[1.]Rade DRAGOVIĆ, [2.]Sanja STANISAVLJEV, [2.]Dalibor DOBRILOVIĆ, [3.]Dragan DRAGOVIĆ, [2.]Vladimir MILOŠEV

SOFTWARE INFORMATION SECURITY MANAGEMENT FOR GOVERNMENT AUTHORITIES

[1.]Institute for standards and technologies, Belgrade, SERBIA
[2.]University of Novi Sad, Technical Faculty "Mihajlo Pupin", Zrenjanin, SERBIA
[3.]Serbian Business Registers Agency, Belgrade, SERBIA

Abstract: This article treats two very important items in the functional matrix of the state bodies work: information security and software development. Information security is not only a recommendation with content in the domain of organization, technology, and procedure but is also defined by legal and by–laws. Lately, software development has been increasingly outsourced, so it is important for state authorities to know that software development is no longer a free assessment of the client and programmer, how and what will be developed, and to what extent the software will be delivered.

Keywords: software development, standards, information security, state authority, cyber security

INTRODUCTION

Digitalization of the state bodies through information systems implies the application of appropriate laws and standards in the management of ICT systems. The increased number of existing information systems is a consequence of legislative changes and digitization of work of the state bodies so that they can respond to the specifics of work tasks related to the maintenance of the existing state and the improvement of their information systems both to other state bodies and to legal and natural persons. The initial requirements refer to the requirements by the law, prevention of security incidents, system control and management of access to information systems, and the prevention of data leaks, but also the technological monitoring of adopted security acts, the introduction of technological measures for monitoring and preserving data security and documenting the application of security solutions within the implemented ICT systems. Considering the number and complexity of these systems, as well as the fact that their operator is the state as well as relevant ministries (which establish and maintain them), it is necessary to manage software development organizational, technological, and procedural according to the requirements of the Information Security Act and the ISO/IEC 27001 – Security standard information, cyber security and privacy protection – Information security management systems – Requirements.

INFORMATION SECURITY

Frequent incidents in the immediate and wider environment impose the need to strength the field of information security in state bodies and to establish a strengthened framework for information security management called ISMS (Information security management systems). ISMS should represent a systematic approach for establishing, implementing, functioning, monitoring, reviewing, maintaining and improving the information security of the state body, in order to achieve business goals, but the risk matrix must not be ignored. ISMS must be based on an assessment of information security risks and the level of acceptability of such risks by the state authority in such way that effectively and efficiently treats the risks and manage the risks in an appropriate manner. Requirements for the protection of information assets, whether they are legal, regulatory, contractual or as a consequence of risk management and the application of appropriate controls, when necessary, contribute to the successful implementation of ISMS. The requirements of the standard mean all the obligations that the standard stipulates that the state body must fulfill [1].

The Cyber Security Program should be developed for the entire organization of the state body, including all software through business and IT–related functions, considering the fact that attacks and threats to information security can occur anywhere within the state body. It is necessary to implement the requirements of the standards ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27032, ISO/IEC 22301, in areas that include security in the intranet/internet space, i.e. intranet/internet security issues that focus on bridging results risk analysis between different domains of information security in intranet/internet space. According to the stated standards, it is necessary to implement technical guidelines for solving intranet/internet security risks, including social engineering attacks, hacking, spyware and attacks using other potentially malicious malware software. These technical guidelines should provide controls for the treatment of these risks, including controls for preparing responses to attacks from malicious software (malware), malware organizations for detecting and monitoring attacks [2].

It is necessary to generate a framework for efficient and effective information exchange, coordination and incident management among interested parties in the Internet space. Stakeholders that may be involved are employees, clients and third parties, which may be different types of organizations or individuals, as well as providers, which include service providers as well as all those identified by the risk matrix.

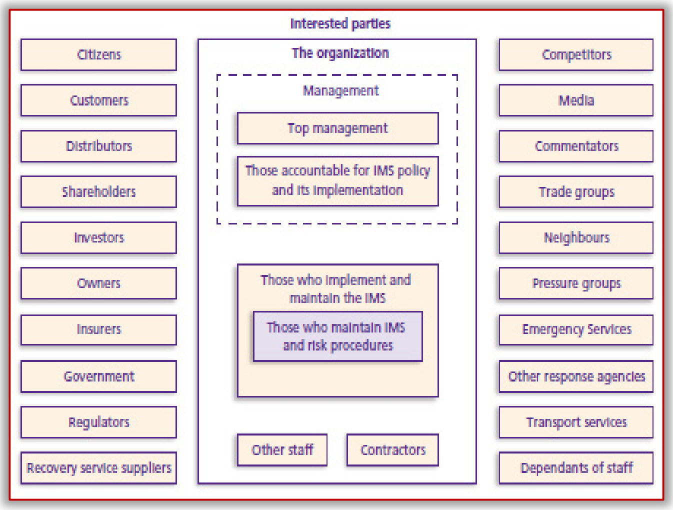

Figure 1. Stakeholders by ISO 22301 [2]

The implementation of the requirements of the standard through the delivery of the Cyber Security Program according to the requirements of the ISO/IEC 27032 standard should include at least the following units: Stakeholders, Information means (information carriers), Threats against intranet/internet space security, Roles of interested parties in information security, Guidelines for interested parties, Information security controls [4].

Requirements of the information security standard ISO 27001 in the domains [5]:

— A.5 Organizational controls, 37 control requirements
— A.6 Human controls, 8 control requirements
— A.7 Physical controls, 14 control requirements
— A.8 Technological controls, 34 control requirements (a total of 93 requirements) inevitably refer to numerous requirements for software development.

SOFTWARE AND STANDARDS FOR SOFTWARE DEVELOPMENT

According to the ISO/IEC 2382 standard, the software is "the whole or part of the programs, procedures, rules and related documentation of an information processing system". State authorities rarely use open–source operating systems and more often vendor development. Application software consists of program/code units made for a specific purpose, according to user needs. This type of software is not directly related to computer hardware, but relies on system software, especially the operating system, to perform its functionality. The need to develop application software most often arises when a state body wants to solve a problem or get a new service.

Any problem that is solved by software development can be solved in several ways. The methods differ from each other in terms of efficiency, precision, comprehensibility, usefulness, modifiability and/or other characteristics. The main goal of software development is for the software to be comprehensive, stable, understandable, easy to maintain and efficiently works for what it was created for. The development of certain software is almost never finished, but it is constantly improved according to the requirements of the market, the customer, changes in legislation, perceived deficiencies or other procedural, organizational or technological needs.

All over the world there is a large number of software manufacturers in every area of life, business of government bodies or industry when there is not only one exclusive solution for a certain area.

In order to develop quality software, it is necessary that its development is based on adopted standards (international, national, internal) and that numerous evaluations are carried out during its life cycle. The expansion of software development, in various fields, has been accompanied by the proliferation of standards, procedures, methods and tools for software development and management. Proliferation has created difficulties in managing software, especially software that is integrated into products and services. This led to the need to define a common framework for the software discipline that would help everyone who deals with software to "speak the same language" in the design, development, management and maintenance of software in their environments.

ISO/IEC IEEE 12207 Systems and software engineering – Software life cycle processes. The standard established a common framework for software life cycle processes, with well–defined terminology that the software industry can refer to. It contains processes, activities, and tasks that are applied during the acquisition, supply, development, operation, maintenance, or disposal of software systems, products, and services. These life cycles are achieved through the involvement of stakeholders, with the ultimate goal of achieving user satisfaction. The standard applies to the acquisition, supply, development, operation, maintenance, and disposal (regardless of whether it is done internally or externally within the framework of a government body) of software systems, products, and services and the software part of any system, Software includes the software part of the firmware.

There are also included aspects of the system definition needed to provide context for software products and services. This standard also provides processes that can be used to define, control and improve software life cycle processes within a government agency, department or project. The processes, activities and tasks of this document can also be applied during the procurement of systems containing software, alone or in combination with ISO/IEC/IEEE 15288, Software and systems engineering – Systems life cycle processes. This international and national standard establishes a common process description framework that describes the life cycle of human–made systems. It defines a set of processes and related terminologies from an engineering point of view. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the entire life cycle to manage and perform the systems phase of the life cycle. This is achieved through the involvement of all interested parties, with the ultimate goal of achieving user satisfaction [6].

The basic premise of the standard is that the application and practice of software engineering is a relatively young discipline comparing to traditional branches of engineering. Therefore, the control that usually accompanies traditional engineering projects is not always achievable when it comes to software. Underlying the philosophy of ISO/IEC 12207 is that aspects such as software development and maintenance must be conducted in a manner that represents engineering. The processes specified in this standard form one comprehensive set. Each organization, depending on its goals, can choose the appropriate subset to achieve the goals. The standard is designed in such a way that can be adapted to the needs of the organization, project or specific application. It can be applied in cases where the software is an independent entity or an integral part of a complex system [6].

The standard describes the architecture of software life cycle processes without specifying the way of execution of the activities and tasks that the processes contain. It does not prescribe a specific software life cycle model or method for developing software. The activities and tasks of the development process are selected and mapped into the selected life cycle model and may overlap or mutually influence each other, and be executed iteratively or recursively. ISO/IEC 12207 provides a framework in which processes, activities, and tasks can be identified, planned, and adequately responded to.

In order to ensure an easier application of the ISO/IEC 12207 standard, ISO/IEC TR 24748–3 System and software engineering – Life cycle management – Part 3: Guidelines for the application of ISO/IEC 12207 (System and software engineering – Software life cycle processes) was published. The standard explains how ISO/IEC 12207 can be used in the development of different types of software and which processes, defined by the standard, are relevant in each case. Fundamental life cycle models are also defined and supported by examples: waterfall, incremental, and evolutionary [6].

The evaluation and standardization of tools used in the process of developing information systems create the possibility that the quality of the process itself as well as the final products will be at the desired and expected level. Viewed from the perspective of complex information systems in the development and implementation of which several state authorities participate, the application of standards not only ensures the appropriate quality of the final software as a product and development process but also creates opportunities for the exchange of projects between individual state authorities, facilitates user training and creates conditions for common work on projects of representatives of various state bodies.

Analogously to living organisms, the software is considered to arise, grow, mature, and disappear, so this process is called the term "system life cycle". The life cycle of an information system based on information technologies includes several stages: planning, analysis, design, implementation, and maintenance.

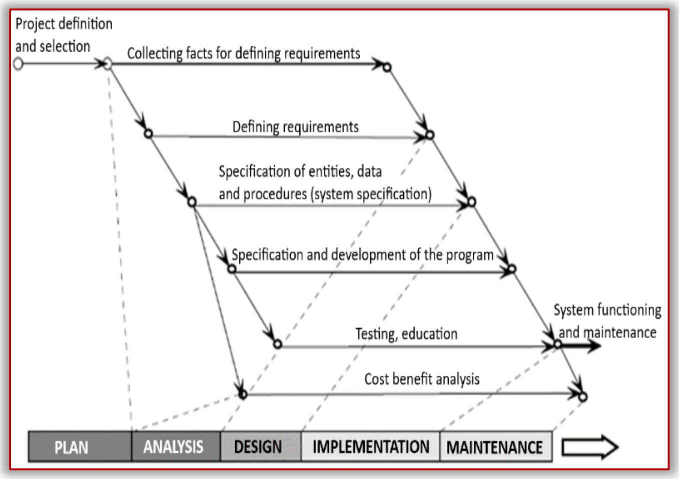
Project definition and selection
Collecting facts for defining requirements
Defining requirements
Specification of entities, data and procedures (system specification)
Specification and development of the program
System functioning and maintenance
Testing, education
Cost benefit analysis
PLAN
ANALYSIS
DESIGN
IMPLEMENTATION
MAINTENANCE

Figure 2. Presentation of software development phases based on ISO 12207 [6]

Planning the development of information systems is one of the most important and difficult functions in modern management. Information system development planning is carried out continuously in order to change things as business circumstances change.

The development planning of an organization's information resources requires the achievement of an architectural framework in which special parts of the system will be harmoniously integrated and which will enable the staged development of the information system and that various special subsystems in the organization can be branched out by various teams of people, successfully planning and rationally using the necessary and available resources. The main purpose of planning and setting up an architectural framework is to achieve information consistency [4].

Information system analysis is the second stage in the life cycle process of information system development. The analysis aims to reveal important information about three key aspects of the analysis:

- analysis and description of the object–system,
- analysis of the existing information system,
- identification of business and user information requirements.

In order to correctly evaluate the existing software of a state body, it is necessary to understand the mission, functions, structure, form, culture, climate, goals, environment and behavior of that state body.

The immediate goals of the analysis of the existing information system are an accurate description and assessment of its properties, and the main purpose is to determine the difference between the properties of the existing software and the desired properties of the newly designed and developed software, which would effectively and efficiently serve in setting and achieving the goals of the state authority for which it is developed.

The final and perhaps the most important segment of the analysis is the identification of user requirements. Users differ according to the nature of the work they perform, the positions they occupy in the structure of the state body, their cognitive and other capabilities, and therefore their functional requirements are also very different.

Investigating the content of those requests, the way and form of their presentation, time and place of delivery, frequency, volume, response time and similar are very difficult, long–term and responsible tasks of the analyst. Much of this information can be successfully found out during the execution of the planning phase however continuity is ensured and more comprehensive and deeper analysis is carried out with changed purpose.

The design of the information system should fully answer the question: how will the system enable the satisfaction of the user needs? In this phase of system development, the logical model of the new system is conceived, the model is developed and the database is designed, the process model is developed, manual and automated procedures are specified, input/output screen forms are designed, reports, printed documents, user dialogue procedures with the system, computer program specifications and program module design, control system design and many other aspects and details of design work.

System design can be defined as drawing, shaping, planning, sketching or arranging many special elements and putting them together into a powerful and unique whole. The analysis system answers the question "What does the system do?" and "What should he do?" to satisfy user requirements, while system design focuses on the key and most complex problem: how to develop the system and how it should work to satisfy those requirements. System design is a skill and a creative process of finding the best solutions and answering the question "How to do it the best?" Information system designers, by solving all these problems and key design tasks, look for possible alternative "design solutions" that will satisfy the identified information needs of the designer, in the best possible way, during the analysis phase.

The implementation of the information system is very important and in most cases, from the point of view of the end users, the key stage of development. The system can be planned, the analysis carried out, and the design conceived and implemented at an enviable expert level, but its functionality and success will depend on the way of planning and realization of its implementation. Such a plan and its implementation include many important aspects of implementation:

- preparation of implementation,
- implementation and testing of the technology,
- programming,
- testing software products,
- testing of inputs, outputs, databases, and control procedures,
- user education,
- system conversion.

Implementation is the process of complex and responsible transfer of the system from the hands and responsibilities of analysts and designers to the hands of users and operational personnel responsible for the functioning and maintenance of the information system.

Therefore, implementation includes various processes of acquisition, installation, testing, learning, conversion, documentation and its a vital step in ensuring the success of the information system of the state body.

System maintenance is the last stage in the life cycle of the development of the information system of a state body. When the system is fully implemented and put to use by the state authority and its users, the function of its operation and maintenance begins. During the life cycle of the system, numerous changes will occur; many new functional requirements will appear, old functional requirements will be modified or replaced, the real world will change, the environment of the state body, the organization of the state body itself, many technological changes will occur, which will all cause corresponding changes in the model and structure of the information system. Therefore, it is not only a matter of changing existing programs and writing new ones to satisfy new information requirements, but also the development of new versions that require and cause significant changes and modifications in the previous development phases of the system. System maintenance includes the activities of monitoring, evaluation and modification of the system, in order to satisfy desired and necessary continuous improvement.

INFORMATION SECURITY REQUIREMENTS MODEL FOR SOFTWARE

The production of software through standardized phases of the life cycle requires additional efforts in order to establish a software product with the required functionalities. In addition to the initial functionality required for the software by the state authority, which solves some procedural needs in the jurisdiction, it is necessary during all phases to establish and implement measures related to information security. Information security requirements for software are not just a favorable feeling of someone but are defined by the legislation of the state through the Law on Information Security, the Law on Protection of Personal Data, the Law on Critical Infrastructure, the Law on Electronic Services as well as through the acts in the Criminal Code of the Republic of Serbia [7]. Behind the mentioned laws there are by–laws, regulations and other legal procedural acts as well as special state bodies that control the implementation of the stated. In the vast majority of state bodies, persons who perform tasks in the field of information security have been appointed. There is no modern state body that does not use information technologies in its work. All of the above describes the necessary procedural, organizational and technological framework as a prerequisite for a functional information security management system – ISMS.

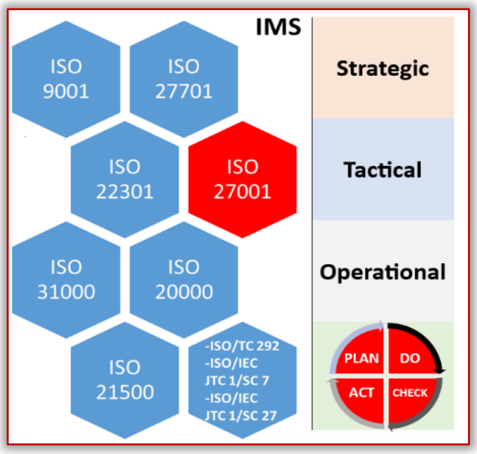

Figure 5. Information security software development matrix

The information security management system must be placed in the strategic, tactical and operational domain, during which it must be coordinated with the actions within its department, but also with other state services. The strategic, tactical, and operational domains must be implemented in the organizational, technological, and procedural framework by fully applying the PDCA – Deming cycle [8].

Table 1. Experienced recommendations for software information security [10]

ISO/TC 292 Security and resilience	ISO/IEC JTC 1/SC 7 Software and systems engineering	ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
ISO 22301 Business continuity management systems	ISO/IEC/IEEE 26511 Requirements for managers of information for users of systems, software, and services	ISO/IEC 27001 – Information security management system
ISO 22320 Emergency management	ISO/IEC/IEEE 26531 Content management for product life–cycle, user and service management documentation	ISO/IEC 18033 – Encryption algorithms
ISO 22376 Authenticity, integrity and trust for products and documents	ISO/IEC 26550 Reference model for Product Line Engineering and Management	ISO/IEC 19772 – Authenticated encryption
ISO 28000 Security management system	ISO/IEC 25000 Systems and software Quality Requirements and Evaluation	ISO/IEC 29192 – Lightweight cryptography
ISO 22341 Protective security	ISO/IEC/IEEE 12207 Software life cycle processes	ISO/IEC 15408 – Evaluation criteria for IT security
ISO 22316 Organizational resilience	ISO/IEC 33000 Family Process assessment	ISO/IEC 30111 – Vulnerability handling processes
ISO 22361 Crisis management	ISO/IEC 29155 Benchmarking	ISO/IEC 27035 Information security incident management
. . .	ISO/IEC 10746 Open Distributed Processing	ISO/IEC 27036 Cybersecurity – Supplier relationships
	ISO/IEC 19770 IT asset management	ISO/IEC 27099 Public key infrastructure
	ISO/IEC/IEEE 29119 Software testing	ISO/IEC 27701 Privacy information management
	ISO/IEC/IEEE 42010 Architecture description	ISO/IEC 29100 – Privacy framework
	. . .	ISO/IEC 29184 – Online privacy notices and consent
		. . .

Software is a technological category that has defined requirements in international and national standards of modern countries for many years. In addition to the initial requirements of the ISO 27001 standard – Information security management systems, it is necessary to pay special attention to the fact that the software is not designed to function on a desert island but in interaction with other government bodies. It is necessary to implement the following requirements:

- ISO 27701 – Privacy information management systems,
- ISO 20000 – Information technologies – Service management through the application of the well–known principles of ISO 9001 – Quality management systems with ISO 10001 – Quality management – User satisfaction,
- ISO 31000 – Risk management and ISO 21500 – Project management [8].

The above is only a basis that should be expanded, specifically for the competence of individual state bodies, with the requirements of ISO/TC 292 – Security and resilience, ISO/IEC JTC 1/SC 7 – Software and systems engineering and ISO/IEC JTC 1/SC 27 Information security, cyber security and privacy protection [10].

The above table provides guidelines for the analysis of a clear and complete definition of software in the domains of Security and resilience, Software and systems engineering and Information security, and cyber security and privacy protection, which represent indispensable members of the initial analysis of the phases of planning, analysis, design, implementation, and maintenance of the software life cycle.

CONCLUSION

It is necessary to establish an effective way of dealing with information security risks in software development, which should include a combination of multidisciplinary teams and multiple strategies, taking into account all interested parties, legal requirements, organizational knowledge and technological experience.

These strategies should include the best practices in the field of state administration with the cooperation of all interested parties (especially competent state authorities: prosecution, police, intelligence services) in order to identify and address information security and risk issues, broad education of clients and employees, providing a reliable resource for initial identification and addressing of specific risks related to intranet/internet security in state bodies with a special emphasis on software (all software in use in individual state bodies) as well as innovative technological solutions that help protect against various cyber–attacks.

The given guidelines are focused on providing best practices in government administration to help stakeholders in the intranet/internet space to understand the role of software and act preventively with the goal of playing an active role in solving information security challenges.

References

[1] Rade Dragovic, Functional recommendations for the establishment of judicial information system, ISDOS – Information system of the state bodies of Serbia, Conference Proceeding 2010

[2] Rade Dragović, Dragan Dragović, Bojan Perović, Đuro Klipa, Strategic management in the judiciary based on decision support systems, YUINFO Conference Proceeding 2013

[3] ISO 22301 – Security and resilience – Business continuity management systems – Requirements, International Organization for Standardization

[4] Zvonimir Ivanović, Rade Dragović, Sergej Uljanov, Strategic regulation model on the high–tech crime vulnerable targets, Western Balkans: from stabilization to integration, International Scientific Conference, Conference Proceeding 2011

[5] ISO/IEC 27001 – Security standard information, cyber security and privacy protection – Information security management systems – Requirements, International Organization for Standardization

[6] ISO 12207 – Systems and software engineering – Software life cycle processes, International Organization for Standardization

[7] Rade Dragovic, Vladimir Kačanovski, Bojan Perovic, Security policy in judicial information system, YUINFO Conference Proceeding 2011

[8] Rade Dragović, Ivan Peljević, Đuro Klipa, Implementation strategy for cryptographic protection in ejudiciary, INFOFEST Conference Proceeding 2012

[9] Rade Dragović, Bojan Perović, Security policy and recommendations for increasing security database in the justice information system, BISEC Conference Proceeding 2012

[10] Internet source: International Organization for Standardization, website: www.iso.org

[11] Rade Dragović, Bojan Perović, Ljubiša Pešić, Enver Nuhović, Đuro Klipa, Recommendations for improving security databases in the judicial information system, YUINFO Conference Proceeding 2012

[12] Rade Dragović, Miodrag Ivković, Bojan Perović, Đuro Klipa, Dataveillance and data mining as a technology support to the process of investigation, TELFOR Conference Proceeding 2011, IEEE conference

[13] Vojkan Nikolić, Rade Dragović, interoperability and security of egovernment of Republic of Serbia, TELFOR Conference Proceeding 2014, IEEE conference

Note: This paper was presented at IIZS 2023 – The XIII International Conference on Industrial Engineering and Environmental Protection, organized by Department of Mechanical Engineering and Department of Environmental Protection of the Technical Faculty "Mihajlo Pupin" Zrenjanin, from the University of Novi Sad, in cooperation with partners – University Politehnica Timisoara, Faculty of Engineering, Hunedoara (ROMANIA), University "St. Kliment Ohridski", Technical Faculty, Bitola (MACEDONIA), "Aurel Vlaicu" University of Arad, Faculty Of Engineering, Arad (ROMANIA), University of East Sarajevo, Faculty of Mechanical Engineering East Sarajevo, Sarajevo (BOSNIA & HERZEGOVINA) and University of Giresun, Faculty of Engineering, Giresun (TURKEY) – in Zrenjanin, SERBIA, in 05–06 October, 2023.

ISSN: 2067-3809