can only establish limited control mechanisms over the completeness, accuracy, authorization, and timeliness of the information provided for processing. Errors in information obtained from outside sources are usually beyond the organization's control. As a result, if the data source is not internal to the system, this should be stated explicitly in the relevant documentation.

The control of processing process entails establishing policies and procedures for the efficient management of planned processes, the protection of their output, the monitoring of IT infrastructure, and the provision of preventive hardware maintenance. Processing control effectively helps to maintain data integrity while also reducing unplanned delays and IT costs. The following control objectives have to be met in order to achieve this:

- To maximize educational benefits, management has to ensure that tasks and processes are organized in the most productive sequence possible. Monitoring, analysis, and evaluation of the capabilities and characteristics of the organization's processes, as well as consultations with third parties, should all be done for this purpose.
- To avoid unintentional abuse of processes by their users, policies have to be defined, implemented, and maintained to ensure that employees and customers are aware of the processes they use.
- In order to avoid hardware failures and increase speed, periodic maintenance procedures have to be defined and implemented, as well as the state of the information infrastructure monitored.
- Evaluate endurance and recovery capabilities in the event of incorrect data and attacks.

2.3. Automated Control Mechanisms

Maintenance and monitoring are required as a preventative measure. (The IT manager chooses the elements of the IT infrastructure to be monitored based on the risk assessment, the chosen specific approach, and his experience.) The frequency, indicators, monitoring method, and measures to be taken in the event of non-compliance are all determined by the same factors.) of the IT infrastructure to ensure educational continuity and early detection of potential problems.

Each of these control objectives can be automated in part or entirely. Define and implement control mechanisms for specific parts of the organization's information system in accordance with the objectives to achieve quality process management (see Figure 1). Controlling processing is an important part of the overall security management system and identifying areas where control mechanisms can be implemented is a difficult task that requires the participation of qualified specialists in both risk analysis and implementation. There is a need to monitor and evaluate the effectiveness of the chosen control mechanisms after they have been implemented.

Some data have to be checked on a regular basis to ensure the proper operation of the control mechanisms. Such checks typically entail approving the output of specific processes after comparing it to the desired result. Some events, such as a significant increase [7] in activity, may indicate attempts at unauthorized system access and/or fraud. Monitoring mechanisms that monitor such parameters report suspicious activities to the appropriate responsible parties, who decide whether the concerns are justified and what action should be taken.

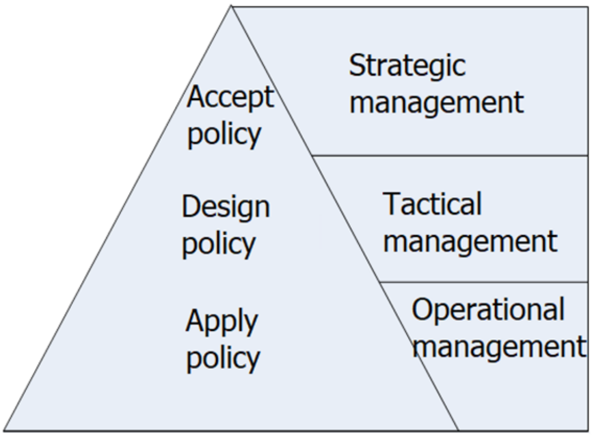

Figure 1. IT control mechanism hierarchies

As digitalization progresses, software that continuously monitors certain control mechanisms can be developed. Software that monitors network traffic for traces of breaches in firewalls and anti-virus programs is an example of continuous monitoring. This is a process that can be used to generate an immediate report and is used in high-risk situations or when a large amount of data needs to be processed. Between the completion of fieldwork and the delivery of the observation report, there is a time lag, which makes the information in the report less useful and valuable to its users. This is due to the "aging" of data in the report concerning the deterioration of the situation in the problematic control mechanisms.

To shorten this period, ongoing insurance is used, and theoretically, in some circles, it should be possible to shorten the time it takes to create a report so much that it can be provided immediately. Continual provision necessitates a high level of dependability in the organization's information systems. In this regard, before implementing such technologies, the specialist should assess the quality of the systems and the information they provide. Low-quality systems or those that provide less reliable information (and thus necessitate a greater degree of human intervention) are less prone to continued provisioning than those that provide more reliable information. The time it takes to deliver a final report in a highly reliable information quality environment is shorter, whereas in a low-quality environment, the time it takes to deliver the report is longer because the information has to be verified and approved.

Continual provision is an important part of modern systems and incorporating it into a fully automated monitoring system would improve the effectiveness of both the monitoring process and the educational organization's operations.

We propose that the values of the following parameters be monitored and analyzed to determine the quality of control:

- The number of system components affected by operational incidents;
- Unplanned hours when the system was unavailable due to poor processing management;
- The number of incidents and operational delays caused by incidents;
- The number of incidents caused by deviations in the parameters submitted;
- The percentage of processes that were scheduled but were not completed;
- The number of incidents caused by insufficient procedures;
- The frequency with which procedures are updated;
- The proportion of tasks that are automated.

We recommend using a 6-grade scale to assess the state of each organization in terms of processing quality control. The lowest level is 0 and the highest level is "optimized" (see Table 1).

Table 1. A scale to assess the state of organizations in terms of processing quality control

Level/ Name	**Description**
Level 0 Non-existent level	When no time or resources are allocated for the creation and maintenance of basic IT operations, the control of processing in the organization can be defined as non-existent. Organizations at this level must either advance to the next level or face extinction.
Level 1 Entry level	The organization recognizes the need to structure IT support functions. There are only a few standard procedures in place, and the organization's activities are in response to specific events. Most operational processes are not formally planned, and processing requests are accepted without prior verification. Computer systems and software that support educational processes are frequently unavailable, causing employees to waste time while they wait for the resources they require. Frequently, the system's output is of poor quality or does not exist at all.
Level 2 Intermediate level	The organization achieves repeatable results in an intuitive manner. He recognizes the importance of processing control activities and, as needed, funds are allocated for new hardware and software resources to improve the quality of control mechanisms. Because there are no formally defined rules for what to do, when to do it, and how to do it, the outcome is determined by the abilities of the employees involved in the processes.
Level 3 Defined Mid-level	The organization understands and accepts the need for operational control, and there is a distribution of necessary resources. Duplicate functions are defined, standardized, documented, and disseminated in a formalized manner. The events and outcomes of the completed work are recorded, but only partially or late reach the members of management. Third-party support agreements. Support agreements with third countries are informal.
Level 4 Managed and evaluable level	The processes and related control mechanisms are clearly defined, and the relevant employees are aware of and understand how they work. Formalized training procedures exist. Any deviations from the norm are promptly identified and corrected. There is a constant desire to increase process automation. Third-country agreements are being formalized.
Level 5 Optimized level	IT support operations are efficient and adaptable enough to meet any change in the organization's needs with minimal

	productivity loss. Processing control processes are automated, standardized, documented, and subject to continuous improvement to reach this level. The automated processes that support the systems run smoothly and contribute to environmental stability. All issues are investigated to determine the root cause of their occurrence. If the requirements for the processes change, quick steps are taken to control the new parameters. When using third-party services, the resources they use are always checked for reliability. Preventative maintenance is performed.

It is worth noting that in order to achieve a higher level of maturity in the processing control processes, an automated information system that helps standardize, document, and improve them has to be implemented. We can summarize an application's services for the needs of data management and processing control as opportunities for:

- quick and clear division of responsibilities;
- providing instruction;
- Investigating potential areas for improvement;
- simple documentation;
- backing for standardization.

3. Information Security Implementation Life Cycle and Standards

Security of information is an essential component of any IT control measures. Infrastructure and data, as well as their storage and processing, are all covered by information security. It serves as the foundation for the dependability of most IT control methods. Exceptions include financial components of digitalization (e.g., ROI - Return on Investment or Rate of Return used to measure investment efficiency), budgetary control mechanisms, and some project management control mechanisms.

3.1. Major Information Security Concepts

Over the last decades, three information security concepts have achieved widespread acceptance: confidentiality, integrity, and availability [3], [9].

- Confidentiality - Confidential information should only be used for its intended purpose and should be kept safe from unauthorized disclosure or tampering.

- Integrity - the condition in which data is truthful and full is referred to as information integrity. This involves the consistency with which financial data is processed and reported.

- Availability - educational services, their students, and partners have to have access to information in the appropriate format, at the right time, and in the right place. The capacity to recover from lost or damaged data and IT services is included in availability.

At least one of these principles should be incorporated into any control mechanism. A method for automatically creating control mechanisms has not yet been developed. This, in our opinion, is a trend that will change as artificial intelligence advances. Currently, they are developed and implemented after identifying vulnerabilities in the hardware and software used and categorizing existing control mechanisms. This activity is supported by a variety of frameworks, including COBIT, ITIL, ISO27001, and others. According to our observations, any organization aiming for quality information security management should use the most applicable components of these frameworks to categorize or evaluate existing and necessary control mechanisms. On this basis, you can document your own policy for:

- Compatibility with current laws and regulations;
- Alignment with the organization's objectives;
- Reliable assurance that the activities carried out are in accordance with the strategic and operational management's policies, as well as the organization's risks.

According to research, an information security policy should include the following elements:

- A common policy for the level of security and confidentiality across the organization. This policy must be written in accordance with all applicable national and international legal requirements, and it has to specify the level of control and security required based on the sensitivity of the systems and data processed.
- Guidance on information classification and access rights at each level. The policy should also specify the limitations on how this information can be used by those who have access to it.
- Definition of the concepts of data and system ownership, as well as the power required to create, change, or delete information. Coordination in large organizations becomes difficult without these guidelines, as there may be a lack of responsibility for data or systems.
- Individual policies that define and impose conditions on employees in a variety of sensitive areas. Including background checks on new employees before they join the organization, annual credit checks, and hiring - signing agreements to accept responsibility for the required levels of control, security, and confidentiality.
- Define the overall requirements for educational service continuity. All aspects of disaster and accident education services are covered by these policies.

Separate structures for developing and monitoring the implementation of information security policies should be established in each secondary or large educational organization. It is necessary to understand the life cycle of information security and how it interacts with the various components of information systems in order to monitor it.

Looking at the traditional life cycle of IT security according to the PPDIOO life cycle Cisco model (Prepare, Plan, Design, Implementation, Operation, Optimization) [5], [6], we can see that most of its stages are accompanied by relevant information security services (see Figure 2). One of the biggest issues with IT security and related services, in our opinion, is that potential users are not always ready to fully adhere to the life cycle - often, organizations are limited to only implementing services during the planning and design stages. They remain "on paper" once it is understood that implementing the developed recommendations necessitates investments. Another issue arises when the service provider is unable to provide the information security system throughout its entire life cycle. These issues are frequently caused by educational organizations' narrow specialization (for example, only conducting tests or preparing documentation) or a lack of expertise.

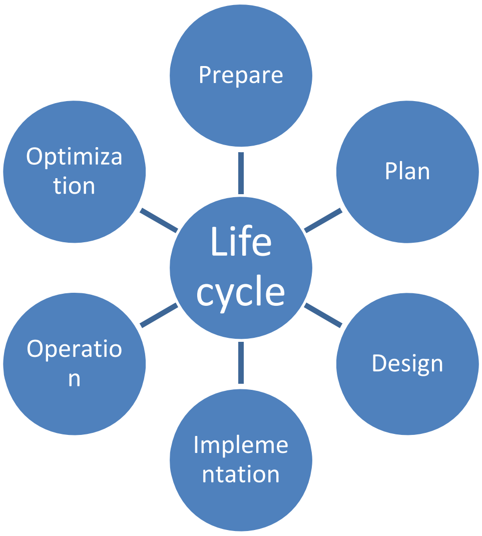

Figure 2. Information security life cycle according to PPDIOO Cisco model

The quality of the "Preparation" stage implementation will determine how secure information will be in the future. It is at this point that the flaws in the current information security system have to be exposed. It would be difficult to plan the next steps, to work on the implementation, operation, and optimization of protection systems and mechanisms, without a clear understanding of them, as well as the specifics of educational services.

Informally, the services for this stage can be divided into two categories: technical and education oriented. The first group consists of various observations and assessments of the current state of networks and information systems in terms of IT security. The lowest level of verification for the security of information architecture is network monitoring. Penetration tests, for example, are frequently performed as part of this measure. The next higher level is the information system security check, which examines firewalls, wireless networks, and specific applications (Learning Management System, Competency Management System, Intelligent Tutoring System, Learning Activity Management System, Student Information System, and so on).

The second set of services pertains to educational processes, which are the highest level of educational architecture. The work of the human resources department, interactions with teachers, partners, and students, and contracts signed by the educational organization for receiving one or more services are all examined at this level. In addition, metrics will be used to evaluate the effectiveness of IT security measures.

Once the flaws in information security have been identified, a strategy for addressing them should be devised. The services related to completing this task are the most in-demand and widely available. These include the creation of various IT security concepts, contingency plans, educational continuity plans, accurate response guides, and user instructions, among other things.

The binding with specific means of protection chosen in previous stages is a feature of the "design" stage. The selected systems may remain in the final version of the project or be replaced by others, depending on the characteristics they exhibit and the needs they have to meet. Replacing them is reasonable, even if the chosen solutions are significantly more expensive than their alternatives. The design can be more general (for example, to limit the location of means of protection) or more detailed (for example, to limit the location of means of protection) (for example, to get to the settings of the equipment). Changing the topology of an existing network to improve the security of a corporate network or an entire information system is frequently required when redesigning the security of a corporate network or an entire information system. The recommendations made during the inspection can be used at this point.

3.2. Information Security Tools

Services for implementing information security tools are in high demand, particularly among large corporations with established territorial structures. Building a comprehensive IT security system is essential for the organization's critical systems to be protected. This complicates the use of implementation services by educational institutions. The services provided in this direction usually include work reorganization in addition to the implementation of relevant technical means.

The action of the established preventive, revealing, and corrective control mechanisms is monitored during the operation and maintenance phase. The analysis of their application's results serves as the foundation for their optimization. Typically, the optimization is followed by another inspection, during which changes in the state of information security are recorded. Following optimization, we return to the planning stage (updating existing documents), redesigning existing networks and information systems, implementing new systems or changing existing ones, and so on.

The results of the inspection process are used in the stages of preparation, planning, design, and optimization to obtain information about the existing system and recommendations for its improvement. There are also clear standards for the acquisition and commissioning of new applications by organizations, as previously mentioned. As a result, the implementation of remedies is subject to information system revision [19], [20], [27]. The support phase corresponds to the idea of a continuous monitoring and monitoring approach to gathering specific evidence with the aid of a computer.

The analysis of the organization's security policy reveals that it is both necessary and feasible to develop an automated information system that supports the stages of the information security life cycle and end-user access to information. This would aid in conducting a quality review and, as a result, improving the organization's information security system. As previously stated, standards exist to support organizations' policy requirements. To achieve a satisfactory level of security and demonstrate it to third parties, the organization has to select and enforce some of the existing information security standards. The ISO 27000 series of standards, the ITIL library, and free alternatives such as the ISF (Information Security Forum) standard have all grown in popularity in recent years.

ISO has retained the ISO 27000 series of standards for information security purposes, and they are related to other topics such as quality control (ISO 9000) and environmental protection (ISO 14000). Hundreds of potential control mechanisms are described in the ISO 27002 standard, all of which could theoretically be implemented and used. The standard establishes guidelines and fundamental principles for initiating, implementing, maintaining, and improving information security management in an organization. The standard's control mechanisms are intended to meet specific requirements identified through a formal risk assessment. The standard also intends to provide guidance for the development of organizational security standards and practices for effective security management, as well as to aid in the development of confidence in internal organizational activities. Some of the main benefits of ISO 27001 certification, in our opinion, are:

- reducing financial losses by ensuring the continuity of educational services, manageability, reliability, and process transparency;
- establishing a clear information security control framework;
- students, teachers, and administrators have more faith in the system;
- increasing the likelihood of being selected for tenders and competitions;
- demonstrate adherence to legal and regulatory requirements;
- enhancing the organization's image and increasing its authority.

The ITIL (IT Infrastructure Library) [2], [10], [22] approach to IT management provides a set of best practices derived from the public and private sectors of various countries. ITIL is a set of rules that describe a systematic approach to IT deployment, implementation, and management. ITIL specifies processes, functions, roles, and responsibilities, as well as building blocks. They serve as the foundation for the efficient and effective use of information technology.

The eponymous standard, developed by the Information Security Forum (ISF) [4], [13], aims to manage the risks associated with every aspect of an information system, regardless of the market sector in which the organization operates, its size, or its structure. End-user security, organization-level security management, critical educational applications, computer deployment, networks, and systems development are all covered by the ISF, which is free to use.

4. Conclusion

In the face of widespread digitalization in educational services, every organization has to strive to meet modern-day quality and security standards for both information and other assets. Simultaneously, one of the primary responsibilities of management is to improve the utilization of available resources such as data, application systems, technologies, employees, and material resources. To fulfill these responsibilities and achieve its goals, management has to establish an adequate internal control system. As a result, a framework that clearly specifies how each employee's activities meet information requirements and affect resources is required.

Various control frameworks (i.e., ISO27001, COBIT, ITIL, and others) emphasize the connection and influence of IT resources, as well as the business requirements for efficiency, operability, confidentiality, integrity, accessibility, completeness, and reliability of the information to be met. All employees involved in the use, design, creation, maintenance, or operation of information systems have to have a responsible attitude for the framework to be implemented effectively. At least one of these principles should be incorporated into any control mechanism but a method for automatically creating control mechanisms has not yet been developed. This, we believe, will change as artificial intelligence advances.

Acknowledgements

This research is financially supported by NPI-45/2020 from University of Economics - Varna Science Fund.

References

[1]. AICPA. (2020). *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Retrieved from: https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf [accessed: 19 May 2022].

[2]. Althobaiti, K., Jenkins, A. D., & Vaniea, K. (2021). A Case Study of Phishing Incident Response in an Educational Organization. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 1-32. https://doi.org/10.1145/3476079

[3]. Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1-11. https://doi.org/10.25008/bcsee.v1i1.2

[4]. Firmansyah, A. F., Aini, Q., Saehudin, A., & Amsariah, S. (2020, October). Information security awareness of students on academic information system using kruger approach. In *2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-7). IEEE. https://doi.org/10.1109/CITSM50537.2020.9268795

[5]. Hernandez, L., & Jimenez, G. (2018, April). Design and validation of a scheme of infrastructure of servers, under the PPDIOO methodology, in the university Institution-ITSA. In *Computer Science On-line Conference* (pp. 367-379). Springer, Cham. https://doi.org/10.1007/978-3-319-91186-1_38

[6]. Hutton, K. T., Schofield, M. D., & Teare, D. (2008). *Designing Cisco Network Service Architectures (ARCH)(Authorized Self-Study Guide)*. Pearson Education.

[7]. Iliev, M., Balabanova, I., Kostadinova, S., & Georgiev, G. (2019, September). Statistical processing and quality of service for incoming traffic in markov chains. In *2019 29th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)* (pp. 1-7). IEEE. https://doi.org/10.1109/EAEEIE46886.2019.9000418

[8]. Ishlahuddin, A., Handayani, P. W., Hammi, K., & Azzahro, F. (2020, September). Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu). In *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)* (pp. 236-241). IEEE. https://doi.org/10.1109/IC2IE50715.2020.9274599

[9]. Kenyon, B. (2019). *ISO 27001 controls–A guide to implementing and auditing*. IT Governance Ltd.

[10]. Kim, H. W., Kang, B. R., Kim, D. S., & Moon, S. C. (2018). A Design of University Information System Operation Audit Model based on ITIL V3. *Journal of Information Technology Applications and Management*, *25*(3), 29-41. https://doi.org/ 10.21219/jitam.2018.25.3.029

[11]. Kuyumdzhiev, I. (2020). A model for timely delivery of it solutions for Bulgarian universities. *International multidisciplinary scientific geoconference: SGEM*, *20*(2.1), 3-10.

[12]. Kuyumdzhiev, I., & Nacheva, R. (2019). Correlation Between Storage Device and Backup and Restore Efficiency in MS SQL Server. *Serdica Journal of Computing*, *13*(3-4), 139p-154p.

[13]. Makhbuba, S. (2021). Security Parameters in the Protection Of Information Systems. *ResearchJet Journal of Analysis and Inventions*, *2*(11), 108-111. https://doi.org/10.17605/OSF.IO/9BZN3

[14]. Marinova, R., & Momcheva, G. (2019, May). Survey of information technology undergraduate degree programs in Canada. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* (pp. 1-4). IEEE. https://doi.org/10.1109/CCECE. 2019.8861715

[15]. Murad, D. F., Fernando, E., Irsan, M., Kosala, R. R., Ranti, B., & Supangkat, S. H. (2018, September). Implementation of COBIT 5 framework for academic information system audit perspective: evaluate, direct, and monitor. In *2018 International Conference on Applied Information Technology and Innovation (ICAITI)* (pp. 102-107). IEEE. https://doi.org/10.1109/ICAITI.2018.8686700

[16]. Pashev, G. (2021). An Adaptive E-learning System for Teaching Mobile Applications. *International Journal of Computer Science and Mobile Computing*, *10*(9), 80-87. https://doi.org/10.47760/ijcsmc. 2021.v10i09.008

[17]. Petrov, P., Radev, M., Dimitrov, G., & Simeonidis, D. (2022). Infrastructure Capacity Planning in Digitalization of Educational Services. *International Journal of Emerging Technologies in Learning (iJET)*, *17*(3), 299-306. https://doi.org/10.3991/ ijet.v17i03.27811

[18]. Petrov, P., Dimitrov, G., & Ivanov, S. (2018, July). A comparative study on web security technologies used in Irish and Finnish banks. In *Conference Proceedings of 18 International Multidisciplinary Scientific Geoconference SGEM 2018* (pp. 2-8).

[19]. Petrova, S., Sergeev, A., Getova, I., & Kostadinova, I. S. (2019). Online Public Access Catalogs in Bulgarian University Libraries an Empirical Study of Seven-Year Evolution. In *12th Annual International Conference of Education, Research and Innovation (ICERI)* (pp. 230-236). International Academy of Technology, Education and Development. https://doi.org/10.21125/ iceri.2019.0091

[20]. Petrova, S., Stefanov, S., Ivanov, S., Sergeev, A., & Getova, I. (2019). Information systems used in Bulgarian university libraries as online public access catalogs. *International Multidisciplinary Scientific GeoConference: SGEM*, *19*(2.1), 353-360.

[21]. Radev, M. (2017). Using the TOPSIS Method to Evaluate Projects for Virtualization. *Izvestia Journal of the Union of Scientists-Varna. Economic Sciences Series*, (2), 234-241.

[22]. Rubio Sánchez, J. L. (2021). Methodology to Improve Services in Small IT Centers: Application to Educational Centers. *Computers*, *10*(1), 8. https://doi.org/10.3390/computers10010008

[23]. Sardjono, W., Priatna, W., Lusia, E., Putra, G. R., & Juwitasary, H. (2021). Information Technology Implementation And Its Performance In Educational Institution Using The Cobit Framework. *ICIC express letters. Part B, Applications: an international journal of research and surveys*, *12*(12), 1091-1099. https://doi.org/10.24507/ icicelb.12.12.1091

[24]. Saridewi, A. I., Wiharta, D. M., & Sastra, N. P. (2018, October). Evaluation of integrated university management information system using COBIT 5 domain DSS. In *2018 International Conference on Smart Green Technology in Electrical and Information Systems (ICSGTEIS)* (pp. 210-214). IEEE. https://doi.org/10.1109/ICSGTEIS.2018.8709144

[25]. Steuperaert, D. (2019). COBIT 2019: A significant update. *EDPACS*, *59*(1), 14-18. https://doi.org/10.1080/07366981.2019.1578474

[26]. Stoev, S. (2017). Integration of Risk Management Processes into the Business of IT Companies. *Izvestia Journal of the Union of Scientists-Varna. Economic Sciences Series*, (2), 225-233.

[27]. Stoev, S. (2019). Using of additional packages of components for accelerated application development. *Izvestia Journal of the Union of Scientists-Varna. Economic Sciences Series*, *8*(2), 171-179. https://doi.org/10.36997/IJUSV-ESS/2019.8.2.171

[28]. Vasilev, J., & Stoyanova, M. (2019). Information sharing with upstream partners of supply chains. *International multidisciplinary scientific geoconference: SGEM*, *19*(2.1), 329-336. https://doi.org/10.5593/sgem2019/2.1/S07.043