Journal of Social Sciences *Vol. IV, no. 1 (2021), pp. 84 - 94*
Fascicle *Social Science* *ISSN 2587-3490*
Topic *Sociology* *eISSN 2587-3504*

https://doi.org/10.52326/jss.utm.2021.4(1).11
UDC 004.056:006(478)

ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE REPUBLIC OF MOLDOVA THROUGH THE ISO 27001 STANDARD

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

Technical University of Moldova, 168, Stefan cel Mare Bd., MD-2004, Chisinau, Republic of Moldova
**arina.alexei@tse.utm.md*

Received: 12. 03. 2020
Accepted: 02. 01. 2021

Abstract. Data protection in public organizations in the Republic of Moldova (RM) is ensured by implementing mandatory cyber security controls (MCSR) adopted by the Government. In order to analyze the completeness of the controls, a comparative study was conducted between MCSR and the cyber security standard ISO 27001. The intention to comply with international cyber security standards is reflected in the Strategy on Information Security in the RM for 2019-2024. Compliance with national cyber security controls to international standards will ensure the security of the organization's data and resources by implementing effective, time-verified security controls. Another benefit is the confidence of foreign partners in public organizations of the country, because there will be guarantees that the data provided is confidential, complete and available. It is very important to increase the number of public organizations, certified with the ISO 27001 standard in Moldova in order to ensure the level of compliance with international cyber security requirements. The gap method, which was used in this study, measures the completeness of the MCSR, which is mandatory for public institutions in the Republic of Moldova, compared to the international standard ISO 27001. Based on the results obtained, a series of recommendations were developed which include: the creation of information security management systems (ISMS); performing internal and external audit of systems to meet trends; alignment of the MCSR, issued by the Government of the Republic of Moldova to the security controls of the ISO 27001 standard. It is very important to ensure an acceptable level of cyber security in public institutions in the Republic of Moldova, therefore implementation and certification with international standards is mandatory.

Keywords: *control, ISO 27001, ISMS, MCSR, public organization, security, standards.*

Rezumat. Protecția datelor în organizațiile publice din Republica Moldova (RM) este asigurată prin implementarea controalelor obligatorii de securitate cibernetică (MCSR), adoptate de guvern. Pentru a analiza exhaustivitatea controalelor, a fost realizat un studiu comparativ între MCSR și standardul de securitate cibernetică ISO 27001. Intenția de a respecta standardele internaționale de securitate cibernetică este reflectată în Strategia privind securitatea informațiilor din RM pentru 2019-2024. Conformarea controalelor naționale de securitate cibernetică, la standardele internaționale, va asigura securitatea datelor și resurselor organizației, prin implementarea unor controale de securitate eficiente, verificate în timp. Un alt beneficiu este încrederea partenerilor străini în organizațiile publice ale țării, deoarece vor exista garanții că datele furnizate sunt confidențiale, complete și disponibile. Este foarte importantă creșterea numărului de organizații publice, certificate cu standardul ISO 27001 în Moldova,

pentru a asigura nivelul de conformitate cu cerințele internaționale de securitate cibernetică. Metoda decalajului, care a fost utilizată în acest studiu, măsoară completitudinea MCSR, care este obligatorie pentru instituțiile publice din Republica Moldova, în comparație cu standardul internațional ISO 27001. Pe baza rezultatelor obținute, au fost elaborate o serie de recomandări , care includ: crearea sistemelor de management al securității informațiilor (ISMS); efectuarea auditului intern și extern al sistemelor pentru a îndeplini tendințele; alinierea MCSR, emisă de Guvernul Republicii Moldova, la controalele de securitate ale standardului ISO 27001. Este foarte important să se asigure un nivel acceptabil de securitate cibernetică în instituțiile publice , prin urmare implementarea și certificarea cu standarde internaționale sunt obligatorii.

Cuvinte cheie: *control, ISMS, ISO 27001, MCSR, organizație publică, securitate, standarde.*

Introduction

In the new global conditions, the need to ensure information security is growing, in the context of the massive migration of data from different organizations in the virtual space. The impact of the Covid-19 epidemic has significantly influenced organizations, which use ICT technologies in their work, as more companies have started to operate remotely and the vulnerability of data increases. The complexity of the data management process has increased considerably, thus ensuring data security is an ongoing challenge for ICT specialists.

To meet the new challenges, organizations need certification based on international information security standards, which contain procedures, methods and tools, capable, as a whole, of ensuring data security.

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 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 [1].

Under these conditions, the Information Security Strategy will be implemented in the period 2019-2024, which aims to increase information security at the state level, by achieving specific objectives in the field. Adapting national security controls to international security standards will undoubtedly increase electronic security, but also the confidence of foreign partners.

Currently, within the international cyber security standards of the ISO 27000 suite, certification is achieved through the ISO 27001 standard, which certifies the compliance of organizations with the provisions of this standard and the creation of Information Security Management System (ISMS), to ensure IT security [2]. Thus, ISMS allow the implementation of a complex mechanism that determines the security areas of organizations, sets objectives and determines controls, which will increase the credibility of both business partners and their own employees.

According to Decision no. 201 of 28.03.2017 of the Government of the Republic of Moldova [3], on the approval and implementation of mandatory minimum requirements for cyber security (MCSR) for all public institutions, in which the ministry or other central administrative authority is a founder, are required to implement the minimum requirements mentioned above.

The purpose of the research is to identify the degree of compliance of the requirements mentioned in Government Decision (GD) 201/2017, with the international security standard ISO 27001, on the approval of mandatory minimum requirements for cyber security, level 1 (use of ICT in the institution).

1. ISO/IEC 27001:2013

ISO 27001 is the international standard that allows the implementation of ISMS. The specifications of the ISO 27001 standard allow the protection of the company's assets, by creating an ISMS. To ensure information security, ISO 27001 addresses systematic processes, technologies and human resources, as needed, through risk assessment and assistance in the information management process [3].

Cyber security is ensured on the basis of the ISO 27001 standard, in accordance with the following three principles:

- The first is the principle of confidentiality of information, which confirms that only authorized persons have access to information.
- The second is the principle of information integrity, it determines the accuracy with which the data is processed.
- The third is the principle of availability of information, which ensures that authorized persons access the data on request [4].

ISO 27001 guarantees that information in all its forms is secure, and ISMS protects all forms that information can take: transport, processing or storage. Regardless of where they are stored: physically or in the cloud, taking into account security risks [5].

The Plan-Do-Check-Act chain is used by the ISO 27001 standard, for the implementation of ISMS and is based on the idea of a continuous process of implementing information security [6].

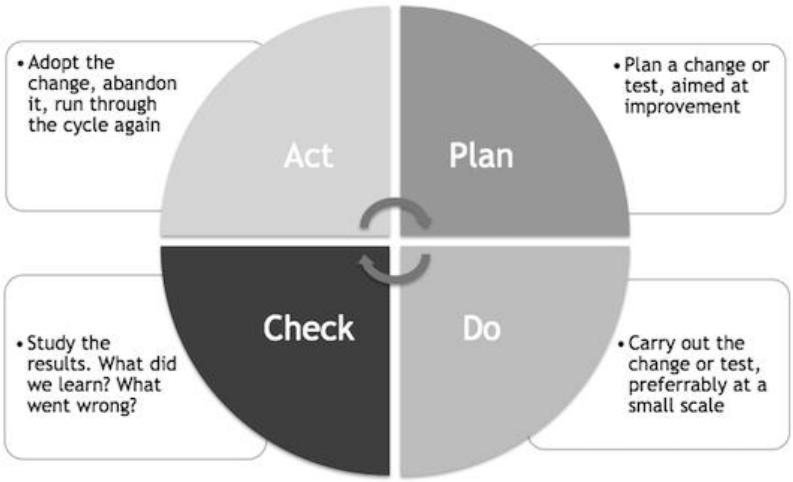

Figure 1. Plan-Do-Check-Act [6].

Certification, according to the ISO 27001 standard, is possible after performing the actions described in Figure 1, which is a closed cycle of actions, designed to support the information security management process.

Also, through the implementation of ISMS, it will increase the resistance to attack, as a result of continuous changes, depending on objectives, controls and security clauses.

According to the annual survey conducted by the International Organization for Standardization ISO [7], the number of valid certificates of ISO management standards (including ISO 27001) are reported for each country, each year. In 2019, the number of organizations certified with ISO 27001, at international level, was 36,362, while in 2018 there were 31,910 organizations. Thus, the number of certified organizations showed an annual increase of over 12%. The result of the survey showed that developed countries have widely implemented certification with the ISO 27001 standard, so that in Germany there are 1332 certified organizations, Japan - 6015 organizations, in China - 9508, in Romania the number of certified organizations is 668 organizations. While in the Republic of Moldova only 4 organizations are ISO 27001 certified [7].

ISO 27001 controls

As information security is not only strictly related to the IT field, the ISO 27001 standard also contains provisions for human resources management, legal framework, organizational management and physical security, for a complex approach to information security. Thus, the security controls contained in Annex A to the standard are organized into 14 sections, 35 objectives and 114 security controls, reflected in Table 1. Each section focuses on a specific aspect of information security [8].

Table 1

Security areas, objectives and controls in Annex A, ISO 27001

No.	Security domains	Objectives	Controls
A.5	Information Security Policies	1	2
A.6	Organization of Information Security	2	7
A.7	Human Resource Security	3	6
A.8	Asset Management	3	10
A.9	Access Control	4	14
A.10	Cryptography	1	2
A.11	Physical and Environmental Security	2	15
A.12	Operations Security	7	14
A.13	Communications Security	2	7
A.14	System acquisition, development and maintenance	3	13
A.15	Supplier Relationships	2	5
A.16	Information Security Incident Management	1	6
A.17	Information Security Aspects of Business Continuity Management	2	4
A.18	Compliance	2	8

In order for an institution to be certified with ISO 27001, it is necessary for it to meet the basic regulatory requirements, mentioned from clause 4 to 10, which are otherwise key clauses [9]. The elements of the main clauses are reflected in Table 2.

Table 2

Main clauses of ISO 27001

No clause	Main clause	Sub-clause
4	Context of Organization	Understanding: The organization and its context, The needs and expectations of interested parties, Determining the scope of ISMS, Information security management system.
5	Leadership	Leadership and commitment, Policy, Organizational roles, responsibilities and authorities.
6	Planning	Actions to address risks and opportunities, Information security objectives and planning to achieve them.
7	Support	Resources, Competence, Awareness, Communication, documented information.
8	Operation	Operational planning and control, Information security risk assessment, Information security risk treatment.
9	Performance Evaluation	Monitoring, measurement, analysis and evaluation, Internal audit, Management review.
10	Improvement	Non conformity and corrective action, Continual improvement.

The standard requires organizations to review the measures implemented with the controls in Annex A and, if they are lacking, to implement or document them as inapplicable [8].

2. MCSR

MCSR adopted by the Government of MD and apply to the State Chancellery, ministries, other central administrative authorities subordinated to the Government, including organizational structures within their sphere of competence (subordinate administrative authorities, decentralized and subordinated public services, public institutions in which the State Chancellery, Ministry or another central administrative authority as founder), of the autonomous administrative authorities and of the units with financial autonomy [3], for the following:

- Devices and software
- IT systems and resources existing in the institution, as well as those that are being developed, tested and implemented.

MCSR have been classified as follows:

- level 1: basic cyber security (use of ICT in the activity of the institution);
- level 2: advanced cyber security (use of ICT in the institution's activity and provision of ICT-based services).

The research will be performed for level 1, MCSRs. MCSR level 1, have been classified into 4 security domains:

1. Access Control
2. Physical security
3. Operational security
4. Secure exchange of data and communications

3. Research method

Consequently, it was examined compliance of the MCSR level 1 and the reference controls contained in the international standard ISO 27001.

The research was conducted using the gap analysis method, between GD 201/2017 and the international standard ISO 27001. The gap analysis is a tool or technique that allows an organization to compare the actual performance (or proposed, as in this case) with the standard international, taken as a reference example [10]. Thus, the gap analysis evaluates the response to "where are we?" in relation to "where we want to be" [10].

Based on the content of the MCSR level 1, in Table 3, the alignment to the controls from the ISO 27001 standard was performed, only the security domains were taken into account, which coincide in both documents. In order to identify security areas and controls related to ISO 27001, Annex A of this standard has been analyzed.

Table 3

Alignment of MCSR (level 1) with the controls in Annex A ISO 27001

MCSR, level 1	Annex A ISO 27001
15. Access Control	A.9 Access control
16. Physical security	A.11 Physical and environmental security
17. Operational security	A.12 Operations security
18. Secure exchange of data and communications	A.13 Communications security

4. Results and discussion

Table 4, shows those security controls of the ISO 27001 standard, which were partially or totally reflected in the MCSR (level 1), access control.

Table 4

Access control

No	MCSR level 1	A.9 Access control
1	The rights, obligations, restrictions and responsibilities of users are established by the person in charge of the process and communicated to the cybersecurity manager / subdivision;	A.9.1.1 Access Control Policy
2	The person performing system administration activities uses different accounts for administration functions and user functions;	A.9.1.2 Access to Networks and Network Services
3	Each user account is associated with a specific person. If the system does not allow the use of these accounts by other persons, then the system must include special technical means that do not allow the use of these accounts by third parties;	A.9.2.2 User Access Provisioning
4	If the system is not used for multifactor authentication, system users must use a password;	A.9.2.3 Management of Privileged Access Rights
5	The system user must use a password that is a combination of numbers (0-9), Latin characters (lowercase and uppercase) and special symbols (! #%), Consisting of the minimum number of characters, established by the internal security regulations, but not less than 7 characters;	A.9.2.4 Management of Secret Authentication Information of Users
6	Electronic storage and encryption of system users' passwords, including the user authentication process, is prohibited. It is allowed to transport them through an unencrypted public network only in the case of using a single-use password, with a validity of 48 hours from the moment of their transmission;	A.9.2.5 Review of User Access Rights
7	The system must have password management mechanisms, as well as ensure user authentication and identification for a limited period of time;	A.9.3.1 Use of Secret Authentication Information
8	The use of default passwords in equipment and software products is not permitted	A.9.4.2 Secure log-on Procedures
9	Data on activities in the system (logging) are stored in real time and kept for the period established by the internal security regulation, but not less than 6 months;	**A.9 Access control**
10	Any activity in the system must be identifiable in a specific user account or IP address;	A.9.4.3 Password Management System
11	User rights management must ensure that each user can only use his or her rights. The verification of the activities in the system is performed periodically, at time stages established according to the internal security regulations, but not less than once every 6 months;	
12	Access control management must be set to allow authorized access from the external network via the Internet with only a single-use password, including the electronic signature of the government electronic service of authentication and access control (MPass).	

Assessing compliance, can make the following recommendations related (missing or incomplete in paragraph 15):

- User registration is a good practice related to the security of human resources, which provides for the establishment in the shortest possible terms of the registration / deletion of users from the system, according to control A9.2.1. Registration and deregistration of users.

- The access rights of all external employees and users who have access to information processing, must be eliminated / restricted at the time of dismissal / change of job. Control A.9.2.6. Removing or adjusting access rights.

- The conditions for complying with the policies and keeping the secrets related to authentication must be stipulated from the moment of employment, implementation of control A9.3.1. Use of secret authentication information.

- Access to systems and applications must be controlled by a secure connection procedure to prove the identity of the user provided by A.9.4.2. Secure connection procedures, because the MCSR lacks clarification in case of successful / unsuccessful connection / disconnection and setting alerts for failed attempts and possible blockages. Depending on the nature of the system, access should be limited to certain times of the day or time periods and possibly be restricted depending on the location.

- Utilities must be monitored, as they can overwrite system rights, be easily found and downloaded, so it is very important to restrict the installation of software by users, according to control A.9.4.4. Use of privileged utilities.

- Access to the source code of programs used within the organization must be restricted to eliminate the risk of unauthorized modification. Control 9.4.5. Access to the source code of the program.

Table 5 shows the security controls of the ISO 27001 standard, which were partially or totally reflected in the MCSR, point 16, physical security.

Table 5

Physical security

No	MCSR level 1	Annex A.11: Physical & Environmental Security
1	Clear delimitation of the perimeter reserved for different groups of IT equipment, drawing up the plans of the server rooms and networks;	A.11.1.1 Physical Security Perimeter A.11.1.2 Physical Entry Controls
2	Ensuring the heating, ventilation and air conditioning conditions of the specialized rooms;	A.11.1.3 Securing Offices, Rooms and Facilities
3	Ensuring access to specialized spaces strictly according to the competencies;	A.11.1.5 Working in Secure Areas
4	Ensuring energy security by using devices in accordance with current regulations and with overload protection;	A.11.1.6 Delivery & Loading Areas A.11.2.2 Supporting Utilities
5	Ensuring adequate maintenance, according to technical requirements;	A.11.2.4 Equipment Maintenance
6	record of equipment and program products, use within the institution.	A.11.2.9 Clear Desk & Screen Policy

In point 16 of GD 201/2017, does not reflect how the physical protection against internal and external threats should take place, according to control A.11.1.1. But it is important to describe and stipulate how the company's assets will be physically protected against accidents, unauthorized actions and natural disasters.

Another aspect of physical protection is the security of cables, which must be adequately protected to limit access by unauthorized persons and thus minimize the risk of interception, interference or damage, as controlled by A.11.2.3. Wiring safety.

A very important role not covered by the MCSR (Level 1) is how the disposal of assets will take place, according to control A.11.2.5 Disposal of assets. It refers primarily to classified, valuable assets for which there must be processes to request and authorize their disposal or return. Limit the time in which assets can be removed depending on risks.

Security controls should also be applied to off-site assets (A.11.2.6), taking into account the different risks involved in remote work. This is a common area of vulnerability.

A final recommendation to ensure adequate physical security is to protect unattended equipment. Especially in workplaces, where exist a large flow of visitors, the frequent change of staff holding different roles, or when the equipment stays on overnight in spaces where other people have access.

Table 6 shows the security controls of the ISO 27001 standard, which were partially or totally reflected in the MCSR, point 17, operational safety.

Table 6

Operations security

No	MCSR level 1	Annex A.12: Operations security
1	Equipment and software products must be protected to ensure operability of systems;	A.12.1.1 Documented Operating Procedures
2	The following must be: a) an operating system with the current updates applied; b) antivirus program; c) firewall activated; d) installation of automatic locking features;	A.12.1.4 Separation of Development, Testing & Operational Environments A.12.2.1 Controls Against Malware A.12.3.1 Information Backup
3	The technical control is performed periodically, according to the internal security regulation	A.12.4.1 Event Logging A.12.4.2 Protection of Log Information
4	Application of cyber security requirements for the use of networks.	A.12.4.3 Administrator & Operator Logs
5	Elaboration of the continuity plan	A.12.5.1 Installation of Software on Operational Systems
6	Establishing the mechanism for decommissioning the equipment, destroying the data containing it and reusing it;	A.12.6.1 Management of Technical Vulnerabilities
7	Establishing security requirements and restrictions for personal equipment used within the institution.	

Implementing change management control, A.12.1.2, is essential in most environments to ensure that changes are appropriate, effective, authorized and carried out in a manner that minimizes the likelihood of unauthorized or accidental action.

It is necessary to take into account capacity management, control A.12.1.3. Identify future requirements that will meet the objectives of the organization and for which it is necessary to ensure the performance of the system. Such as the ability to: data storage, processing, communications. It is also necessary for capacity management to be proactive (capacity considerations as part of change management) and reactive (alert triggers, for the moment when capacity utilization reaches a critical level).

Another critical aspect is the implementation of control A.12.4.4, clock synchronization. The clocks of all relevant systems involved in processing information within an organization or security domain, to sync with a single reference time source for possible investigation.

Restriction of software installation, control A.12.6.2, especially on local devices. The installation of software by users raises a number of threats and vulnerabilities, including the

threat of malware and the potential violation of software licensing laws. Ideally, users could not install any software on the organizational equipment, however, there may be commercial or practical reasons why this is not possible.

Table 7 shows the security controls of the ISO 27001 standard, which were partially or totally reflected in the MCSR, point 18, the secure exchange of data and communications.

Table 7

Secure exchange of data and communications

No	MCSR level 1	Annex A.13: Communications Security
1	Applying the guidelines of Service e-mail system;	
2	To prohibit: automatic forwarding of messages; send or transmit messages considered obscene and other antisocial messages; transmission/retransmission of irrelevant content; usage of the e-mail service for obtaining a material gain, for personal, political or other purposes; distribution of copyrighted materials; transmission of confidential information by unsecured electronic messages; the use of the e-mail service for spread malware; hiding and attempting to hide identity when a message is sent by e-mail;	A.13.2.1 Information Transfer Policies & Procedures A.13.2.3 Electronic Messaging
3	Limiting staff access to irrelevant content.	

For this security domain, MCSR is different from the international security standard ISO 27001. Although this domain has a great impact on the security of information in communications networks. Even those controls, which were mentioned in Table 7, are partially specified in the MCSR.

It is not specified how the network controls for information protection take place, referring to the indications in A.13.1.1 Network controls. Depending on business requirements, risk assessment, classifications and segregation requirements, it is necessary to design and implement balanced network controls. Examples of technical controls are: access control lists, intrusion detection and prevention systems, network-level firewalls, physical, logical or virtual segregation.

To secure network services A.13.1.2, as a first step it is necessary to assess the risks. Subsequently, it is determined whether the relationship between business and security requirements was taken into account when designing the network. It is also advisable to include security measures in agreements for the provision of network services.

It has not been stipulated exactly how the organization's network is segregated (A.13.1.3). Information service groups, users and information systems should be separated into virtual networks (VLANs). The design and control of the network must support information classification policies and network segmentation requirements.

At the same time, it is important to create agreements for the transfer of information (A.13.2.2) within the organization, but also with third parties. Often, communication and transfer procedures are implemented without a real understanding of the risks, which therefore creates vulnerabilities and data compromise.

It is necessary to take into account confidentiality and non-disclosure agreements (A.13.2.4). Good control describes how the requirements for confidentiality or non-disclosure agreements should be identified, reviewed periodically and documented, reflecting the organization's information protection needs. Agreements are usually organization-specific and should be developed taking into account the value of the assets, through risk analysis. These include:

- General non-disclosure agreements.
- Agreements with customers using standard terms and conditions.
- Association/provider/partner agreements used for small and independent service providers that the organization uses to provide services.
- Conditions related to employment.
- Privacy policies.

Conclusion

Cyber security has become a priority for institutions in the Republic of Moldova, through the development of information technologies and their application more and more in daily activities. Moreover, the Republic of Moldova ranks among the top 10 European countries, with the most dynamic developments of the information society.

The results of the annual ISO survey, for 2019, showed that globally, the number of organizations certified with ISO 27001, increased by more than 12%, compared to 2018. Countries with developed economies have aligned with the ISO 27001 standard, on while in Moldova the number of certified companies is very low and this is necessary to increase the number of certified organizations, for two important reasons:

- Information security at the state level to protect services and assets;
- Increasing the trust of foreign partners that the organizations in the Republic of Moldova have complied with international standards.

In the conditions of the pandemic with Covid 19, the need to use ICT tools in business has increased even more, using new technologies to ensure the continuity of processes and the functioning of state and private enterprises.

According to the National Information Security Strategy, for the years 2019-2024, there is a tendency to align with international standards. Creating an information security management system (ISMS), depending on the value of the organization's assets, is an important step. ISMS guarantee by approaching information security as a whole, that implemented controls will increase the resistance of organizations to information attacks.

If certification to ISO 27001 is not possible because it is a very costly process, it should be aligned with the mandatory requirements of cybersecurity for organizations at the state level, taking into account the objectives and security controls of ISO 27001. This would ensure a high level of security for organizations, which is in line with international trends and is not outdated.

Thus, gap analysis, between mandatory cyber security requirements (MCSR) reflected in GD 201/2017 and controls ISO 27001 may be proposed following recommendations:

- To analyze security risks, at the organizational level, to classify assets and information, for more effective security.
- Creation for the level 1 organizations (uses ICT in its activity) an ISMS, which will allow the implementation of complex mechanisms, distributed on security domains, according to the prescribed objectives.
- The approach to information security within the organization is a complex process, constantly changing, for which the internal or external audit of the information system is

a key process, with the identification of the path to follow for assure information security.

- MCSR compliance, level 1 with the ISO 27001 standard controls, to ensure that information is secure, regardless of its status: processing, transport or storage (physical or in the cloud).

The method used in this paper, such as the method of analyzing the gap between MCSR level 1 and ISO 27001 controls, allows us to determine "where are we?" in relation to “where we need to be”, in order to adjust the process of ensuring information security, in public organizations in the Republic of Moldova, to the modern trends described by international standards.

Bibliography

1. Moldova climbed four places in the global report on developments in the information society. [online]. [accessed 20.10.2020]. Available: http://mec.gov.md/ro/content/republica-moldova-urcat-4-pozitii-raportul-mondial-privind-evolutia-societatii. [in Romanian].
2. Susanto H., Almunawar MN., Tuan YC. Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. In: International Journal of Engineering & Technology [IJET], 2012; 2 (1), pp. 67-75.
3. Decision 201/2017 of the Moldovan Government on the approval of the Mandatory Minimum Cyber Security Requirements. In: Official Monitor. 07.04.2017, L 109-118/277. [Accessed 2.11.2020]. Available: https://mei.gov.md/sites/default/files/hg_201_2017_cerinte_minime_obligatorii_de_securitate_cibernetica.pdf . [in Romanian].
4. Disterer G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. In: Journal of Information Security, 2013, 4(2), pp. 92-100.
5. 27000:2018[E], ISO/IEC: Information technology — Security techniques — Information security management systems — Overview and vocabulary, [online]. [accessed 1.11.2020]. Available: https://www.iso.org/standard/73906.html.
6. Stefan F., Gernot G., Andreas E., Bernhard R., Edgar W. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. In: 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007), Melbourne, Qld., Australia, 17-19 December 2007, pp. 381-388.
7. ISO Survey of certifications to management system standards - Full results. [online]. [accessed 2.11.2020]. Available: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&sort=name&viewType=1.
8. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, [online]. [accessed 1.11.2020]. Available: https://www.iso.org/standard/54534.html.
9. Valdevit T., Mayer N., Barafort B. Tailoring ISO/IEC 27001 for SMEs: a guide to implement an information security management system in small settings. In: O’Connor R.V., Baddoo N., Cuadrago Gallego J., Rejas Muslera R., Smolander K., Messnarz R. (eds) Software Process Improvement. EuroSPI 2009. Berlin, Heidelberg. Berlin: Springer, 2009, 42, pp 201-212.
10. Al-Mayahi I., Mansoor SP. ISO 27001 GAP Analysis-Case Study. In: International Conference On Security & Management [SAM’ 12]. Las Vegas, July 16-19, 2012.