**POLITEHNICA UNIVERSITY OF BUCHAREST**

**Doctoral School of Industrial Engineering and Robotics**

**Decision No. ___/___.__________**

# DOCTORAL THESIS
## - SUMMARY

---

RESEARCH AND CONTRIBUTIONS ON THE IMPLEMENTATION OF QUALITY-RISK SYSTEMS IN ORDER TO ENSURE INFORMATION SECURITY IN PUBLIC INSTITUTIONS

---

**Doctoral supervisor:** Prof. univ. em. dr. ing. ec. Constantin MILITARU

**Autor:** Adrian-Viorel Dragomir

THE DOCTORAL COMMITTEE

| | | | |
|---|---|---|---|
| President | Prof.univ.dr.ing. Nicolae Ionescu | from | Politehnica University of Bucharest |
| Doctoral supervisor | Prof.univ.em.dr.ing.ec. Constantin MILITARU | from | Politehnica University of Bucharest |
| Reviewer | Conf.univ.dr.ing.mat. Ovidiu BLAJINĂ | from | Politehnica University of Bucharest |
| Reviewer | Prof.univ.dr.ing.mat. Adriana Alexandru | from | National Institute of research and development in computer science |
| Reviewer | Conf.univ.dr. Răzvan Grigoras | from | National Academy of Information Bucharest |

**BUCHAREST**
**2022**

# THANKS

In this way I would like to express my full gratitude and to thank Professor em. dr. eng., ec. Constantin Militaru for the entire support offered during the drafting of the doctoral thesis and intermediate scientific reports. The entire research was carried out under the direct guidance of the professor, who guided my steps through all the steps that this approach involved and supported my decision to approach such an interesting field, such as information security management systems in the context of their implementation within public institutions.

I thank my family and especially my wife, children, friends and collaborators for their patience and trust, which helped me to carry out such a sustained activity.

I would like to thank the management of the "Faculty of Industrial Engineering and Robotics" of the "Politehnica University of Bucharest" for the efforts made to continuously improve the quality of the educational process, which I found here during my doctoral studies, both from a logistical and operational point of view, as well as from the point of view of the high level of quality of formal education, which was a real support for me throughout the doctoral internship.

I also thank the heads of the public institutions in which I have spent twelve years my professional activity and the heads of IT departments and information technology of which I have been honored, thanks to which I have accumulated consistent information in this complex but interesting and equally competitive system, but that offers a lot of professional satisfaction when you look at what you left behind.

The experience gained during the years of activity in the field addressed in this paper in public institutions, helped me to understand in depth the importance of information security and to realize that in order to ensure a security climate it is not enough to spend public funds on complex systems or programs, it requires security measures and procedures that regulate all internal processes in order to implement, test and maintain technical and operational information security measures within the institution.

The entire research activity carried out during the PhD I was able to materialize it with the support of colleagues and collaborators in the IT&C field and on this occasion, I want to be grateful for the information provided and their full support.

# CONTENTS

# INTRODUCTION

Around four billion people use the Internet daily in the context of the explosion of the Internet of things (IoT) concept, which is the connection to the Internet of increasingly complex equipment, IT&C, home appliances, social networks, blogs, etc. Digital platforms, all of which are tools that through connection to the Internet allow the generation of content by the user.

National security is the foundation of the normal functioning of any society, where citizens can have optimal living and working conditions by protecting against risks, hazards, and security threats. It can be said that security is a good that the whole people must benefit from, and therefore all countries must ensure the conditions of normal life for their citizens.

Global security risks require changing methods of identifying, managing and combating security risks and hazards, from the individual level to the national and regional level. In the era of globalization, security threats have taken on a cross-border basis, and governments are forced to find smart and innovative solutions whenever they face a problem that has the potential to affect national stability and security.

A few decades ago, national security was defined by a single component, namely military, but nowadays this concept has taken on multidimensional valences, the most important being economic, social, human, political, diplomatic, energy and environmental. It can be observed at national level the preservation of the main governmental objectives in terms of quality-risk management in this area, namely, the increase of the level of security, the minimization of information security risks and threats at the level of the public administration, taking into account that Romanian public institutions continue the development and modernization processes in order to align with the European Union standards.

At the level of our country, the information paradigm has changed a lot in the last 3 decades, starting to use mainly information technology in most fields of activity and especially in the governmental environment. The information, which until then had paper as its support, began to turn into electronic format. Thus, in recent years, information infrastructures have developed significantly, leading to the global interconnection that has also attracted the risks specific to digitalization.

Regardless of the name of the approach chosen, it is always important to identify and raise awareness of threats to information security, which can exist at the level of each country, to consistently select, implement and maintain policies, strategies, adequate information security processes and measures, both at the level of state and private institutions.

In the 5 chapters of the doctoral thesis is conducted a study on the current trends in the implementation of information security management systems within public institutions with the aim of increasing the degree of information security in these entities.

# CHAPTER 1
# THE CURRENT STATE OF INFORMATION SECURITY RESEARCH

## 1.1.THE ROLE AND PLACE OF INFORMATION SECURITY AT THE CONCEPTUAL LEVEL

In Chapter I we conducted an analysis of the current situation regarding information security through quality-risk management at national, European and international level.

For the purposes of this research, the information will be defined and used from the perspective of the concept of security in general and information security in particular, the definition of which is found in Article 15 letter a) of Law no. 182/2002 on the protection of classified information, chapter General provisions – definitions, respectively "information – any documents, data, objects, or activities, regardless of the support, form, a way of expressing or circulating." […] [1]

The information is at the basis of national security and the elaboration of documents specific to information is managed through the information systems, which are found in the architecture of all the state management bodies.

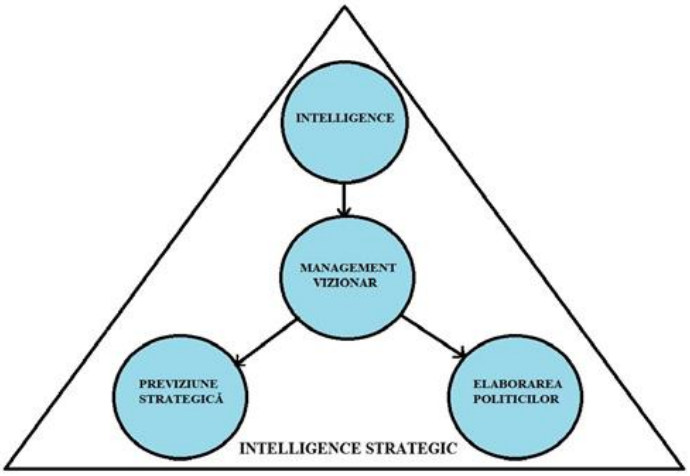


*Fig. 1.1. Principles underlying the concept of strategic intelligence (author proposal)*

### *1.1.1.Delimitation of the coverage area of information security in the online environment*

Online information vulnerability is a flaw in an information management system that can leave doors open to attack and can refer to any kind of weakness of an information system. a set of procedures or in any context that exposes information security to any type of threat.

Online information vulnerabilities are defined as neuralgic points or weaknesses that creep into the design or building of hardware, software, information networks or security procedures through which information is managed. In short, "vulnerability is a weakness that allows for unauthorized action."[2]

The system is one of the basic concepts when it comes to information, but it is often used in many fields of science as well. Being a very common primary concept, it has not been defined very strictly, in a generally accepted way, but by describing its main characteristics, the concept can be understood in an intuitive way.

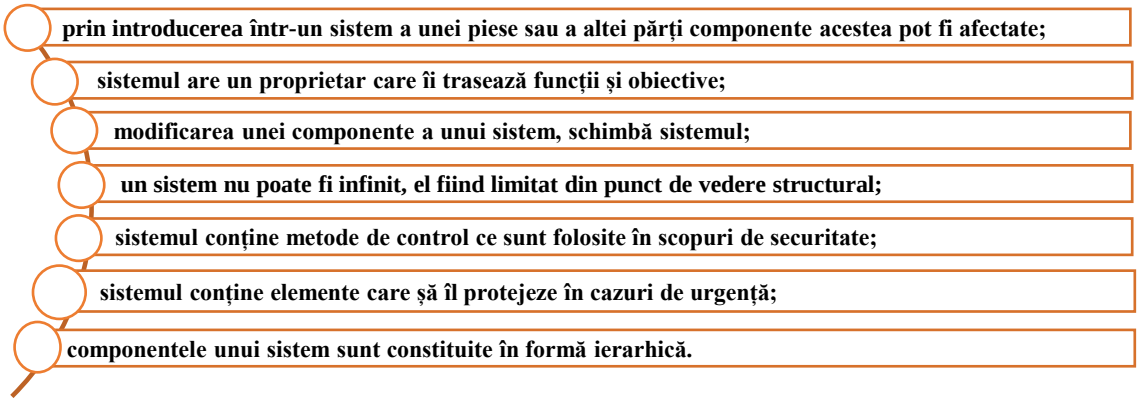


*Fig. 1.2. Main features of the systems (author proposal)*

The objectives of a security system can be determined by analyzing in detail the objectives of the system in general for which security must be ensured and how it interacts with the online environment to achieve the purpose for which it was created. Any information system that is connected in the virtual environment needs security, which justifies the common objectives of the two types of systems.

***1.1.2. Analysis of technical and legal aspects of cyberspace***

Cyberspace or cyberspace is defined by any human interaction with the online environment that has become a habit for a large part of the population. Cyberspace can also be characterized by a universal presence in most aspects of everyday life that can take place in the online environment.

One of the most important components of cyberspace is **the Internet**, the network through which most other networks interconnect, which can have different types or structures, be public or private and managed in almost all countries of the world.

Cyber threats have become daily and common impediments in our lives, and most specialists already talk about this scourge as being similar to a cyber war, the best example of which is the United States of America, which, in the United States of America, is the most common threat to our lives. for a long time, it has framed specific legislation for cyber-attacks among terrorist attacks.

***1.1.3.Some aspects of malicious exploitation of cyberspace***

In the current context characterized by major security vulnerabilities, information has become an invaluable value for any entity, being perhaps outclassed only by human resources. Every aspect of society is influenced by the online environment, as most infrastructures are interconnected. By this statement we do not support the hypothesis that all aspects of life are directly related to the online environment, but that any individual or entity, whether active or not in the virtual environment, can be affected by this aspect.

From the perspective of any type of entity, public or private, information is a commodity of great price, which has imposed information security as an activity of particular importance for them, whether they conduct electronic business or serve the interest of the general public.

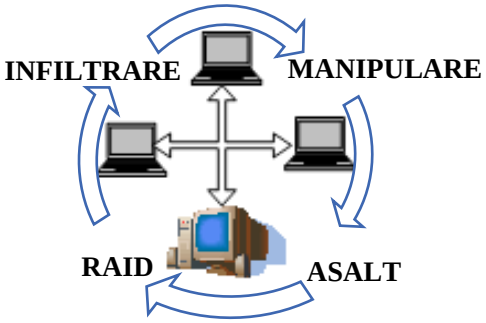


*Figure 1.4. Sequences of an attack on information from information networks (author proposal)*

Information security plays a basic role in information systems security management, its importance being taken into account more and more recently, after seeing the negative experiences of website owners who did not strengthen their cyber security and had problems due to the exploitation of vulnerabilities by hackers, the result is reputational damage and large financial losses. public or private entities

## 1.2. RESEARCH ON INFORMATION SECURITY

**Over time , information technology** has seen a rapid development, and advances in the field have attracted the implementation of these technologies in all societal areas. Today, the existence and functioning of human society is closely linked to information technology, if not dependent on the normal functioning of information infrastructures in certain critical sectors.

Cyberattacks aimed at stealing information as a threat to global security are presented in close connection with organized crime, illicit trafficking and terrorist attacks. The causes of attacks on information networks may have financial reasons, namely the financing of organized crime and terrorism activities, or to facilitate the occurrence of these types of attacks, here referring to terrorist attacks that occur in correlation with the exploitation of vulnerabilities of the systems through which information is managed.

Information technologies used for the purposes for which they were originally designed, respecting information integrity and security and general principles of good conduct, such as responsibility, vigilance and respect for others, are models to be followed in terms of maintaining security and a safe climate.

Cyberspace is the medium that hosts most of the information nowadays and is synonymous with terms such as "virtual reality, online environment, digital space, which together make up a conceptual apparatus". [3]

### *1.2.1.Methods to ensure information security in the online environment*

The importance of information security derives from the fact that today, most confidential or classified information such as information on a state's defense systems and their basic elements, manufacturing technologies, military personnel and devices, data relating to communications systems, maps, data relating to electricity supply, water, gas, scientific, technological data, they are stored on computer infrastructure.

In order to ensure information security and improve policies on the fight against information crime, the European Parliament and the European Commission have created strategies and legislation to address this scourge of the 21st century. The European Parliament adopted Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of network and information security in the Union in 2016, also known as the NIS Directive.

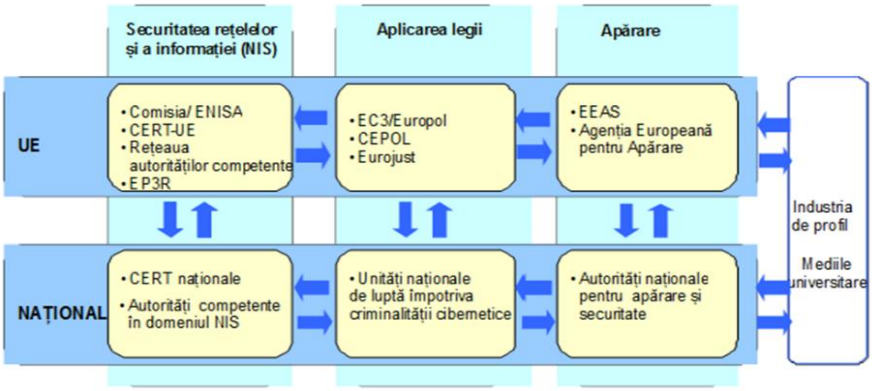


*Fig. 1.6. Main pillars of the NIS Directive (source: European Union Cybersecurity Agency-ENISA)*

### *1.2.2.The importance of ensuring the security of communications networks to protect information*

The information network is an interconnected group of processing equipment, switching equipment and interconnecting branches, and ensuring the security of a communications network is done both through physical protection and information protection.

It should be noted that a network does not need to be connected to the Internet to operate, on the contrary, today important networks are not connected to the Internet in order not to be vulnerable to attacks coming from the Internet area.

Information network security is the branch "responsible for the design, implementation and operation of networks so that information security achieves its purpose, in an interconnected network at the organizational level, between organizations and between organizations and users". [4]

### *1.2.3.Security of information on the Internet*

Internet security refers to "the protection of Internet-related services and information communication technology systems, as an extension of network security in organizations and at home, in order to achieve the purpose of security." [5]

Every person or entity wants to feel safe when browsing the Internet, from all points of view, from personal, financial, informational to that of their image in the public area.

Internet security is the activity responsible for the operation, availability and reliability of services accessed through the Internet. Internet security differs from internal network security mainly for quantitative reasons, in that the Internet accounts for billions of users, while an internal network can have a much smaller number of users.

### *1.2.4.The security of the technology through which information is managed*

The definition of this information security component comes from the English language - information communications technology security - and refers to the surveillance of the security of the equipment or programs through which information is processed, stored or transmitted, as well as the way these devices or software are manufactured, so that they comply with information security standards.

Cyberattacks are often used to access the flow of information about technology or design plans in various fields, from military technology to civil industry, to disrupt or disrupt the normal operation of infrastructure. to stop the communication and transmission of public messages and to influence decision-making processes.

## 1.3.RESEARCH ON INFORMATION SECURITY MANAGED BY CRITICAL INFRASTRUCTURES

The power of a state is always relative, it cannot be accurately established, it is evaluated according to the power of national institutions, the level of the state's financial reserves and the purchasing power of the citizens of the country, but at the same time it must be stated that the basis of power lies information. The power of a state is made up of a series of elements of national institutions, elements identified by Hans Morgenthau in his book "politics among Nations – the struggle for Power and Peace". [6]

The critical infrastructures of any state need to ensure a strong security environment that has as its stated purpose the protection of information that is owned or operated by them. The security of critical infrastructures must be ensured by the entities designated for this purpose by the competent authorities of the State.

In 2010 Romania implemented the EU provisions on the protection of critical infrastructures, by transposing the provisions of the "European Directive no. 2008/114/EC of the Council into the national legislation", which was achieved by the adoption at the level of the Romanian Government of the "Emergency Ordinance no. 98 of 2010 on identification, 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

The elements underlying the national power of the Romanian state are: Population, information, positioning on the geo-political map, natural riches, characteristics of the people, level of government, nations morale, economic capacity and level of endowment and training of the army.

When referring to critical national infrastructure, we must bear in mind that it is an essential condition of life, the stability and functioning of critical infrastructure can decisively influence any other social or economic activity. In all the military conflicts that have occurred in history, critical infrastructures have been the first to be targeted by attacks, but in the 21st century the risk of critical infrastructure attack has shifted to the virtual dimension, and there is no need for their physical destruction.

## 1.4.TYPES OF INFORMATION SYSTEMS ATTACKERS AND PURPOSES PURSUED

In the literature we have identified six categories of information system attackers, defined according to the objectives of the attacks and what motivates them to attack, as follows: The hacker, the spy, the terrorist, the economic attacker, the professional criminal and the vandal.[7]

Cybercriminals are generally referred to as hackers and are "those individuals who attempt to illegally gain control of a security system, computer or network in order to gain access to confidential information or material advantage."[8] Interestingly, the term hacker originally did not always have a negative connotation, referring to the beginnings of the technological era as "developer or user."[9]

When we look at the purposes of cyberattacks, we see that attacks aimed at economic and political espionage are usually associated with States, and criminal and terrorist attacks are linked to non-state actors.

Intelligence espionage, and we refer here mainly to commercial espionage, where the attacks are directed at large companies and corporations, is aimed at "obtaining by illegitimate means or the unlawful disclosure, transfer and use, or without any other legal justification, of a trade or industrial secret, with the intention of causing economic harm to the person who has the right to secrecy or of obtaining for himself or for a third party unlawful economic advantage." [10]

Information warfare is considered to be the next type of war of our century, attacks on information being extremely effective in the event of such a conflict, causing panic and destruction and facilitating the superiority of the attacker.

Electronic espionage filters information by focusing exclusively on important targets, the information obtained being exactly what you want. In classical espionage, when the source of the leak is detected, the agent or network is detected and interrogated, and their belonging to a country can be found, triggering a diplomatic scandal between the two countries involved. In contrast, electronic espionage, even if detected, cannot accurately state the country responsible, removing from the outset such accusations of espionage, which they can declare unfounded for lack of incriminating evidence.

Information crime is an international problem simply because the majority of online attacks have people outside borders as perpetrators, which derives from the characteristics of virtual space, a borderless space. Therefore, the State in which the incident occurred is unable

to detect and hold the person responsible. “Legislation valid in all countries of the world” is needed[11] in order to be able to effectively combat such attacks.

## 1.5. PRINCIPLES OF THE INFORMATION SECURITY STRATEGY IN THE EUROPEAN UNION

Both the Internet and the entire virtual space have lately had a defining influence on most of the vital components of society. Everyday life, fundamental human rights, social interaction and the finances of every person depend to a large extent on information and communication technology and its permanent functioning, because failures or non-functioning of these systems can create imbalances in society, or even disasters.

The rule of law and human rights must be protected in cyberspace equally by EU Member States and by entities with legal powers to protect them, whether state or private. The freedoms and well-being of every citizen are intrinsically linked to the existence of a protected and progressive Internet, which can have these qualities if private companies in this field constantly bring innovations to be supported by civil society, so that it continues to grow.

Information and communication technology, with its massive development, has been transformed into the main means of economic growth and the main resource for the development of different sectors of the economy. ICT is currently the foundation for supporting all complex information systems, through which national economies operate optimally in key sectors and critical infrastructures such as energy, finance, health and transport.

The European Cybersecurity Strategy, in force since 2013, sets out the principles guiding cybersecurity policies in Member States and in their relationship with other countries at international level. According to this strategic document, fundamental European values must be applied in the material environment in equal measure with the virtual one.

The EU vision in the Cyber Security Strategy is articulated on five main priorities, addressing a number of information security challenges that we detail below and mention in Figure 1.11:

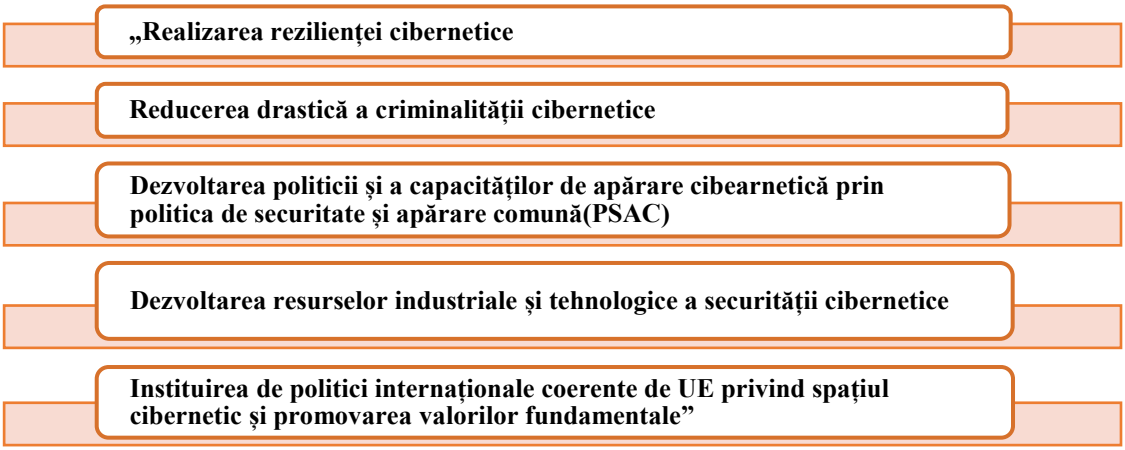


*Fig. 1.11. EU strategic priorities for cybersecurity (source: European cybersecurity strategy [12])*

In December 2020, the European Commission published for approval a new enhanced version of the European Union’s Cyber Security Strategy that will significantly modify the provisions of the Strategy in force since 2016. and member states will have to adopt measures to implement the new information security concepts contained in the new variant.

The aim of the new European Cybersecurity Strategy is to strengthen the cooperation relations of government security entities with non-governmental organizations and academia, integrate all existing coordination centers to cooperate and take actions to strengthen knowledge of information security risks through incentive plans and collaboration between military-civilian and public-private environments.

## 1.6. VULNERABILITIES OF INFORMATION IN THE ONLINE ENVIRONMENT AND WAYS OF REMEDIATING

In recent decades, society has increasingly used electronic information, a way that has gained more and more ground because the world needs information in motion and in real time. Today, there is a lot of sensitive, confidential or secret information that is processed, transferred or stored in the electronic environment that needs to be protected from malevolent.

Most entities, whether governmental or private, carry out their daily activities with the help of information technology, and its failure or modification of their data may involve serious financial or reputational damage. Vulnerabilities that can occur in an information network can be of several types, as follows: a) target fingerprinting information, b) malicious codes, c) denial of service, d) compromise of accounts, e) access through attempted penetration, f) unauthorized access to information, g) unlawful changes of information, h) unauthorized access to communication systems, i) Spam.

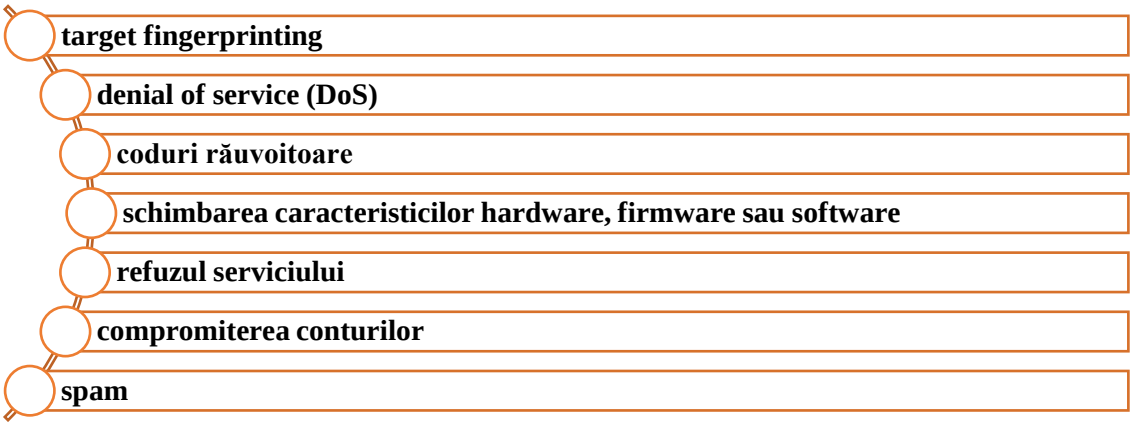


*Fig. 1.12. Vulnerabilities of information in the online environment (author proposal)*

The computer Emergency response team (CERT) was created to solve these problems.

### *1.6.1. The CERT Community and specific actions in the field of information security*

A group of experts responsible for responding to information security incidents is called the computer Emergency response team (CERT). These entities are also referred to as the computer Security incident response team (CSIRT), with the two names representing largely the same type of entity, differences between the two being minor. The term CERT has been registered in the register of registered trademarks, thus being protected by copyright laws. [13]

The primary responsibilities of a CERT/CSIRT are proactive and reactive actions to protect the security of an organization's information. THE CPTS cannot have similar or standardized responsibilities, as each team carries out activities according to the needs identified at the level of each client. The technical objectives of a CERT must be aligned with the general and specific objectives of organizations benefiting from security services, whatever the type of services they choose in the multitude of this field.

### *1.6.2. Theoretical aspects of information security audit*

Information systems auditing is a process by which a team of experts in the field make an independent and objective analysis of the level of security of an information system. These activities must be carried out in compliance with the rules and objectives imposed by universally accepted auditing standards in this area.

At the same time, very well-defined audit objectives**,** such as compliance with certain information security management systems, or simply the analysis of the protection afforded to the information system by means of a protection device, must be established, an example of this is the audit of firewall equipment within an information system.

Risk-based information security audit is completer and more effective for the management of the organization than a classic system audit, which only performs a multi-criteria X-ray of the organization. Because of the importance of information to any type of entity, public or private, the assessment of information security risks should be considered as an objective of strategic importance and management should continuously update these assessments and check security controls.

### *1.6.3. Analysis of general aspects of information security risk management*

The field of information security risk analysis is a current concern of all entities that have created a purpose of protecting security, optimizing their operation in terms of risk management helps them to increase their level of performance.

The risk definitions we have identified during the bibliographic research focus on threat management as a combination of the probability of an event and its consequences, and the response techniques that are generally used to treat them are based on the negative risk characteristic. Of these definitions we mention the one given in the "Explanatory Dictionary of the Romanian language", respectively, "the possibility of reaching a danger, of facing a trouble or of facing a damage, a possible danger"[14] and the one in the "Dictionary of Ergonomics", where risk can also be understood to mean the possibility of obtaining a gain, namely, "a measure of a possible inconsistency between the possible outcomes – favorable or unfavorable – and those envisaged in a future action subject to the influence of random factors". [15]

In the digital age, both public and private entities use information systems to manage information, and security risk management is one of the main ways of protecting the information of organizations and implicitly their basic activity, from the security risks related to information systems.

"To ensure some uniformity in the way risk management is managed, there are a number of standards applicable at the level of any organization, regardless of the field of activity or type of risk, including:

- ISO 31000:2010 – "Risk Management. Principles and guidelines";
- SR EN 31010:2010 – "Risk Management. Risk assessment techniques;
- ISO 73:2010 – "Risk Management. Vocabulary."
- SR BS 31100:2013 – "Risk Management. Code of practice and guidance for the implementation of SR ISO 31000" [16].

In order to detail as suggestively as possible, the functions of information security risk management, we present in the following graphic form in Figure 1.15 the process of carrying out the activities to be undertaken for implementation:

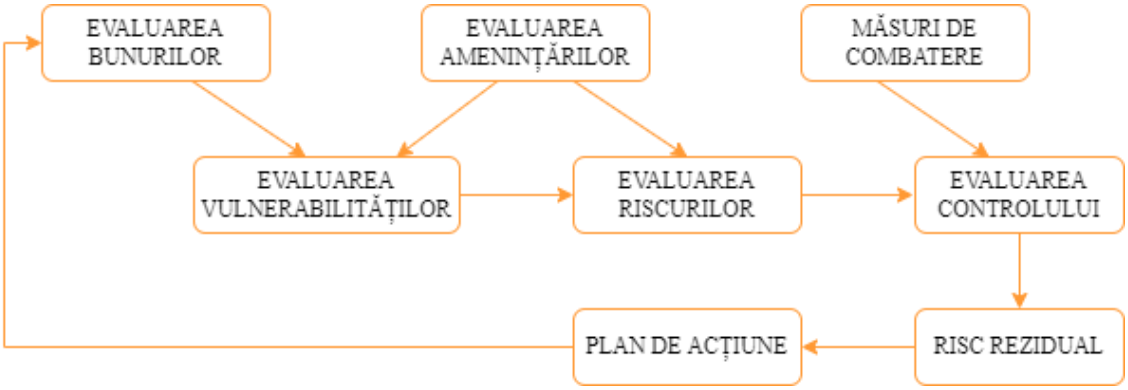


*Fig. 1.15. The process of achieving security risk management (proposal author)*

Among established risk management models, which can be implemented both in state institutions, in university and in private entities, because it contains complete ways of assessing security risks in terms of the methodology used or the scope of application, we chose for the study one of the most established and complete risk management models, namely the one described in **the NIST standard 800-37** of the US Department of Commerce.[17]

In Figure 1.16 below we present the link between risk assessments based on threat analysis and vulnerability assessments within a risk management system model described in NIST Standard 800-37:

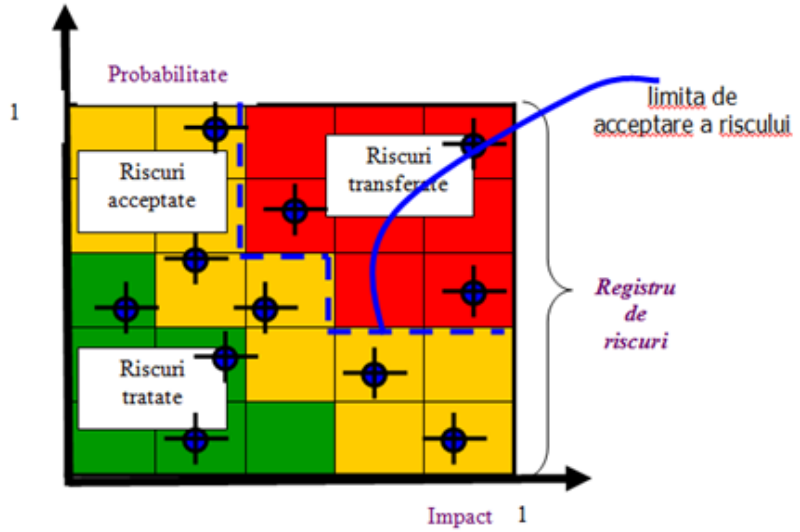


*Fig. 1.16. Risk matrix (source: NIST standard 800-37 )*

### *1.6.4.Dimensions of security education to reduce human errors related to information security*

Ensuring information security is impossible in the context of a precarious general security culture or a lack of sustained and continuous security education. If, in the case of security culture, we are dealing with a combination of preconditions and circumstances related to the social, cultural and historical factors that will have manifested at national or regional level, security education must be an objective in constant attention for all governmental organizations, defense and national security, but also for other types of state or private organizations.

Thus, the management of these organizations must provide regular training to all users on their obligations with regard to information security before allowing them access to it.

These trainings must certify that employees have understood and have sound skills in enforcing security rules and that they must seek advice and help with any issues that may have connotations to the security of the information they exploit.

Within the framework of an organizations information security policies, it is necessary to provide for a special section dedicated to security education, which should include complete and detailed requirements on the program of knowledge and protection of information security within the organization. This section shall include, inter alia:

- roles and responsibilities;
- programmatic elements for the development of information security education;
- measures to implement the information security education program;
- how to update this plan and measure its effects.

**However, information security education** cannot be addressed only at the level of training programs and responsibilities of the personnel involved in the exploitation of information resources, but also on the level of psycho-social mechanisms and concepts applied to their users. The best argument for this approach is social engineering, very often used by attackers to overcome security barriers installed by information system administrators. [18]

Thus, training and education in the field of information security is transformed into an important goal, which must be achieved at the level of any entity and any employee, regardless of the level at which they operate at a certain point in their career.

## 1.7. ACTIVITIES THAT LEAD TO INFORMATION RESILIENCE

The vital role that information security plays in protecting information privacy stands out more than ever in these times, as critical infrastructures increasingly need to manage their information online, making them vulnerable to digital attacks.

Information resilience can be defined as "the ability to resist despite threats to information infrastructure and communication infrastructure." Analyzing critical functions and infrastructure we can see their dependence on the proper functioning of cyber systems, whose vulnerabilities have been analyzed and mitigated through security policies and procedures of international standards, and based on the risks and threats inventoried within the entities, steps can be taken to improve resilience. [19]

The improvement of information resilience is achieved through the mechanisms of prevention, detection, mitigation and recovery[20], established at the technical and decision-making level of an entity card, as illustrated in Figure 1.18, in such a way that the information infrastructure is able to maintain its ability to operate during or after an attack:


*Fig. 1.18. Information resilience (author proposal)*

In the current context characterized by hybrid threats to information security, it is of interest to remember that public institutions must focus on the human side of information security by implementing technical controls, this activity being the defining activity for ensuring security. This aspect is often forgotten by the management of institutions, which leads to a lack of awareness of employees and a poor general culture of information security.

From a theoretical perspective, in order to ensure information security in the online environment, public institutions must comply with security policies and operational procedures in order to be resilient. In the following, we will present some important aspects to be pursued by these entities, in order to reduce the risks that can affect the security [21]:

a) the exchange of security information
b) information provision;
c) the workforce specialized in information security;
d) self-defense of information security;
e) the information security supply chain;
f) cross-border information security;
g) awareness, education and training;

Public institutions must have measures aimed at their own employees, their awareness of the risks of a cyber-attack against the information they manage and their negative consequences. Equally, measures are being taken to educate employees and train them in computer use, especially on the Internet, so that they are not exposed and vulnerable.

Prevention aims to reduce cyber dependence and reduce vulnerabilities of information systems. It should be noted that all these activities that are carried out with the aim of preventing, are planned and thought out in advance by implementing operational information security policies and procedures to take place before a cyber-attack occurs

**Information security policies** will also include ways to mitigate attacks, which is related to developing a resilience capability against attacks on public institutions information.

Plus, the value of the implementation of information security management systems at the level of public institutions is generated by the previous experiences of experts from other similar entities and those who participated in the thinking of these management systems regarding the protection of information systems or methodological ones through which manage or store information.

Through the implementation of an information security management system, complete information security strategies and policies can be developed and adapted to the current needs, which can include in addition to methodological norms and the specific roles of each expert involved in the implementation of the system, responsibilities and relationships between all experts who have responsibilities in protecting these systems.

# CHAPTER 2
# OBJECTIVES OF THE DOCTORAL THESIS

## 2.1. PRELIMINARY CONCLUSIONS FOLLOWING THE BIBLIOGRAPHIC RESEARCH OF THE TOPIC OF THE DOCTORAL THESIS

During the bibliographic research carried out within the doctoral thesis I have deepened the opinions of authors of books and scientific articles on the same topic and for this purpose I used qualitative methods that consisted in the analysis of comparative studies and case studies identified in the studied bibliography and quantitative methods that they were used to verify the hypotheses identified in qualitative research.

The main hypothesis from which this research started, as a result of the critical approach of the specialized literature in the field and the assimilation of the present level of research, but also based on the practical knowledge of the information security phenomenon, is: the implementation of information security management systems, together with risk management systems and other technical measures to ensure security, can contribute to the efficiency of the state institutions response to current threats regarding information security.

The implementation of an information security management system within public institutions involves the implementation of security policies necessary to achieve the specific objectives of the information security field, which must comply with the norms of the international standards in force and the legal requirements applicable to the activity they carry out. An important component of the ISMS is the training/education of civil servants in terms of maintaining a security climate by observing the security measures adopted by the management of the institutions where they are implemented.

## 2.2. DELIMITATION OF THE RESEARCH AREA

Following the bibliographic research, I concluded that in the case of state entities, to ensure an adequate response to the risk factors that can affect the state of information security is not enough only the purchase and installation of information security equipment and / or software, but also policies, measures, operational security rules and procedures and training and awareness-raising activities of personnel/users about security threats. These security tools can be implemented through an information security management system, through which the general framework can be created and provide the premises for maintaining the security state of the information.

We believe that it is necessary for an information security management system, implemented at the level of a public institution, to be audited by a third-party entity that ensures the management that it is well implemented and treats as large a range of risks as possible. Such an audit must be done by an entity accredited by internationally recognized standardization authorities in order to have the necessary expertise in quality certification of the management system that has been implemented.

Due to the complexity and sensitivity of this area and in order to ensure the compliance of the management system, it has been found necessary to ensure that after the implementation of the ISMS it is viable and well-tailored to the security needs of the entity, this is made possible by certification of the management system based on the requirements and conditions of an internationally recognized standard. Following the bibliographic research, we found that the most suitable standard for certification of an ISMS implemented in public institutions is SR/EN ISO/IEC 27001:2018.

## 2.3.OBJECTIVES OF SCIENTIFIC RESEARCH WITHIN THE DOCTORAL THESIS THEME

Following the bibliographic research carried out within the doctoral thesis, starting from the main hypothesis of the research, outlined on the positive impact that information security management systems can have on the level of information security within public institutions, the main objective of the doctoral thesis is profiled from which the corresponding specific objectives derive, which we present in the following.

The main objective is to identify the best methods and examples of good practices for implementing an information security management system and to certify it according to an internationally recognized standard within public institutions.

The aim of this approach is to increase the security of information and reduce the risks in this area.

In order to achieve this main objective, we propose to approach theoretical and practical aspects, less developed and tested at the level of public entities, by which to treat the particularities of implementing the ISMS in this type of organization, which is of major importance for the field investigated.

The specific objectives we propose to achieve the main objective and confirm the hypothesis are divided into:

**1. Theoretical objectives of the doctoral thesis**:

- ❖ theoretical and comparative-critical analysis of the current state of research on information security;
- ❖ establishing the role and importance of information security in public institutions;
- ❖ research on methods, ways and systems to ensure information security at the level of public institutions;
- ❖ Theoretical analysis of information security management systems and their certification according to the international standard SR EN ISO/IEC 27001:2018
- ❖ Identifying the particularities of the applicability of the ISMS in the context of implementation in state institutions;

**2. Practical objectives of the doctoral thesis:**

- ❖ Designing a model of practical implementation of the ISMS and its certification according to the international standard SR EN ISO/IEC 27001:2018 at the level of the Permanent Electoral Authority in Romania;
- ❖ Propose a set of measures that may form part of the security policy to be adopted under the ESM of the EPAs;
- ❖ Establish the procedures, documents and policies to be adopted by the EDA under the ISMS;
- ❖ Identification of information security risks at the level of the AEP in order to deal with them;
- ❖ Proposal of the action plan for the implementation of the ISMS at the level of the EDA containing the phases the terms of implementation, the responsible and deliverable.

As part of the analysis model that we will present in detail in the chapter that will contain practical contributions to the implementation of the ISMS, we will present a number of tangible security objectives, documents and operational security procedures, which will be designed to treat or cover as much as possible the information security risks to which the institution is exposed, in order to fulfill its specific tasks and increase the prestige of the EPAs at all levels of representation.

# CHAPTER 3

# RESEARCH AND THEORETICAL CONTRIBUTIONS ON THE IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS ACCORDING TO ISO/IEC 27001:2018 AT THE LEVEL OF PUBLIC INSTITUTIONS

The information age has the same effect on humanity as the discovery of basic materials, so useful to people like oil, fire and iron. This effect increases exponentially with the development of technology and the possibility of easy access to information in multiple ways. In this dynamic environment, the development of information security activities, in order to keep them in good conditions and with as few risks as possible, requires the existence of a functional information system, kept up to date from a technological point of view and protected against security threats.

When we look at the reputational or social cost/benefit balance of public institutions, we can say that investing in better security of information protection equipment and networks generates high costs, which institutions often do not afford, and the social benefits that are not directly and adequately reflected in their overall image to the general public.

Therefore, there is a need for other types of security measures to be adopted at the level of public institutions, in addition to implementing operational information security solutions, through information security management systems.

The implementation of a well-structured information security management system (ISMS), designed in accordance with international standards, can underpin an appropriate security strategy, especially at a time when threats and information security in general, these are prevalent issues that any type of public or private entity is facing.

An important aspect of information security is the establishment of the security policy, which is the document that specifies information security measures and which must be subject to reviews and assessments at certain clear deadlines.

In order to be able to ensure that the ISMS has been well implemented and provides the premises for information security, it must be verified, audited and certified according to a globally recognized standard in this field, The EC sets out the general framework to ensure that ISMS meets the highest quality standards. Thus, during the research we analyzed "ISO – International Organization for Standardization" or "International Organization for Standardization, is an independent, non-governmental international organization, whose members are part of 167 national standardization bodies, which aims to develop international standards that can be adopted voluntarily, consensus-based, market-relevant, supporting innovation and providing solutions to global challenges." [22]

For the purpose of this paper, we have identified as relevant for the research the implementation of the "SR EN ISO/IEC 27001:2018 – information technology, security techniques, information security management systems, requirements"[23], It is part of the 27000 series of standards and was approved in January 2018 by the Romanian Standardization Association, being identical to the European version of the standard. This series of standards is composed of ISO/IEC 27001 ISMS requirements; ISO/IEC 27002 Catalog of control measures; ISO/IEC 2700x Implementation standards; ISO/IEC 2701x Sectoral standards; ISO/IEC 2703x Control standards"[24], and in Figure 3.1 we present their list and their relations, as presented by the International Organization for Standardization:

ISO 27001:2018 is based on the classical principles of information security, namely confidentiality, integrity and availability of information, which generally define the state of

information security. The implementation of this standard provides the premises for long-term information security based on the implementation of security policies, procedures and methods designed to protect the information and resources of institutions. Minimizing risks, it ensures that the management system is well implemented at the level of the institution, meets all the needs of its service recipients and complies with the legislation in force.

State organizations can learn to respond to security risks by implementing and maintaining an information security management system, as they will adopt the security measures provided under ISO 27001:2018, which contain plans to treat these risks. These entity-level plans help the management of the institution to choose the types of controls appropriate to the context in which the institution operates.

The ISO 27001:2018 standard currently has exemplified 114 control measures and security objectives which are divided into 14 groups, which we detail as presented in the standard in Table 3.1: [25]

*Table 3.1. Control measures groups in standard 27001:2018 (source: https://www.itgovernance.co.uk)*

| **Coding of groups** | **Name of the groups** | **Number of control measures** |
|---|---|---|
| A.5 | Information security policies | 2 |
| A.6 | Organization of information security | 7 |
| A.7 | Human resources security applicable at any time before, during or after employment | 6 |
| A.8 | Management of resources | 10 |
| A.9 | Access control | 14 |
| A.10 | Cryptography | 2 |
| A.11 | Physical and environmental security | 15 |
| A.12 | Security operations | 14 |
| A.13 | Security of communications | 7 |
| A.14 | System procurement, development and maintenance | 13 |
| A.15 | Relations with suppliers | 5 |
| A.16 | Management of information security incidents | 7 |
| A.17 | Information security aspects in business continuity management | 4 |
| A.18 | Compliance with internal requirements - policies and external requirements - laws | 8 |

ISO 27001:2018 requires a public institution to use a management strategy that uses a process-oriented approach. When this approach is used, it means that management controls the processes, the interactions between these processes and the results that come out of them.

The standard suggests structuring each process within the ISMS by using the Plan-execute-Check-Act (PDCA) model, the graphical representation of which we find in Figure 3.3, and each process within the model represents:

- planning objectives together with specific information security objectives;
- The implementation of the plan in practice, managed and maintained;
- verification, measurement, auditing and evaluation based on process efficiency measurement through performance indicators;

- action to implement the most appropriate solutions to improve the efficiency of the processes". [26]


*Fig.3.3. PDCA model (source: Ministry of Development, public works and Administration)*

Risk analysis is an activity supporting information security, and the importance of this process derives from the definition of ISO 27001:2018, respectively the identification of incidents that may occur in institutional activities and the most useful ways of addressing them.

ISMS certification in accordance with ISO 27001:2018 requirements can equally apply to any public institution having among its general objectives the creation of a positive image for the general public by maintaining a state of information security. This can be achieved by:

- public communication of information security policy;
- training of personnel in the field of information security protection;
- increasing the trust of all state or private entities, through certified evidence showing the ability to protect information, regarding its confidentiality, integrity and availability.

The implementation of an ISMS at the level of a public entity will help both management and its employees to ensure the premises and means by which it is perceived as a digitized public institution, using innovative technologies, with a good reputation at European and international level, worthy of trust to the citizens whose interests they represent, because this demonstrates the provision of quality services and ensures the fulfillment of the mission of the institution.

Among the basic purposes that public institutions can pursue through ISO 27001:2018 certification, we list measures to protect the personal data of employees or institutions with which they exchange data or information, as well as citizens benefiting from their services, managing information security risks, complying with European regulations in the field of personal data protection and improving the organizations image in public.

# CHAPTER 4
# RESEARCH AND PRACTICAL CONTRIBUTIONS REGARDING THE IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM AND ITS CERTIFICATION ACCORDING TO SR/EN ISO 27001:2018 AT THE LEVEL OF THE PERMANENT ELECTORAL AUTHORITY

## 4.1. PRESENTATION OF THE STANDING ELECTORAL AUTHORITY AND THE CATEGORIES OF INFORMATION IT MANAGES

In order to present as much detail as possible how to implement a model of information security management system within a public institution, we considered it necessary to present a practical model, a case study through which to transpose the theoretical side, Rather abstract in terms of the activities to be carried out, in the practical area, that is, creating a practical model for implementing the ISMS, similar to the initial advice of such an approach and then the steps to be followed for its certification according to the ISO 27001:2018 standard.

In order to achieve this approach, we have chosen for practical analysis and case study a public institution representative of the Romanian state, namely the Permanent Electoral Authority. We made this choice because the institution is the guarantor of compliance with the basic principles of democracy in Romania, which implies a high degree of security of the information it manages.

During the bibliographic research carried out within the doctoral paper, we found that in order to ensure the information security of such an important institution, a high degree of sophistication of the results of practical research is needed. This choice involved the need for in-depth knowledge of the operational, legal and technical mechanisms of the institution, knowledge of the categories of information, the equipment through which it is processed or stored, and the ways and flows through which it circulates inside and outside it.

"The Permanent Electoral Authority is an autonomous administrative institution with legal personality and general competence in electoral matters, which has the mission to ensure the organization and conduct of elections and referendums, as well as the financing of political parties and electoral campaigns, in compliance with the Constitution, the law and international and European standards in this matter." 27

Thus, the objectives in terms of digitization and debureaucratization of the Permanent Electoral Authority can be achieved through the IT&C department, which has all the levers for transferring as much information as possible managed by the institution to the online environment, which would lead to the transition to e-government, easy and real-time interoperability for the exchange of information with other information systems of public administration entities.

In order to achieve these objectives, a suite of it systems and applications operates at the institution level, which are used to provide operational support for all processes and information that the structures within the institution have as legal attributions.

The internal IT&C infrastructure of the Permanent Electoral Authority supports on the one hand the daily activities of all employees, namely the network infrastructure, the necessary equipment for office work, Internet access, intranet, file exchange and joint work, internal and external communication by email and on the other hand all it applications developed with own resources or purchased from the market, necessary for the institution to carry out operational activities.

The hardware infrastructure that supports the information system of the Permanent Electoral Authority operates in a data center located in the institutions headquarters, which also contains equipment with the role of back-up and data recovery in case of disaster, which is located in a secure space within the building. The logical scheme of the system architecture is presented in graphic form in Figure 4.1:

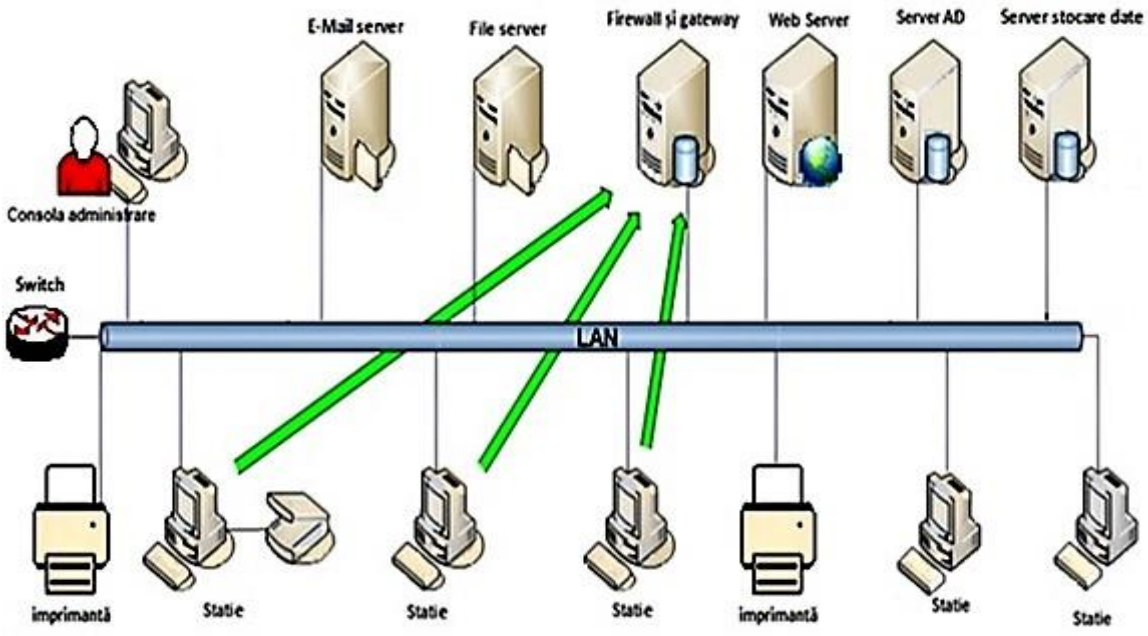


*Fig. 4.1. Communication network architecture at AEP headquarters (source: AEP internal network technical documentation)*

A very important component of the information system of the institution is the electoral registry information system (SIRE), being represented by a complex IT portal that was created in order to ensure a correct and transparent record of Romanian voters and their placement on polling stations in Romania and abroad.

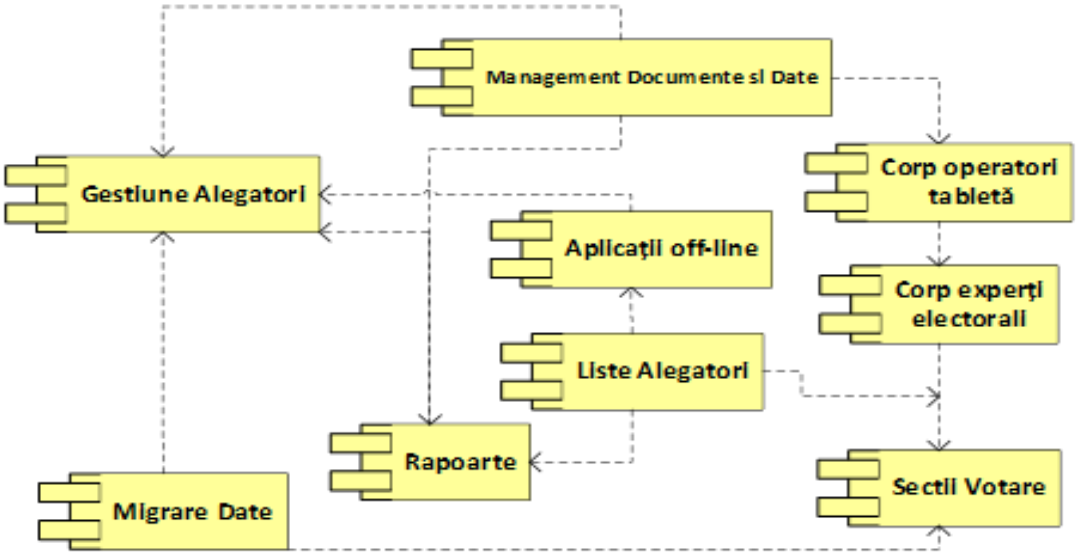


*Fig.4.2. Logical architecture of SIRE (source: SIRE technical documentation)*

## 4.2.PRACTICAL CONTRIBUTIONS REGARDING THE IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM AT THE LEVEL OF THE PERMANENT ELECTORAL AUTHORITY

The analysis of the results of the scientific research resulted in a series of information security risks managed at the level of the Permanent Electoral Authority which may represent major reputational challenges for the management of the institution in the current geo-political context, and the practical method that I proposed in my paper for maintaining an information security climate is to create, Implementation and continuous improvement of an information security management system and its certification according to the rules of "SR EN ISO/IEC 27001:2018 on information technology – Security techniques – information security management systems".

We will present explicitly and in detail in the analysis the benefits of implementing an individually customized ISMS for the needs of AEP, which complies with the requirements imposed by ISO 27001:2018, for certification by an accredited certification body.

In order to go through the steps that are necessary at the AEP level in order to implement the ISMS, it is necessary to take the following steps:

- ❖ Planning, preparation of the elements to be covered by the ISMS;
- ❖ Carrying out the implementation activities of the ISMS at the institution level;
- ❖ SMSI certification that has been implemented at AEP level according to ISO 27001:2018;
- ❖ Maintenance by complying with security measures adopted by the ISMS and its regular internal or external auditing.

In parallel with the implementation of ISMS and its certification according to ISO 27001:2018, other internal or international standards and management systems, which have similar principles or scope and which are aimed at improving or maintaining the state of information security, may be used or implemented.

### *4.2.1. Components and stages of implementing the ISMS at the level of the Permanent Electoral Authority for ISO/IEC 27001 certification*

In order to implement the ISMS, technical and organizational measures that are still known in this area and abbreviated as "MTO" should be adopted at the level of the AEP, in order to achieve and maintain an information security climate in order to achieve the required level of protection required for certification of the system in accordance with ISO 27001:2018.

At the AEP level, in order to achieve this major objective, a thorough analysis of the Romanian and Community legislation governing the AEP activity, of the practices in the field and of the official documents available in the public environment regarding the ISO 27001:2018 standard must be carried out, And the attributions of the Department of Informatization of Electoral processes within the institution that has the task of ensuring the information security of the Authority.

The first procedural step of this process is to carry out an audit of the IT&C system owned or managed by the institution, which will have the role to ascertain the current state of information security at AEP level and to identify the steps to be taken at the level of equipment and software, in relation to the requirements of the standard, in order to achieve the specific objectives of the structure and implicitly of the institution.

### *4.2.2.Determining the scope of the information security management system within the Permanent Electoral Authority*

During the implementation of the ISMS, one of the first tasks is to accurately determine **the scope of the management system** and analyze the requirements and situation of the institution and stakeholders in this process.

According to the standard, the scope must be well documented and in addition to the processes and divisions covered by the ISMS, it must also include an analysis of the requirements depending on the situation in which the institution is at the time of its execution

At the level of the Permanent Electoral Authority, following the study of the organizational chart and the normative acts that state the organization of the institution and its legal obligations, the proposal on the scope of the ISMS could be the Department of Informatization of Electoral Processes (DIPE), which is the structure that can implement, Pursue and permanently improve the institutions ISMS, as evidenced by the powers conferred by the AEPs Organization and Operation Regulation, approved by the Decision no. 4/2020 of the Standing Bureaus of the Chamber of Deputies and the Senate[28], by which it was assigned responsibilities in the field of management, Administration and information security of IT&C components owned by the institution.

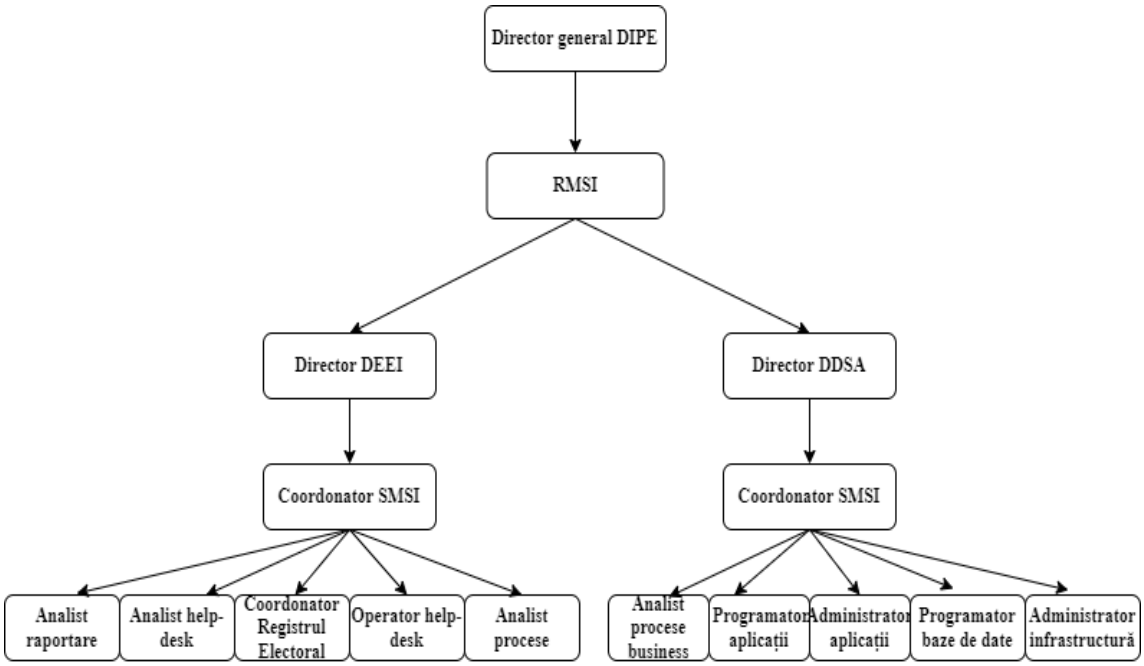


*Fig. 4.8. DIPE organizational chart restructured according to the needs of the ISMS (proposal author)*

Once created, the scope document at AEP level will be made available to management and management of all departments for analysis and verification, which is the only way all stakeholders can verify that the scope of the ISMS covers all processes, infrastructure, subjects or requirements relevant to the entire institution.

Another important document that is part of the management system is the Declaration of applicability, a mandatory document required by the ISO 27001:2018 standard. The statement details and explains the decisions to implement the controls – i.e., check whether each proposed control at the institution level is useful and whether or not it will be used under the ISMS, including the appropriate justification for each verification.

### *4.2.3.Analysis of the current situation and operational requirements at the level of the Permanent Electoral Authority*

The purpose of an analysis of the situation at the level of the AEP is to place the ISMS in the general environment in which the Authority operates, based on the scope defined in the previous implementation steps and approved by the management of the institution. After establishing internal and external organizational relations, the analysis should establish the technical relations between the information applications managed by the AEP, which are relevant for the implementation of the ISMS.

The analysis will also have to include the specific conditions typical for the AEPs field of activity, given the importance of the information systems that the institution is justified by their use in all electoral processes in Romania and Europe

In addition, for a good foundation of the ISMS components, the external context in which the AEP operates will be carefully analyzed, such as the type and profile of major service providers and providers, who are the strategic partners of the institution and any other relevant organizations with which there are collaborative relationships.

The persons responsible for implementing the ISMS will have to have a very clear picture of information security and its implications in relation to the core activities of the institution, as well as those of all stakeholders.

### *4.2.4. Management, roles and responsibilities in relation to ISMS at the level of the Permanent Electoral Authority*

A successful information security management system must be implemented vertically in the "top-down" model, with the involvement and support of senior management, which is the key factor for the success of the management system implementation process and its certification according to ISO 27001:2018. [29]

The most important role in the implementation of the ISMS is played by the senior management of the Permanent Electoral Authority, which must be actively involved in making the decision to implement the system and subsequently support and approve all the steps, Documents and activities that are created throughout implementation and certification according to ISO standards.

If the AEP leadership will accept the proposal on establishing the scope of the ISMS at the level of the Department of Informatization of Electoral processes, then the management of the entire implementation process will have to be ensured this department.

In this context, the management of the DIPE together with the senior management of the AEP will have to assign responsibility and managing authority to an information security management system manager. This will be the most important role in the system implementation process, as it is responsible for the successful implementation of the information security management system at the institution level.

Taking into account the institutional organizational structure currently existing within the AEP, in order to implement the ISMS, we propose as a project management tool the implementation of a RASCI matrix**,** the purpose of the commission will be to successfully identify all responsibilities correctly and completely and to respect them at the level of the entire staff. This concept is also known as the responsibility allocation matrix.

The responsibility for supporting and complying with security policies will lie with the entire institution, under the guidance and assistance of management personnel, who encourage the commitment of all staff to approach the ISMS as part of their professional skills.

ISO 27001:2018 sets out the responsibilities that any Member of the implementation team must assume to ensure compliance with the conditions set out therein, which include:

- establishing security policy objectives that must be consistent with the strategic policies and general objectives of the institution;

- ❖ Compliance with generally valid conditions and specific objectives for the implementation of the ISMS.
- ❖ compliance with information security measures in the institutions day-to-day activity;
- ❖ Ensuring resources for the implementation of the ISMS;
- ❖ definition of responsibilities in the job description for civil servants who will implement security measures to carry out their duties.

### *4.2.5.Information security policies to be adopted at the level of the Permanent Electoral Authority*

An information security policy is the assurance of management regarding the analysis and treatment of information security issues at the level of the institution. It provides directions and operational support to information security issues according to the institution's regulations, laws and technical norms in force.

At the level of the EDA, an information security policy document will be developed as part of the activities of the ISMS, which will ensure that employees and interested external entities are informed, On the obligation to comply with information security requirements and the institutions commitment to continuous improvement of the ISMS will be declared.

The policy will include the general principles and objectives of information security for the successful implementation of the ISMS and will apply to all AEP activities related to information, information systems, network and physical infrastructure.

The information security policy shall contain measures regarding the management of IT&C resources held by AEP. Asset protection must be achieved and maintained and for this reason there must be a register of all assets that manage information on the ownership of the institution.

Equipment and computer programs owned by AEP and in the use of the employees of the institution, which will be subject to security policies adopted under the ISMS will be recorded in a special register, which will be part of the system records and will contain all data about origin, acquisition, the primary place of use and their status when handed over to the user, or any change in any of the above-mentioned data or the security status found in the system controls.

### *4.2.6.Risk management and management within the ISMS at the level of the Permanent Electoral Authority*

Risk management is the activity that analyzes everything that could happen negatively within the AEP ISMS, as well as the potential impact of these events from all points of view in order to prevent possible material, financial or reputational damage. The main purpose of risk management within the institution is to reduce the risks identified by each department to an acceptable level. The definition of the level of risk acceptability shall be decided and defined by the persons who have received this responsibility from the management of the institution.

During the bibliographic research for the doctoral thesis, we identified several peculiarities of how to address the risks that have been identified and assessed within the ISMS at the level of a public institution. One of the most important particularities in relation to the private environment is the obligation of public institutions to organize their risk management activity according to the standards and rules imposed by "order of the Secretary General of the Government no. 600/2018 on the approval of the Code of Internal Management Control of public entities", what is the primary legislation in this area?

For proper implementation, we have identified the need for cyclical and objective assessments to contribute to systematic identification, transparent risk assessment and presentation in the context of information security and ensure an acceptable and long-term

improvement of the level of security within the scope to be established and adopted at the level of the institution.

In order to ensure the implementation of risk management at the level of the Permanent Electoral Authority, the "monitoring Commission (CM) of the Management Internal Control System (SCIM)" was established, by order of the President of the institution, which has among its duties the obligation to implement, modify and ensure the functioning of the management identification, evaluation, analysis and monitoring of the risks identified at the level of the institution. respectively,

All risk management activities within the AEP are carried out in accordance with the system procedure "PS.08 – risk management procedure", which describes the specific process by which the institution is implemented "Standard 8 – risk Management of the Code of Internal Management Control of public entities, Approved by order of Secretary General No. 600/2018".

In conclusion, we can say that in order to implement the information security management system at the level of the DIPE, the entire apparatus of the Permanent Electoral Authority will have to thoroughly review the principles underlying the information security risk assessment activities, defining new specific risks and criteria for their acceptance and evaluation procedures in accordance with the underlying documents and requirements of the system as outlined in ISO 27001:2018.

### *4.2.7.Procedures, documents and policies proposed for adoption within the ISMS at the level of the Permanent Electoral Authority*

At the level of the Permanent Electoral Authority, information security policies and procedures must be created and implemented, detailed for each control that will be defined at the level of the ISMS, these being express requirements of the ISO 27001:2018 standard.

The information security procedures and policies that will be created within the ISMS at the AEP level will be transmitted to all employees who will have tasks in relation to the activities for which they were created, to be informed and used, so that everyone knows their responsibilities under the field and management can control the individual activities in the best conditions.

In order to identify which procedures, need to be documented at the institution level, see the "statement of applicability" - SOA, which details and explains the decisions implementing the controls, verifying whether each proposed control at the institution level is useful and whether or not it will be used under the ISMS, including the appropriate justification for each verification.

Below we present the proposal for a list of the documents, policies and procedures we make to the management of the AEP to be adopted at the level of the institution in the context of protecting information security, what has been analyzed and will have to be created in accordance with the clauses we identified in Annex A to ISO 27001:2018, which we consider useful to be created and adopted under the ISMS at the AEP level:

- ❖ "Information security policy statement;
- ❖ Scope of the ISMS;
- ❖ PO-SMS-Organization of information security;
- ❖ PO-SMS-Publicly available information;
- ❖ PO-SMS-Handling of storage media;
- ❖ PO-SMS-Awareness and training;
- ❖ PO-SMS-Information resource management;
- ❖ PO-SMS-Classification and labeling of ISMS information;
- ❖ PO-SMS-Access control;
- ❖ PO-SMS-Physical security;

- ❖ PO-SMS-Asset inventory;
- ❖ PO-SMS-Equipment security;
- ❖ PO-SMS-Correct data processing in applications;
- ❖ PO-SMS-Operational procedures and responsibilities;
- ❖ PO-SMS-Protection against mobile and harmful codes;
- ❖ PO-SMSI-Security backup;
- ❖ PO-SMS-Security of system files;
- ❖ PO-SMS-Monitoring;
- ❖ PO-SMS-Network Security Management;
- ❖ PO-SMS-Planning and acceptance of the system;
- ❖ PO-SMS-Management of services provided by third parties;
- ❖ PO-SMS-ISMS incident Management;
- ❖ PO-SMS-Activity continuity Management;
- ❖ PO-SMS-Compliance with legal requirements;
- ❖ PO-SMS-procurement, development and maintenance of systems;
- ❖ PO-SMS-Internal Audit procedure;
- ❖ Declaration of applicability (SOA);
- ❖ Risk register and treatment;
- ❖ Supplier security policy;
- ❖ Internal audit program;
- ❖ Information classification policy." **[**30]

It can be said that a large number of policies and procedures are only a burden for the institution, and this can only be true if they were written only for the purpose of passing the ISO 27001:2018 certification audit. We conclude that the set of documents containing policies, procedures and documents proposed for adoption within the ISMS at the level of the Permanent Electoral Authority must be written with the intention of reducing the information security risks and thus will prove their value as time goes by, reducing the number of security incidents at the level of the institution.

#### *4.2.8. Monitoring performance through indicators at the level of the Permanent Electoral Authority*

In the context of the implementation of the ISMS at the level of the AEP, a number of information security provisions and objectives will be defined, which will also contain guidelines or concepts for their implementation by all departments, and compliance with these provisions will be continuously monitored.

In the analysis of management processes, the performance at the team level or of each individual employee will be one of the major objectives to be pursued at the level of the management of the institution, given that this indicator will always relate to the quality of the services that the AEP law has to provide to citizens.

In order to measure the level of achievement of specific information security objectives and to measure the effectiveness of the strategies implemented through the ISMS, it will be necessary to define an integrated system of performance indicators, which the institution will have to use to self-assess results.

Performance indicators are effective tools to measure the performance of security activities and actions, as well as their success in meeting the overall and specific objectives of the institution set out in the framework of the ISMS. The indicators provide information about the performance of the whole ISMS and each activity and serve as catalysts for management to get involved when they are not reached and take action accordingly. This involvement can mean evaluating the situation at a certain point in comparison with the desired situation and corrective intervention of management to remedy and achieve indicators.

In the framework of the activities carried out for the implementation of the ISMS, new performance indicators will have to be rethought, established and adopted, which will have to follow the concept of smart objectives **(**specific, measurable, accessible, relevant/achievable, timely). As a result, performance indicators must be specific, measurable, accessible and achievable, both along the time axis and through their implementation in all departments of the institution, and they must be systematically structured and based on appropriate and sound statistical and mathematical foundations.

In order to add value to the creation of a mechanism to support the performance of the monitoring and evaluation processes in the AEP, particular attention will need to be paid to the ongoing professional training of the staff in charge of monitoring and evaluation of performance indicators in the implementation of the ISMS.

#### *4.2.9. Management of security incidents at the level of the Permanent Electoral Authority*

Although not explicitly mentioned in the normative section of the standard, information security incident management is an essential component of a functional ISMS that will need to be implemented within the management system that will be implemented at the AEP level.

Security-relevant incidents are generally non-conformities that can have a decisive impact on the continuous improvement process and on the maturity of the ISMS, if their causes are investigated. Once mistakes have been identified and relevant conclusions drawn from them, activities and strategies will be reconsidered and measures found to be ineffective removed or replaced, the existing security concepts will be updated or new solutions will be implemented and thus the greatest benefits will be obtained from a management system that will work under predictable conditions.

For a correct and predictable implementation of incident management, an incident management policy will be drawn up at the AEP level. This document will set out the activities through which the security measures will be implemented by the AEP technical team, which will have knowledge and skills in this field. In order for the policy to bring added value to the institution in implementing the ISMS, it must be based on the results of the security risk analysis, which must be done in advance.

The information management process during incident management should start with the collection of information, which may differ on a case-by-case basis because the acquisition of incident data can be done by receiving incident reports from employees or beneficiaries, or by receiving alerts from the incident monitoring computer system.

RMSI is required to report to the management of AEP all incidents related to information, providing regular reports on all security incidents. Management together with DIPE and RMSI employees decide whether security incidents occurred should be reported further to state research bodies and/or CERT/CSIRT.

In order to minimize the likelihood of a security incident occurring at the AEP level, the team designated to ensure the implementation of the ISMS should carefully analyze the incident or vulnerability data, which are transmitted by the institutions partner CERT/CSIRT, the IT security service providers, state authorities with competence in information security, etc.

#### *4.2.10.Communication in the context of the implementation of the ISMS at the level of the Permanent Electoral Authority*

In order to implement an ISMS, the cooperation of the Department of Informatization of Electoral processes, which will implement and manage the system, with the other departments of the institution will be necessary at the AEP level to permanently raise the level of information security. Interinstitutional cooperation of this kind is achieved through communication, which is the key element in terms of reaching the security target, which will have the effect of preserving the AEPs reputation as a prestigious constitutional institution of the Romanian state.

The main task of the Communication component within the mission of implementing the ISMS and its certification in accordance with the reference standard is to determine and or also the needs for internal and external communication of the AEP on this subject. At the AEP level, communication in general is within the remit of the International Cooperation Department, which is the most appropriate department to take over as attributions the communication component within the SMSI requirement

External communication in this context refers to communication with collaborators outside the institution, which are usually providers, external auditors, institutions acting as CERT/CSIRT or with other state institutions with which the AEP has collaborative relations in terms of information security assurance.

When information about security incidents that have occurred within the institution will be disseminated, the communicant shall be very careful in order to filter sensitive or classified information that may be slipped into the material to be communicated and shall consider taking all necessary measures to ensure the confidentiality of the information to be communicated, especially the ones that will be transmitted through external channels.

#### *4.2.11. Competence and awareness among the staff of the Permanent Electoral Authority*

The entire staff of the institution is required to take note of the information security policy, to carefully analyze it, to assume responsibilities in relation to the ISMS, as well as the consequences of its breach or other non-conformities. The awareness of the information security phenomenon shall be proportionate to the level with which management has the ability to disseminate relevant information relating to the ISMS system.

A classic way to achieve collective awareness is to modify the job descriptions of employees in the ISMS field. The job descriptions of the employees involved in the implementation of the system will have to be modified in order to introduce tasks that are mandatory for the implementation of the ISMS and will specify the necessary skills for the employees who will have responsibilities regarding the security of information.

The continuous training of EDA civil servants will play a very important role in the successful implementation of the management system. Success will involve a good knowledge of the field of information security and related activities by all employees who have direct or indirect attributions in the information security of the institution. Vocational training must take place at all stages of the implementation of the ISMS and reach as many of the targets as possible to know the provisions of the standard, the internal policies and procedures related to the system.

It is necessary to put in place information security awareness campaigns, which will have to be divided into three phases, which will include the following activities: Assessment of knowledge and information requirements, planning of the campaign and its implementation. Awareness of information security must be more than a one-off project, as the campaigns that will be carried out at the institution level will have to include mechanisms to ensure its sustainability. The methods for assessing the effectiveness of the campaign, which will be implemented after its completion, will also need to be analyzed in advance at management level.

#### *4.2.12. Internal audit for the implementation of the ISMS at the level of the Permanent Electoral Authority*

The main objectives of the internal audits of ISMS at AEP level will include monitoring the extent to which the ISMS implemented will meet the purpose, objectives and requirements of the institution on the one hand and the requirements of ISO/IEC 27001:2018 on the other hand, which is called compliance control. At the same time, the audit team will monitor the

implementation of the information security measures taken by the system implementation team, which is called "implementation and effectiveness control".

Following the implementation of the ISMS at the AEP level and the creation of all related documentation, internal public audit missions will be planned, which will have as objectives the control of aspects regarding frequency, procedure, roles and responsibilities, planning requirements, traceability and reporting of measures taken within the management system. The management team, together with the technical team, will need to define quick methods for dealing with corrective and preventive actions recommended by the audit team and determine who will follow them in order to implement the measures that have been left by the auditors.

Audit missions are designed to ensure that all institutional processes covered by the ISMS, established in accordance with the scope, are regularly audited and that the audit will always leave behind written evidence of the findings.

Internal audits of the ISMS will be a vital tool in the process of continuous improvement of the management system to be implemented at the level of the AEP. They will be used to ensure that the management system complies with the institutions own requirements and those of ISO 27001:2018 for determining the components of the system that require improvement. The audit program will ensure that control over all aspects of information security within the scope is covered in an efficient way to improve the management system in order to certify it in accordance with ISO 27001:2018.

Once the measures left by internal audits are remedied, the certification procedure can be started, which involves a certification audit which is always an external audit carried out by entities authorized by national and international standardization entities, employing qualified auditors and certified by an ISO 27001:2018 certification authorities.

The results of the preparation of the external audit mission for certification will be materialized in a set of documents to be sent to an ISO 27001:2018 accredited auditor for review and a set of records and evidence that will demonstrate how effectively and completely SMS was implemented at the level of the Electoral Authority Permanent.

#### *4.2.13. Continuous improvement of the ISMS at the level of the Permanent Electoral Authority*

It should be noted that no matter how many managements analyzes or audit missions of the ISMS will be carried out at the level of the AEP, it is unlikely that it will be designed in a perfect final form from the start of its implementation. Even if the institution will benefit from the help and experience of a consulting company that will analyze the context and participate in the actual implementation, the implementation of the ISMS will not be simple because the institutional environment is different, the activities and challenges of the institution are different and a panacea solution has not yet been identified, it works perfectly for all institutions where such management systems are implemented.

Moreover, geopolitical circumstances in terms of security are constantly changing, so there can never be a permanent "perfect solution" when it comes to information security.

For this reason, a continuous process of analysis of the models to be followed in this area will have to be ensured at the level of the EPAs, in order to adapt to their needs and continuously improve the policies, procedures and documents of the ISMS. It is of particular importance that the institution takes advantage of the non-conformities identified in all audit controls or missions, in order to continuously improve the ISMS and to constantly update this system, the process being known as the continuous improvement process.

The results of these information security management analyze will lead to the improvement of information security policies and procedures in the institution, which will aim to continuously improve the ISMS.

# CHAPTER 5
# FINAL CONCLUSIONS, FUTURE DEVELOPMENTS, PERSONAL CONTRIBUTIONS AND WAYS OF CAPITALIZING ON RESEARCH RESULTS

## 5.1. FINAL CONCLUSIONS ON THE EFECTUALE RESEARCH WITHIN THE DOCTORAL THESIS

The research carried out within this doctoral thesis, entitled "Research and contributions on the implementation of quality-risk systems in order to ensure information security in public institutions", had as a starting point the urgent need perceived in the public space regarding information security in public institutions. This need, which has been triggered by the deep reconfiguration of the role, effects and at the same time the vulnerabilities involved in the information management processes, must become a priority of any public institution.

The hypothesis of the paper is the potential to streamline the response of state organizations to information security threats, in the context of the implementation of quality-risk systems and their certification in accordance with international standards in this field. This hypothesis is explored and demonstrated through the practical model detailed in Chapter 4 of the doctoral thesis, "Research and practical contributions on the implementation at the level of the Permanent Electoral Authority of an information security management system and its certification according to SR/EN ISO 27001:2018".

Theoretical objectives of the doctoral thesis:

- ❖ Theoretical and comparative-critical analysis of the current state of research on information security.
- ❖ Establishing the role and importance of information security in public institutions.
- ❖ Research into methods, ways and systems to ensure information security at the level of public institutions.
- ❖ Theoretical analysis of information security management systems and their certification according to the international standard SR EN ISO/IEC 27001:2018.
- ❖ Identifying the particularities of the applicability of the ISMS in the context of implementation in state institutions.

Practical objectives of the doctoral thesis:

- ❖ Designing a model of practical implementation of the ISMS and its certification according to the international standard SR EN ISO/IEC 27001:2018 at the level of the Permanent Electoral Authority in Romania.
- ❖ Propose a set of measures that may form part of the security policy to be adopted under the ESM of the EDA.
- ❖ Establish the procedures, documents and policies to be adopted by the EDA under the ISMS.
- ❖ Identification of information security risks at the level of the AEP in order to deal with them.
- ❖ Proposal of the action plan for the implementation of the ISMS at the level of the EDA containing the phases the terms of implementation, the responsible and deliverable.

The general conclusion of the thesis is that in these times characterized by major political tensions, classical or hybrid wars, in addition to the exponential increase in the number of security incidents in the field of information, the complexity of attacks on them has also increased proportionately, but, especially the degree of sophistication of the means and

techniques of attack, which required the emergence and development of methods, tools and procedures of active defense against these attacks.

## 5.2.PROPOSED FUTURE DEVELOPMENTS WITHIN THE FIELD UNDER INVESTIGATION

The results of the studies carried out within the doctoral thesis led from the research phase to the conclusion that in order to ensure an information security climate in public institutions is appropriate the measure of implementation of information Security Management systems, in accordance with the rigors of ISO 27001:2018.

This justifies the need to continue the present study on the field of information security, aimed at managing security risks by implementing international standards aimed at the field of information security, of which we mention: All other standards in the ISO 27000 series; COBIT standard, ITIL certification, etc.

In order to achieve the purpose of maintaining information security in state entities, we have identified the need for in-depth study regarding the analysis of how information security policies can be transformed into public policies, which will underpin the fulfillment of their general and specific objectives.

Further research in the directions presented above may result in the identification of new practical methods by which public institutions will adopt new information security policies as comprehensive as possible in order to guarantee a security climate of the information they manage.

The findings of scientific research will help public institutions in the initial analysis, consultancy and implementation of standardized information security policies, the results of which have been tested in advance by internationally recognized certificate entities.

Through the implementation of these new policies, the institutions will be obliged to review or completely change the security documentation and procedures, through which they will be able to ensure the prevention of potential information security breaches.

## 5.3. PERSONAL CONTRIBUTIONS OF THE AUTHOR IN THE FIELD RESEARCHED

In accordance with the normative limits identified in the bibliographic research carried out within the doctoral thesis, as well as with the high dynamics of the field investigated, I point out as personal contributions the following:

- **Deepening the studies** on particularities and methods of implementing the ISMS and its certification according to SR EN ISO/IEC 27001:2018 within public institutions, among which we mention the obligation of these entities to comply with the "OSG no. 600/2018 on the approval of the Code of Control of Internal Management of public entities", This requires the adaptation of the implementation process and all the documents of the management system to the rules established by the order;
- **Planning the implementation activities of the ISMS** and its certification in accordance with ISO 27001:2018 in public institutions, establishing the responsible for each activity and measuring the added value of each activity in terms of information security;
- **The analysis of the information security incident legislation in Romania** that was in force at the time of the research and its implications regarding the implementation of ISMS within public institutions in Romania;
- **The practical contribution of the author is the proposal of a model of practical implementation at the level of the Permanent Electoral Authority,** which is a novelty

in the context of information security within this public institution; This future implementation of the ISMS will contribute to raising the level of information security, which will create a positive image of the institution, raising it to the highest standards among the electoral management entities at international level.

- **ISMS certification to ISO 27001:2018 will** bring with it several advantages for maintaining an information security climate in AEP, as it is a globally recognized information security standard. The implementation of the security measures imposed by this standard can help the institution reduce the number or decrease the intensity of security risks and implement information security policies in order to build a good reputation in public conception.

In conclusion, we mention that the implementation of the ISMS and its certification according to the norms of the ISO 27001:2018 standard within the AEP will ensure a positive image of it in the collective mind, based on a high level of security that is permanently verified by external audit entities to ensure information security.

## 5.4. WAYS TO CAPITALIZE ON RESEARCH RESULTS

The results obtained from the research carried out within the doctoral thesis were capitalized through analyzes and case studies created, which aim to convince the top management of the Permanent Electoral Authority in the sense of implementing the ISMS and its certification according to "SR EN ISO/IEC 27001:2018".

Through these results, we will convince service recipients that the institution has created a credible image and a modern and European digital environment, through which it strives to ensure a general framework for information security at a high level. Thus, it was agreed in principle at the management level of the institution the use of Chapter 4 of the doctoral thesis as initial advice for the implementation of the ISMS at AEP level.

Another way of capitalizing on the results of the scientific research within the thesis were the publications of scientific papers in magazines or specialized bulletins and the works published at national and international congresses or conferences, as author or co-author

# SELECTIVE BIBLIOGRAPHY

**[1]** Law no. 182/2002 on the protection of classified information, available at https://lege5.ro /app /document /gm4dsnbx /law no. 1822002 on the protection of classified information?pid=12542165, site consulted on 03.05.2021;

**[2]** Șerb, Aurel, Baron, Constantin, Isăilă, Narcisa, information Security in the information society, Pro Universitaria Publishing House, Bucharest (2010), p. 31

**[3]** Giurcan, Gigi, Cyberterrorism, PhD thesis (2010), p. 94;

**[4]** Klimburg, Alexander (ed.), National Cyber Security-Framework Manual, NATO Cooperative Cyber Defence Center of Excellence, Tallin, Estonia (2012), available at https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/, website consulted on 12.05.2021;

**[5]** Klimburg, Alexander (ed.), National Cyber Security-Framework Manual, NATO Cooperative Cyber Defence Center of Excellence, Tallin, Estonia (2012), available la https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/, website consulted on 15.05.2021;

**[6]** Morgenthau, Hans, Politics Among Nations: The Struggle for Power and Peace, Kalyani Publishers, [2018], p. 290-292;

**[7]** Howard, John D., Longstaff, Thomas A., A common language for computer security incidents, Office of Scientific and Technical Information, United States Department of Energy (1998);

**[8]** Definition of hacker in Romanian, available at https://dexonline.ro/definitie/hacker, website consulted on 10.06.2021;

**[9]** Definition of hacker in English, available at https://www.lexico.com/en/ definition/hacker, website consulted on 10.06.2021;

**[10]** Stan, Emil, Străinu, Emil, cyber terrorism, Publishing House of the Academy of High Military studies (2002);

**[11]** Stan, Emil, Străinu, Emil, cyber terrorism, Publishing House of the Academy of High Military studies (2002), p. 169;

**[12]** Idem

**[13]** Sullivan, Peter, which is the role of a computer Emergency response team (CERT), available at https://www.techtarget.com/whatis/definition/CERT computer Emergency readiness team, site consulted on 30.06.2021;

**[14]** Coteanu, Ion., Seche Luiza, Explanatory Dictionary of the Romanian language, Universe Encyclopedia Publishing House, Bucharest, (1996)

**[15]** Roșca Constantin, Dictionary of Ergonomics, CERTI Publishing House, Craiova, (1997)

**[16]** Romanian Standardization Association - national Standardization Body (ASRO), risk Management. Code of practice and guidance for the implementation of SR ISO 31000, available at http://standardizare.wordpress.com/2013/07/ 02/sr-bs-311002013-risk management-code-practice-and-guidance-for-implementation-standard-sr-ISO-31000/, website consulted on 01.07.2021;

**[17]** The National Institute of Standards and Technology (NIST) - U.S. Department of Commerce, NIST SP 800-37R2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, available la,

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, website consulted on 01.07.2021;

**[18]** Mitnick, Kevin D., Simon, William L., The art of intrusion. The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley Publishing Inc., Indianapolis, Indiana (2005), available la https://repo.zenk-security.com/Magazine%20E-book/ Kevin Mitnick-The Art of Intrusion.pdf, website consulted on 02.07.2021;

**[19]** Papastergiou, Spyridon, Mouratidis, Haralambos, Kalogeraki, Eleni Maria, Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures, Evolving Systems, No.21 (2021), p. 91-108, available at https://link.springer.com/content/pdf/10.1007/s12530-020-09335-4.pdf, website consulted on 01.08.2021;

**[20]** Ravndal, Jacob Aasland, Johnsen, Siw Tynes, Kjeksrud, Stian, Broen, Torgeir, Resilience methodology – multinational experiment 7, Norwegian Defence Research Establishment (FFI) (2014), available la https://publications.ffi.no/nb/item/asset/dspace: 2430/14-00973.pdf, website consulted on 01.08.2021;

**[21]** Rosenzweig Paul, Bucci, Steven P., Inserra, David, A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace, The Heritage Foundation, No. 2785 (2013), available at https://www.heritage.org/defense/report/congressional guide seven steps us security prosperity and freedom cyberspace, website consulted on 03.08.2021;

**[22]** International Organization for Standardization, available la https://www.iso.org/ about-us.html, website consulted on 07.07.2021;

**[23]** ISO/IEC 27001:2018 Information Security Management, available la, https://www. iso.org/isoiec-27001-information-security.html, website consulted on 18.07.2021;

**[24]** ISO 27000 family of international standards, information technology – security techniques – information security management systems, overview and vocabulary, available at https://standards.iso.org/ittf/PubliclyAvailableStandards/c07390 6 ISO IEC 27000 2018 E.zip, website consulted on 18.07.2021;

**[25]** Control measures and security objectives of the 27001 standards, available at https://www.it governance.co.uk/blog/iso 27001 the 14 control sets of annex a explained, website consulted on 24.07.2021;

**[26]** Deming model-based strategy (PDCA), study on the benefits and effects of implementing quality management systems in public institutions in European countries, available at https://www.mdlpa.ro/uploads/articole/attachments/61a87b75ef8 ca072647906.pdf, website consulted on 24.07.2021;

**[27]** about the Permanent Electoral Authority, available at https://www.roaep.ro/ presentation/about-us/, website consulted on 08.08.2021;

**[28]** AEP Regulation of Organization and operation, approved by Decision no. 4/2020 of the Standing Bureaus of the Chamber of Deputies and the Senate, available at https: //www.roaep.ro/presentation/wp-content/uploads/2020/12/the rules of organization and functioning of the Permanent Electoral Authority 2020.pdf, website consulted on 22.08.2021;

**[29]** Henning, David, Tackling ISO 27001: A project to build an ISMS, SANS Institute (2009), available la https://sansorg.egnyte.com/dl/JjBP0dMfnB, website consulted on 22.08.2021;

**[30]** Romanian Standardization Association, SR EN ISO/IEC 27001:2018 information technology, security techniques, information security management systems, requirements. Overview and vocabulary, (2018);