MOLDOVA STATE UNIVERSITY

DOCTORAL SCHOOL OF NATURAL SCIENCES

With manuscript title
C.Z.U. 004.056:336.71(478)(043)

BRICEAG VALENTIN

ANALYSIS AND ENHANCEMENT OF THE INFORMATION SECURITY MANAGEMENT SYSTEM MATURITY LEVEL FOR THE REPUBLIC OF MOLDOVA ENTITIES
(Case study - commercial banks)

232.02 Technologies, products and information systems

Summary of the doctoral thesis in Informatics

Chisinau, 2024

The thesis was developed within the Moldova State University, Doctoral School of Natural Sciences, Department of Informatics of the Faculty of Mathematics and Computer Science.

Scientific advisor:

BRAGARU Tudor	Doctor of Economic Sciences, university professor, Moldova State University

Composition of the Doctoral Committee:

CĂPĂTÂNĂ Gheorghe	Doctor in technical sciences, university professor, Moldova State University - *president*
BRAGARU Tudor	Doctor of economic sciences, university professor, State University of Moldova - *doctoral supervisor*
BOLUN Ion	Doctor habilitate in computer science, university professor, Technical University of Moldova - *referent*
COJOCARU Igor	Doctor in computer science, university lecturer, director - Information Society Development Institute - *referent*
OHRIMENCO Sergei	Doctor habilitate of economic sciences, university professor, The Academy of Economic Studies of Moldova - *referent*

The thesis defense will take place at 18.09.2024, at 15:00 o'clock during the Meeting of the Public Defense Commission of the Doctoral Thesis at the Doctoral School of Natural Sciences, USM. The venue is the State University of Moldova (http://www.usm.md), located at M. Kogălniceanu Street, 65 A, building 3, room 332, MD-2009, Chișinău, Moldova.

The doctoral thesis and the abstract can be consulted at the National Library of the Republic of Moldova (31 August Street 78a, Chişinău, MD 2012) and the Central Library of the State University of Moldova (Alexei Mateevici Street 60, Chişinău, MD 2009), and on the webpage of ANACEC (http://www.cnaa.md) and on the webpage of USM (http://www.usm.md).

The summary was sent to "____"_____2024.

The President of the Doctorate Commission, Doctor of technical sciences, university professor _____ (signature) CĂPĂTÂNĂ Gheorghe

Author: _____ (signature) BRICEAG Valentin

© Briceag Valentin, 2024

CONTENT

THE CONCEPTUAL LANDMARKS OF RESEARCH 4

THESIS CONTENT 7

FINAL CONCLUSIONS AND RECOMMENDATIONS 26

BIBLIOGRAPHY 29

LIST OF PUBLICATIONS ON THE THESIS TOPIC 31

ADNOTARE 32

ANNOTATION 33

АННОТАЦИЯ 34

THE CONCEPTUAL LANDMARKS OF RESEARCH

The Relevance and Importance of the Addressed Topic. Currently, the vast majority of individuals and legal entities, private and public organizations, governmental, etc., are present in the global digital/virtual space, without any well-defined and clearly delineated borders. The massive presence of people and organizations in the virtual space constitutes a major source of security risks for personal data and sensitive information handled in cyberspace, which are valuable for an individual, an organization, a region, or a state. The confusion of concepts like Information Security (InfoSec), Cybersecurity (CS), informatics, etc. [1], the illusion that data and information are not valuable enough to justify spending money on their security, other illusions that InfoSec resides exclusively in IT/IS security and is solely the concern of the IT department, and that purchasing more tools can strengthen CS, etc., lead to the erroneous treatment of InfoSec/CS**.**

Indeed, the success of a modern organization, regardless of its field of activity, size, form of ownership, etc., depends on **understanding the role that information plays in its life and on the efficient management of this information. This includes ensuring the security of information as a process carried out in an ever-changing environment** that matures *(grows, improves)* over time depending on requirements, culture, intended purpose, investments, personnel involved, etc.

Ensuring the security of information in cyberspace becomes a major concern of all actors involved at different levels, starting from individuals (*protection of personal data*), private and public organizations *(universities, schools, hospitals, city halls, banks, etc. – protection of sensitive data)* and ending with the level of governmental regulatory and supervisory bodies *(for example, the Ministry of Education, the Ministry of Health, the Ministry of Finance, the National Bank, the State Tax Inspectorate, the Information Technology and Cybersecurity Service, etc.)*, where the responsibility for developing and applying coherent security policies in the respective field at the state or global level on certain industries is concentrated.

The topic fits into international concerns in an inter-/ and transdisciplinary context. The researched topic perfectly aligns and strongly correlates with the strategies and good practices generated by specialized global organizations. Among the most important such organizations are the developers of management system standards *(and audit, as an indispensable component thereof)* as well as organizations that offer recommendations, education, and professional certifications in the field of information security such as the global Association of Audit and Control of Information Systems (ISACA, www.isaca.org), the U.S. National Institute of Standards and Technology (NIST, http://nist.gov), the Payment Card Industry Data Security Standard Committee (PCI SSC, https://www.pcisecuritystandards.org*)*, the International Organization for

Standardization (ISO, https://www.iso.org/standards.html), the SANS Institute (SysAdmin, Audit, Network, Security, http://sans.org), the Center for Internet Security/CIS (https://cissecurity.org), the Global Organization of Professional Certification (ISC)² *(Information Security Certifications)* which maintains the current Common Body of Knowledge (CBK) on which professional certifications are based, recognized as a global standard of excellence, etc.

The purpose. The creation of **a multi-profile maturity model (M^{3}SI) that is simple, transparent, easy to administer, and use** for creating **typical InfoSec profiles for industries (PSITI) and individual InfoSec profiles (PISI)**, customized according to the concrete needs of entities, which would support the needs of all actors involved at all levels, from top managers, professionals and experts in information security, etc., to end-users, connected to the network from terminal stations, often remotely located and not managed by the entity.

To achieve the purpose, a set of **major objectives** were accomplished such as: *studying various frameworks for addressing and regulating InfoSec, creating a generic M3SI database about frameworks, areas, requirements, threats, risks, and InfoSec controls; developing a typical information security profile for the banking sector PSITI and an individual information security profile PISI for a hypothetical commercial bank (CB), but with direct applicability confirmed by the National Bank of Moldova (NBM); developing the instrumental application for managing the M^{3}SI multi-profile model, typical PSITI profiles, and individual PISI profiles.*

The research focuses on the organizational and management issues in ensuring information security through an Information Security Management System (ISMS), based on the approach to information security risks, consisting of a set of technical and organizational measures *(e.g., legislative acts, internal procedures, human resources, (e.g., normative acts, internal procedures, human resources, IT/IS processes and services, etc.)* and aimed at achieving the InfoSec objectives within the entity. **ISMS must be seen as an indispensable part of the internal control system.**

Methodology used. The development of the M^{3}SI maturity model, which would allow determining the current state of InfoSec/CS, the ISMS, and the priority development directions is based, fundamentally, on **the synthesis of open security methodologies and models,** taking into account the requirements of the main systemic standard ISO/IEC 27001:2022 [2], aiming at simplifying and automating routine processes.

The results of the thesis include the adoption of a unique generic framework – Multi-profile Maturity Model of InfoSec/CS M^{3}SI, with a unique database regarding the frameworks and InfoSec controls, from which typical and particular InfoSec profiles are generated, suitable for the concrete needs of analysis, measurement, and continuous improvement of CS.

The importance and practical value of the obtained results consist in the safer operation of organizations. The typical PSITI profiles and the resulting particular PISI profiles, simple and

transparent, allow various entities to implement, efficiently manage, and continuously improve InfoSec, which in turn leads to the safer achievement of business objectives.

The M^{3}SI support software application simplifies and significantly eases the management of InfoSec, by automating routine database management operations about threats *(which exploit vulnerabilities and lead to asset losses),* risks, specific requirements and controls, generating particular profiles, assessing the maturity level, and tracking progress. The M^{3}SI application is **a web-based application with controlled access**. All these together allow various entities *to organize, approach, and efficiently manage information security*, prevent and more effectively combat risks and threats to information security, and compare maturity over time and/or between typical entities.

Approval of research results. The scientific results obtained by the author within the framework of the thesis were presented in five reports at three different international scientific conferences and were published in three different journals, one from Romania and two category B journals, included in the National Registry of Moldova regarding professional journals. For details, see the list of publications on the topic of the thesis.

Volume and the thesis structure. The thesis is written in Romanian as a manuscript, typeset and printed on a computer. The paper is structured into an introduction, 3 chapters, general conclusions and recommendations, bibliography, and appendices.

Chapter *"1. Analysis of the current state of information security in the banking sector of the Republic of Moldova"* reviews the state of CS, identifies some major problems and challenges related to CS, the legal and regulatory framework of InfoSec in the commercial banks of Moldova, justifying the timeliness and problems of the research. **Chapter** *"2. Theoretical, methodological, and practical aspects of addressing information security through the lens of ISMS"* succinctly presents the theoretical, methodological, and practical aspects of addressing InfoSec, modern approaches to InfoSec based on standards of good practices, risks, and maturity models, the main directions and recommendations for organizing and continuous improvement of the ISMS. **Chapter** *"3. Multi-profile maturity model of information security M3SI"* presents the innovative essence of the research through the modern approach to InfoSec based on open standards, multi-level, multidimensional maturity models, with computer support, generating typical models for industries PSITI and PISI models, personalized, individualized in accordance with concrete corporate policies, guiding standards of the ISO/IEC27k family, target values of the InfoSec maturity evaluation criteria.

THESIS CONTENT

Chapter *"1. Analysis of the current state of information security in the banking sector of the Republic of Moldova (RM)"* justifies the timeliness and identifies some major common problems related to InfoSec/CS in the commercial banks of RM, elucidating the new paradigm for approaching InfoSec through the lens of ISMS. These are mainly related to remote access to client account resources for obtaining account status information, making payments, account top-ups, and other electronic transactions via Automated Remote Service Systems/Services *(SADD)* provided by the Bank to the Client either through internet banking or mobile banking. SADD are used to make predominantly electronic payments with bank cards, possibly with virtual money *(e-/web-money)*, e-banking systems, Internet/online banking, mobile banking, and/or bank machines/ATMs, and/or automated self-service systems and/or POS terminals *(Point of Sale)* or SST *(Self-services)* terminals. **One of the main tasks of the thesis is identifying unique common criteria for increasing the maturity level of InfoSec,** starting from the unique legal framework of the banking sector in RM, the main applications, tools, and IT solutions as well as modern CS challenges.

The legal and regulatory framework of the banking sector in the Republic of Moldova succinctly elucidates the concept of InfoSec and the set of important Laws, NBM regulations, and internal CB regulations, which prescribe the creation and continuous improvement of ISMS as a means of managing and efficiently ensuring InfoSec in the banking sector.

For proper functioning, the InfoSec mechanisms must be capable of dealing with a wide range of risks, attacks, threats, accidents, which must be handled predictably, simultaneously and/or post facto, with a conscious assumption of risks, within the limits of reasonable, bearable costs.

InfoSec is defined as **the preservation of the three fundamental properties of information,** in any of its electronic forms, on paper support, etc., referred to in the literature as the **CIA triad.** The CIA characteristics are defined in ISO/IEC 27000:2018 [1]: **Confidentiality** (clause 3.10), **Integrity** (clause 3.36), **Availability** (clause 3.7).

The definitions of InfoSec and CS are approximately the same in most sources, e.g., they are identical in ISO/IEC 27000:2018, ISO/IEC 27032:2012. And to correspond to the changes in ISO/IEC 27001:2022, which extended its title from "Information Security" to "Information Security, **Cybersecurity, and Privacy Protection**" in ISO/IEC 27032:2023 (cl.3.6), CS is defined as **"the protection of people, society, organizations, and nations against cyber risks"**. Moreover, InfoSec/CS also refers to other secondary attributes, secured on the basis of the

fundamental ones, such as **information possession** *(who is the owner, possessor, responsible party)*, **information utility** *(or significance, the greater the information is more valuable, more accessible)*, **authenticity of information** *(clause 3.6), (inauthentic information constitutes misinformation)*, accountability *(for example, for justifying mutual payments)*, **non-repudiation** *(or the impossibility of denying certain actions taken, e.g., placing an order, clause 3.48)* and **reliability** *(clause 3.55)* of the aforementioned standard.

Typically, **InfoSec/CS is ensured within proprietary ISMS,** which vary depending on the industry, field, and activity of the organization, strategies and internal policies in accordance with current regulations and the relevant legal framework. And the implementation of ISMS involves sets of controls *(preventive, detective, corrective)* and operational procedures, which ensure the primary and secondary characteristics of information, protection of all assets and informational resources within the entity, including personnel, information and communication technologies, support services, etc. to keep CS risks and incidents at a pre-established acceptable level.

The banking sector in the Republic of Moldova operates on two levels: the first level is the National Bank of Moldova and the second consists of 11 commercial banks (https://NBM.md/ro/content/bancile-licentiate-din-republica-moldova). The thesis is specifically focused on SADD, ICT services, card payments, e-banking etc., regulated nationally by a set of laws and regulations. A complete list of specific regulations for the activity of NBM and CB can be seen at https://www.NBM.md/ro/content/lista-regulamentelor. The official versions, especially of current laws, are available at https://www.legis.md/.

Globally, CB activities are regulated by paired standards ISO/IEC 27001:2022 [2] and ISO/IEC 27002:2022 [3], ISO/IEC 27032:2023, GDPR [4], PCI DSS version 4.x from November 2023 [5], and others *(details to be seen in the thesis).*

The purpose of ISMS for a CB is to provide a clear vision regarding the protection systems and prevention of attacks on information and informational assets in any form. The main requirements for information security, establishing ISMS, implementing and operating ISMS, monitoring and reviewing ISMS, maintaining and improving ISMS, documenting ISMS are set out in the *Regulation on internal control systems in banks*, section 3, clauses 33-37, and in section 4, requirements regarding the internal audit of ISMS (https://www.legis.md/cautare/getResults?doc_id=49565&lang=ro).

The main architectural elements, tasks of the ISMS and the logic of its operation can be seen in *(Fig. 1).* This reflects the PDCA procedural approach of ISMS in the analysis cycle of performance and continuous improvement according to the mission, general business strategy, and security policies.

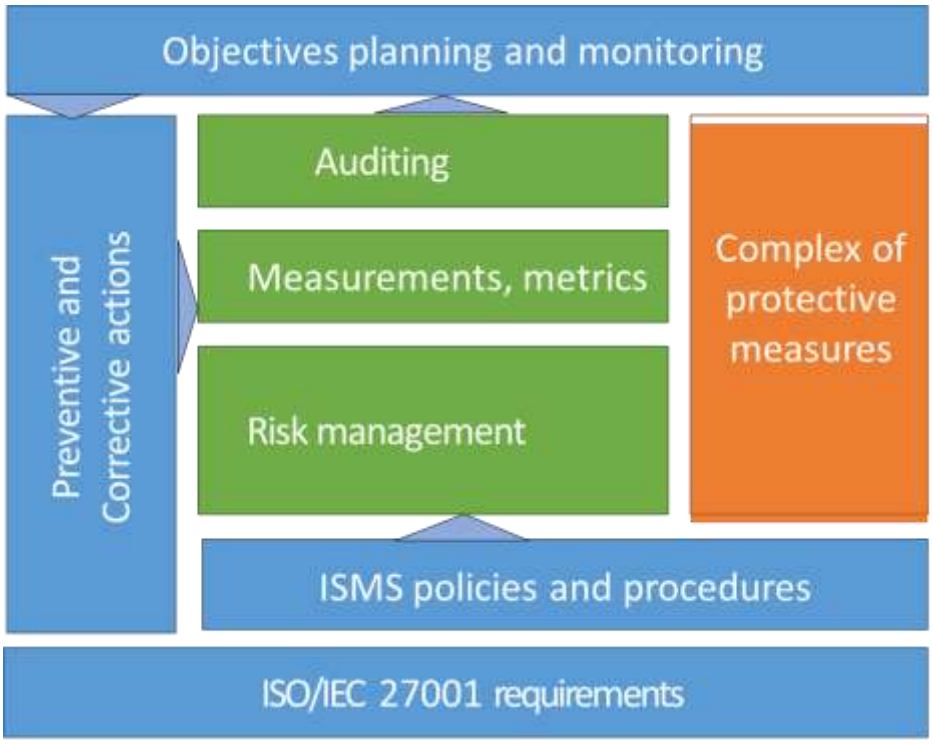


Figure 1. Main ISMS components and logic operation

The objectives of the ISMS are to ensure that banks have an adequate ICT strategy aligned with the general business strategy; that internal governance processes are appropriately established in relation to IT/IS systems; that the internal framework for managing IT/IS risks and internal control adequately protects IT/IS systems; that the online payment system complies with the PCI DSS international standard for payment card industry data security; that rights regarding the protection of personal data are respected according to the Law of Moldova No. 133 from 2011 [6] and GDPR [4] from 2016, applied from 2018.

Basic requirements for InfoSec, CS, and ISMS are in continuous improvement to ensure compliance with legislative provisions, including EU Directives, the NBM Regulation on internal control systems in banks in RM, etc., in a continually changing cyber environment/space.

A genuine ISMS must possess a set of mandatory characteristics [2], e.g.: *to be well-documented/established in writing; to ensure the fulfillment of customer requirements; to ensure the achievement of the organization's objectives in safe conditions; to be applicable in all activities of the organization* and others. Details regarding requirements, including planning, support, operation, systematic performance internal audit, security controls/measures, metrics can be seen, for example, in [2-4], [7-8].

ISMS covers three large areas of resources for ensuring InfoSec, presented in *(Fig. 2)*. The management domains of the ISMS are realized through **processes, policies, procedures, organizational structures, software, and hardware** to protect informational assets.

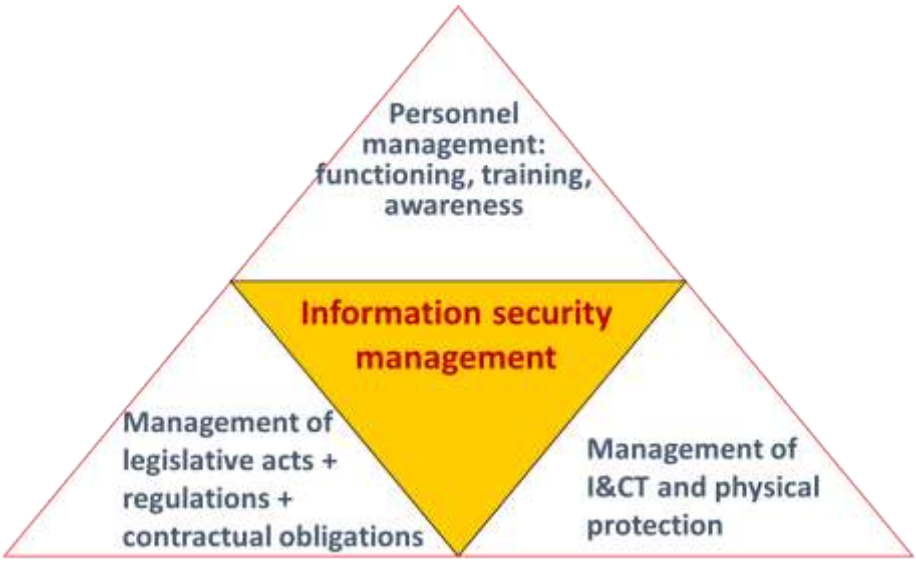


Figure 2. Three large resource areas managed within the ISMS

The type of security controls/measures comply with ISO/IEC 27002:2022 [3]: **Preventive,** aimed at preventing the occurrence of information security incidents; **Detective,** which act when an InfoSec/CS incident occurs; **Corrective,** which act after an InfoSec/CS incident has occurred.

According to the requirements of ISO/IEC 27001 [2], **the ISMS is a documented system,** based on evidence, records, etc., with the structuring of ISMS documentation in a "pyramidal" form across levels, which suggests the volume, contents, and involved personnel *(Fig. 3).*



Figure 3. ISMS documents

Compliance with the international data security standard for the payment card industry, PCI DSS [5], is a mandatory requirement for all organizations that store and process bank card transactions and is voluntary for those that only use electronic payment systems. In Moldova, we have both types of banks. According to Law 133 [6] of Moldova and at the EU level, GDPR [4],

such data must be protected, stored, processed, and disclosed by various organizations and entities only under certain legal conditions, and only if there are specific prescribed guarantees.

The importance, challenges, and major problems of InfoSec in banking activity are confirmed by the vital nature of information in modern societies, **assessed as the fourth essential element after water, air, and fire.** According to NIST, ISO, IEC, ITU, and other international bodies concerned with the InfoSec domain and the endorsement of best practices, information has become a fundamental asset of the organization, state, society, which must be appropriately protected. Moreover, ICT has become the essential element in the creation, processing, storage, transmission, protection, and destruction of information. On the other hand, the rapid evolution of ICT, e-business, e-education, e-governance, e-entertainment, Smart Home, IoT, IoB, etc., leads to a concurrent increase in informational risks and the way in which state institutions, private organizations, individual persons, and society as a whole should respond to the challenges and opportunities created by the technological revolution. The thesis provides compelling data on **losses from cyber-attacks** on InfoSec *(Fig. 4, [8])*, a comprehensive list of statistics and trends can be consulted at [8].

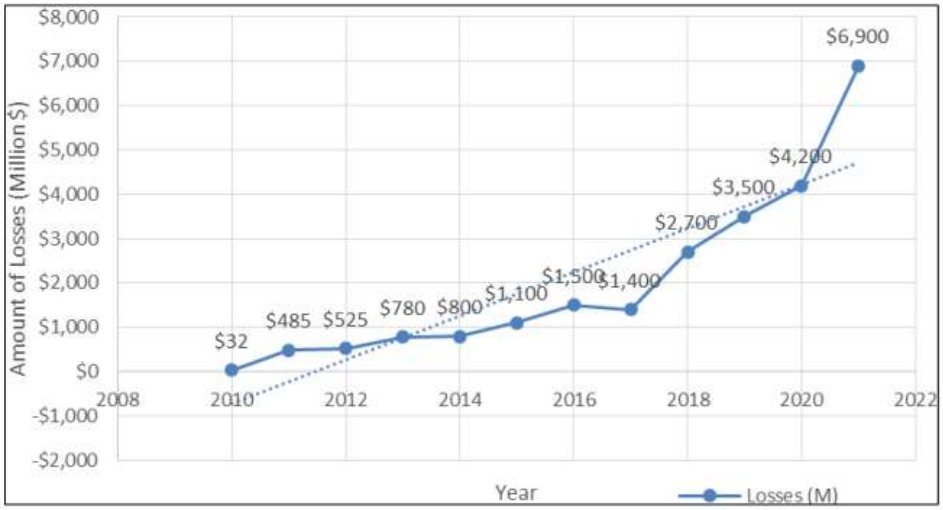


Figure 4. Amount of losses from cyberattacks in the years 2010-2021, USA

According to statistics, cybercrime remains a perpetual threat to the national and economic interests of countries and corporations. Information security has become essential, both for individuals and legal entities, as well as for society and the state as a whole, as a significant component of national and regional security. The costs of cybercrime have increased more than 13 times over five years, from 2018 to 2022, from $0.86 trillion to $8.44 trillion. The estimated growth for the next five years, from 2022 to 2027, is over three times, from $8.44 trillion to $23.82 trillion *(Fig. 5, [9])*. As a result, proper management of information security and the safety of

electronic transactions is crucial and becomes an essential element of good information practices based on ICT.

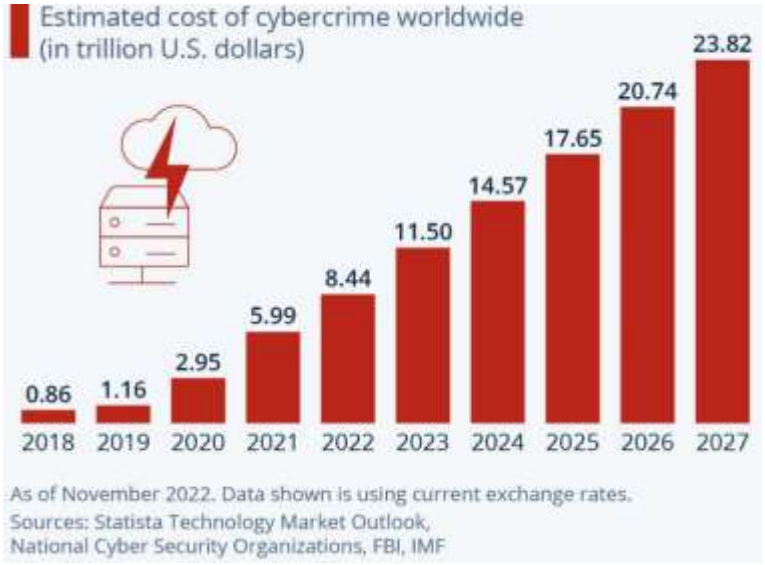


Figure 5. Rising costs of cybercrime

Threats, risks, attacks, and incidents related to InfoSec materialize through the exploitation of vulnerabilities that mostly originate from three primary sources:

- **Humans,** through their intentional or unintentional actions, e.g., loss, theft, or destruction of a laptop containing sensitive information, attacks carried out by hackers on a website, system, etc.
- **Critical infrastructure,** technologies, and business support systems *(information and communication networks, servers, devices, including peripherals, IoT, IoB, including the software embedded in all of these),* unable to maintain their respective functions due to failures, exploitation of vulnerabilities, etc.
- **Nature,** e.g., natural disasters, fires, floods.

A minimum set of informational resources that must be protected to reduce the level of fraud and threats to InfoSec particularly refers to the IT/IS environment:

- Personnel (employees, clients, suppliers);
- Tangible assets (documents, data, knowledge, expertise, records);
- Physical IT/IS assets (equipment, computers, routers, disks, etc.);
- Software (system, application, web, personal/commercial, DBMS, etc.);
- IT/IS services (internal, external, Internet Service Provider, etc.);
- Locations (headquarters, including virtual, websites, etc.).

The fight against the complexity of InfoSec in entities is supported by methods, tools, and techniques assisted by computers, which over time have become much more numerous and financially accessible.

It is worth mentioning **the instrumental applications of information security,** ranging from antivirus programs *(e.g., Top 10 best free antivirus tests [10])* to pre-audit CS tools *(e.g., Top CIS/SANS Controls v.8 [11], CSAT [12], CMMC [13], Free Cybersecurity Assessment [14], NIST Cybersecurity Framework [15]).* The use of these and other specialized professional tools helps entities eliminate information leaks, conduct pre-audit of CS *(detecting vulnerabilities, planning and carrying out continuous improvements, etc.),* and manage the increasingly complex task of ensuring information security. **Such instrumental programs are starting to be implemented even in companies with a relatively small number of employees.**

A useful tool in choosing software products can be **Gartner's Interactive Magic Quadrant** [16]. The interactive features of the Magic Quadrant allow for the generation of personalized views by adjusting the weights applied to each evaluation criterion, specific to the user, saving and sharing these views for internal analysis and decision-making.

In the conclusions of chapter 1, the dominance of contemporary world development within modern society is elucidated, expressed through e-transformation, continuous change of values, structures, phenomena, processes, ways of working, learning, entertainment, etc., through the massive use of ICT, Internet and Web in all areas of human activity, the development of the digital economy and the increased competitiveness of e-businesses; The growing significance of information, estimated at the level of the fourth vital element after water, air, and fire, information becoming one of the most important factors of social progress; The hyper-connectivity of corporate networks, IoT, IoB, and Wi-Fi networks to the global Internet, mass digitization leads to an increase in cyber-attacks. And the fact that InfoSec/CS has become a critical issue for business success and requires a comprehensive, in-depth approach, aligned with business strategies and objectives.

Chapter 2 examines some theoretical, methodological aspects and best practices of approaching InfoSec within the ISMS with the purpose of **justifying the choice of approaching CS through multi-profile maturity models.** The basic task is to align ISO, NIST, ISACA, CMMI, etc., with the requirements, needs of the organization, and specific contexts of quality management systems, InfoSec, business continuity, security incidents (events). This task is confirmed by the new edition of the paired standards ISO/IEC 27001:2022 [2] and ISO/IEC 27002:2022 [3], which have extended their highest title from "*Information Security"* to

"Information Security, **Cybersecurity, and Privacy Protection***",* emphasizing the integration of ISO/IEC 27001:2022 with ISO/IEC 27032:2023 [17].

In the thesis, it is eloquently demonstrated that the best practice standards in the field of information security constitute the foundation, the basis for the design and development of a multi-profile information security maturity measurement model. Some of these frameworks are mentioned in *Figure 6.*

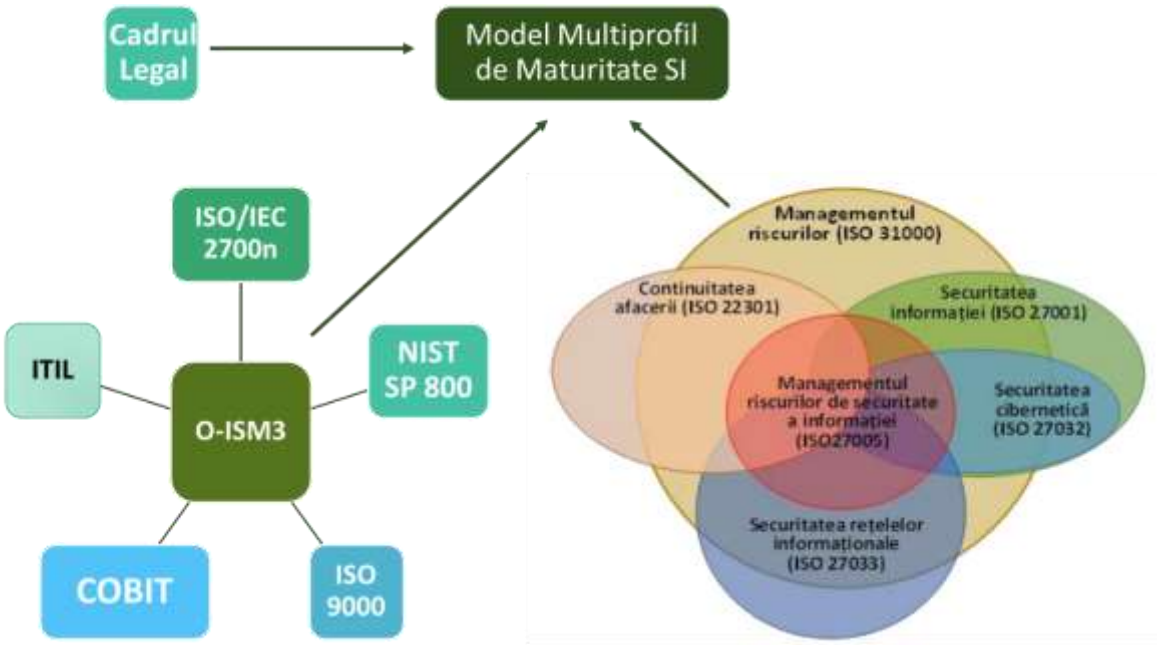


Figure 6. Correlation of some standards for the realization of M3SI

Based on the correlation of best practice standards, a generic maturity model was developed, from which typical information security profiles for industries (PSITI) are generated, initially adapted for the banking sector. This profile serves as a basis for individual PISI profiles, designed for evaluating the InfoSec of banks in Moldova. It should be noted that the models are versatile enough to be implemented in other sectors as well, such as the educational sector, governmental structures, medical services, etc. **The Relevance and Importance of the Addressed Topic**. Currently, the vast majority of individuals and legal entities, private and public organizations, governmental, etc., are present in the global digital/virtual space, without any well-defined and clearly delineated borders.

In all **The Relevance and Importance of the Addressed Topic**. Currently, the vast majority of individuals and legal entities, private and public organizations, governmental, etc., are present in the global digital/virtual space, without any well-defined and clearly delineated borders. **The Relevance and Importance of the Addressed Topic**. Currently, the vast majority of individuals and legal entities, private and public organizations, governmental, etc., are present in the global digital/virtual space, without any well-defined and clearly delineated borders.

frameworks/standards and best practices, **the main principles** of InfoSec are formulated as key requirements, such as: **the PDCA process approach, continuous improvement, customer focus, commitment and support from top management, employee involvement, evidence-based decision making, and management of relationships with stakeholders.** Additionally, in the realization of InfoSec, a number of other principles and paradigms are used, among which are **the risk-based approach [18], zero trust architecture [19], least privilege, security by design, defense in depth, Mayfield's paradox,** and others.

Mayfield's paradox [20] is graphically represented by two asymptotic curves in two-dimensional space, **the risk curve and the investment curve** with the system cost on the vertical axis and the quota of people that can access the system on the horizontal axis, with an optimum at the intersection of the curves *(Fig. 7).* The paradox highlights that perfect access *(without security restrictions)* and perfect security (without access restrictions) are extreme cases with costs tending towards infinity, between which an optimum must be found. As an illustration of Mayfield's Paradox, the Pareto rule/principle can be brought in for balancing the cost-security of CS measures.

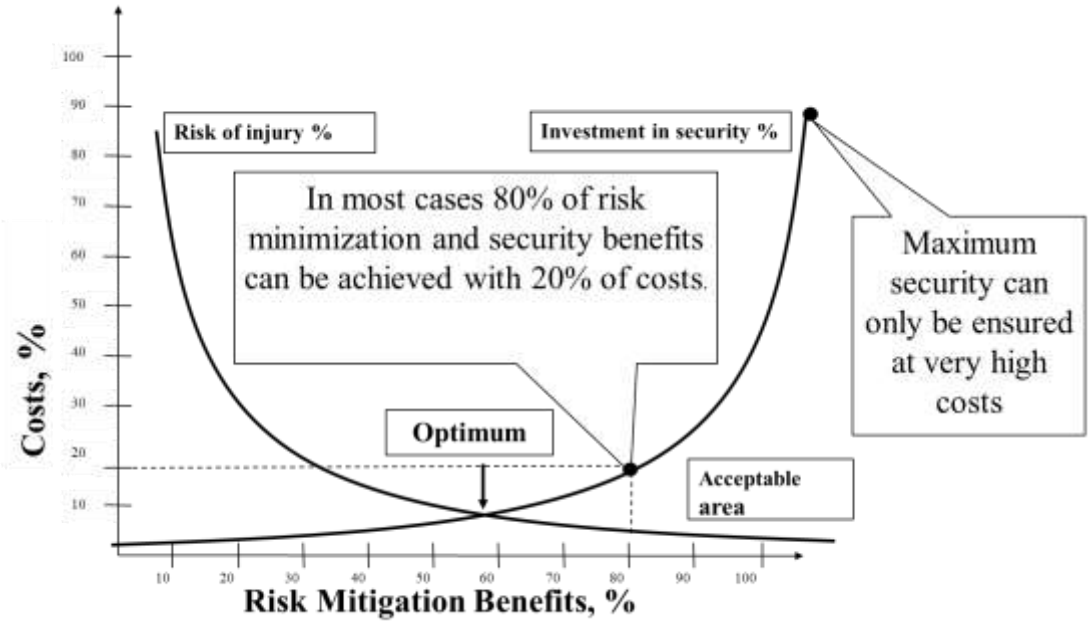


Figure 7. An illustration of the Mayfield paradox on the balance diagram

At a certain point, additional security becomes unrealistically costly, just as adding more users becomes unrealistically expensive, and the difference between these two costs is relatively small. The significance of this paradox lies in realistically correlating risks with the security budget, also confirmed by the ISMS principle of addressing only the valuable information for an entity in achieving its objectives:

- Moving right from the optimum signifies an investment in the future;
- Moving left from the optimum signifies falling behind.

Globally, the most widespread and recognized frameworks/best practices for addressing InfoSec/CS are:

- ISO/IEC 27001:2022 and the ISO27k family, an international standard setting with about 80 operational standards out of the 100 planned, which define the requirements for designing and managing an ISMS, including logical, physical, and organizational security aspects, as well as best practice recommendations.
- COBIT 2019 *(Control Objectives for IT, [21]*) from ISACA *(Information Systems Audit and Control Association).*
- The framework developed by the National Institute of Standards and Technology *(NIST, USA)* [22] in the special publications series NIST SP 800.x.
- The Open Information Security Management Maturity Model *(O-ISM3, 2017, [18], [19]),* developed by the independent consortium The Open Group, which is compatible with/and takes into account the requirements of ISO27k, COBIT, ITIL, and others.

All these emphasize **the holistic approach to InfoSec/CS based on risk, on adaptable**/customizable maturity models of prescribed processes, **on organizational security culture,** etc. The adaptability of the models refers to the size and complexity of the organization, the sector of activity, resource allocation, responsiveness to technological changes in the business environment, alignment with emerging technologies and work models, etc. The importance of maturity levels lies in the fact that they **provide a framework for evaluating the current situation to set improvement goals and measure progress.** As a result, organizations allocate resources efficiently, focusing on areas with the highest risks or those that require urgent improvements. A customizable model allows for prioritizing security initiatives based on the organization's specific risk assessment, ensuring that budget and efforts are directed where they can have the most impact. Focusing on continuous improvement encourages entities to constantly seek to enhance their information security practices and processes, promoting a cycle of continuous improvement. **Information security is not a static goal, but a dynamic process** that requires continuous adaptation to new threats, technologies, and changes in the business environment.

Ongoing training and awareness of the staff are vital to ensure that all members of the organization understand security risks and contribute to information protection. Typically, training and awareness differ across different categories of staff.

A significant aspect of this chapter is the risk-based approach to information security. **The risk management process is a cyclic, continuous, and systematic process** *(Fig. 8, [23]),* with

established responsibilities for identification, evaluation/measurement, monitoring, and adopting control measures with two decision points, either by accepting exposure to risk or by additional treatment to reduce the value of residual risk to an acceptable level.

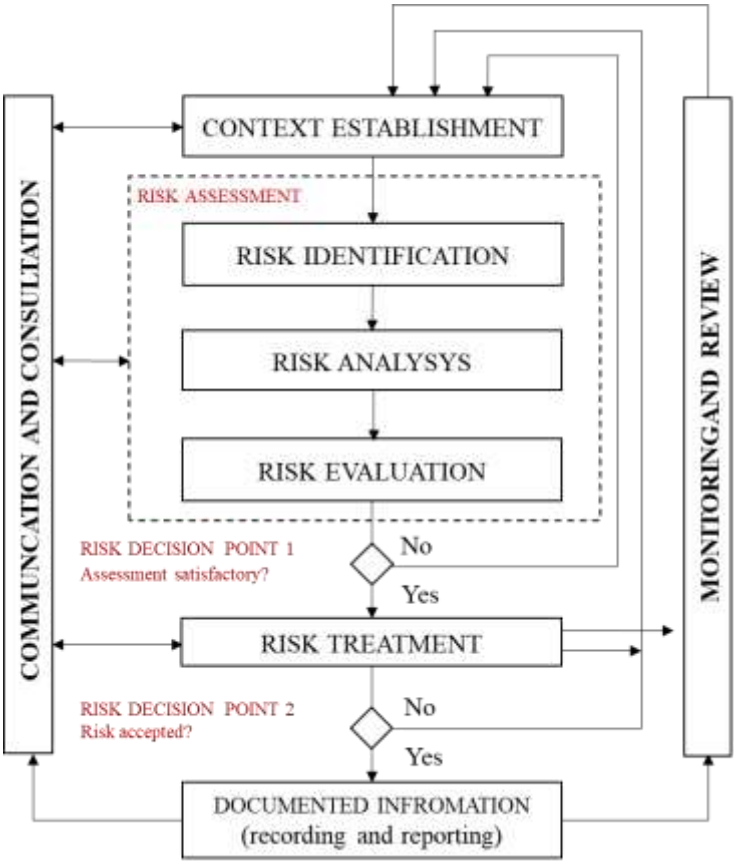


Figure 8. IS risk analysis and management process

The general flow of analysis and treatment according to ISO 27005:2022 [23] includes establishing the context *(Clause 7),* risk assessment *(Clause 8),* risk treatment *(Clause 9),* risk acceptance *(Clause 10),* risk communication and consultation *(Clause 11),* and risk monitoring and review *(Clause 12).* Additionally, the necessary activities for cyber risk analysis presented in Figure 2.10 are described in detail in other standards as well, such as ISO 27001:2022 [2], ISO 31000:2018, NIST SP-1800, and others.

The analysis, evaluation, and treatment of cyber risks focus on qualitative-quantitative analysis methods based on the standards ISO/IEC 27005 [23] and ISO 31000:2018, aiming to combat complexity and reduce the influence of the human factor by automating risk analysis as much as possible. Security risks are analyzed based on the likelihood of risk occurrence and severity, the impact on objectives if the risk occurs. To transition from qualitative to quantitative values of probability, impact, value, and risk level, semi-quantitative values are used, described in Tables A.1-A.5 ISO/IEC 2705:2022 [23] and *Tables 1-2* [24].

The final stage of the risk assessment process is **the assessment report,** which supports management in making appropriate decisions regarding budget, policies, and CS procedures.

After completing the evaluation and assessment of risk, the risk value is compared with the agreed risk acceptance criteria, and risk treatment is carried out, resulting in a residual risk *(Fig. 9).* The decision for treatment is taken in accordance with the risk analysis matrix *(Fig. 10, developed based on Table A.3 [23]).* The risk owner must approve the treatment of selected risks and must accept the residual risk according to predefined criteria.

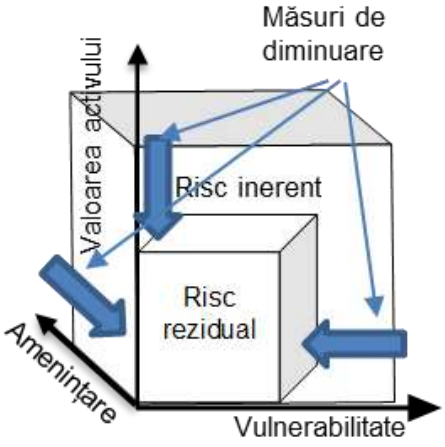


Figure 9. Residual risk vs inherent risk

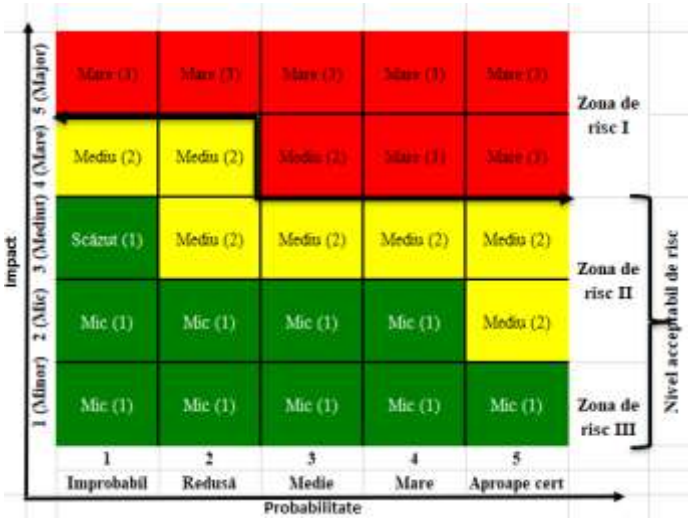


Figure 10. 5x5 3-level risk assessment matrix

In the diagram from Figure 10, the area in the upper-right (colored red) represents risks with high probability and high impact, for which controls must be applied to reduce the risk value. In the lower-left (colored green) are risks with low probability and low impact, which can be ignored (they do not seriously affect the business). The middle area (colored yellow) represents risks with medium probability and medium impact, which can be treated according to the criteria of the security policy.

Chapter ”3. Multi-profile Information Security Maturity Model (M^3SI)” presents the innovative and original part of the thesis on addressing InfoSec based on open standards, multi-level, multi-dimensional maturity models, with computer support, generating typical industry-specific information security profiles (PSITI) and customized individual information security profiles (PISI) in accordance with specific corporate policies, the guiding standards of the ISO/IEC 27k family, and the target values of the InfoSec maturity evaluation criteria.

Maturity is **a measure of an organization's capacity for continuous improvement** in management areas *(O-ISM3, 2017 [18], Muneer, 2023 [19]).* Maturity models represent **collections of best practices for measuring an entity's progression** from lower to higher levels of skill or “maturity”. Essentially, maturity models are sets of proven global best practices that

allow organizations to build and refer to key capabilities that address their most common business challenges. Although the vast majority of existing maturity models, e.g., O-ISM3 [18, 19], COBIT [21], ITIL, ISO 9001:2015, etc. are generally compatible with the requirements of ISO/IEC 27001:2022, there is no clear understanding of how the domains and core processes used by them relate. Unlike these various frameworks of best practices/international standards and isolated maturity models, **the multi-profile information security maturity model M^{3}SI developed in the thesis provides a unique and integrated universal view of InfoSec,** applicable to any entity, at any level, starting from the global/national regulatory and best practices framework, continuing with specific requirements for various industries PSITI and ending with the local/application level PISI, specific to the concrete requirements and contexts of an organization and/or its subdivisions and/or a mission, etc.

The innovative idea realized in the thesis through M^{3}SI also refers to **the relationship between the general model-industry-specific model-customized model** with different frameworks for addressing InfoSec. An entity can start by cloning an existing framework like PSITI, followed by adapting it according to current legislation. Thus, M^{3}SI is based on the best-known information security/best regulatory practices at the time and already mentioned above, *e.g., OISM3:2017, NIST SP 800-53 edition 5, NIST 800-207 Zero Trust Architecture, ISO/IEC 27001:2022, ISO/IEC 27002:2022, PCI-DSS version 4.x, COBIT:2019, etc.*

To some extent, M^{3}SI anticipated the changes in ISO/IEC 27001 and ISO/IEC 27002, 3rd edition from 2022, where the names of the standards were changed from *"ISO/IEC 27001:2013 Information Technology - Security techniques - Information Security Management Systems" to "ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems"*. This change emphasizes the unique approach to the three types of security mentioned in the standard title and facilitates the mapping of various security controls to different requirements and standards, bringing security concepts closer together.

M^{3}SI offers high flexibility so that it allows for adding, removing, or modifying new structured knowledge about existing threats and risks, controls, and metrics planned for evaluating the level of InfoSec maturity. M3SI is accompanied by a software application tool that allows generating typical industry-specific information security profiles/PSITI, e.g., education, banking, medicine, and customized into individual information security profiles/PISI at the level of a specific entity, e.g., Moldova State University, "Alfa Bank" commercial bank, or at the level of subdivisions or separate areas/spheres, e.g., the area of the electronic payments department of the commercial bank or the security area of the information systems with specific internal/external context requirements. A simplified hierarchical view of M3SI can be seen *(Fig. 11)*.

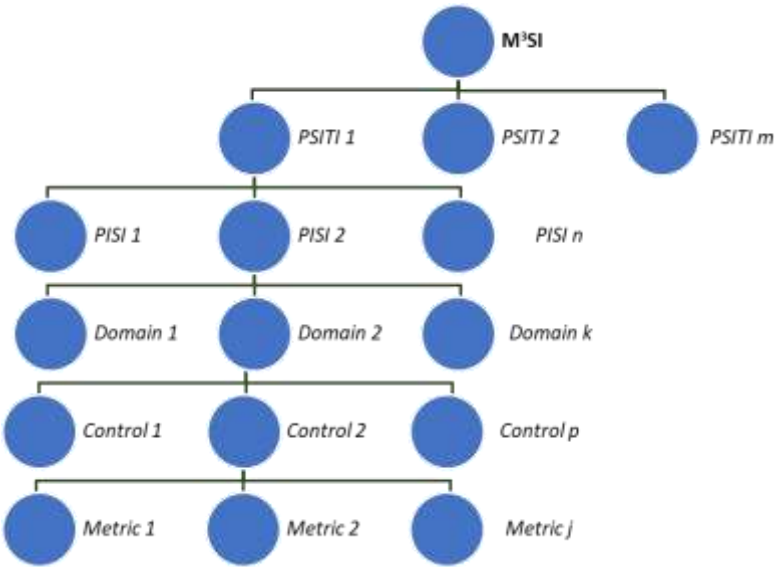


Figure 11. A simplified hierarchical view of maturity models in M³SI

At the highest level, M³SI comprises a certain number of pre-determined CS domains, established according to the general frameworks of the related mapping approach. The multi-profile model spans several industrial sectors with typical PSITI models, which in turn cover typical entities with similar PISI patterns *(Fig. 12)*.

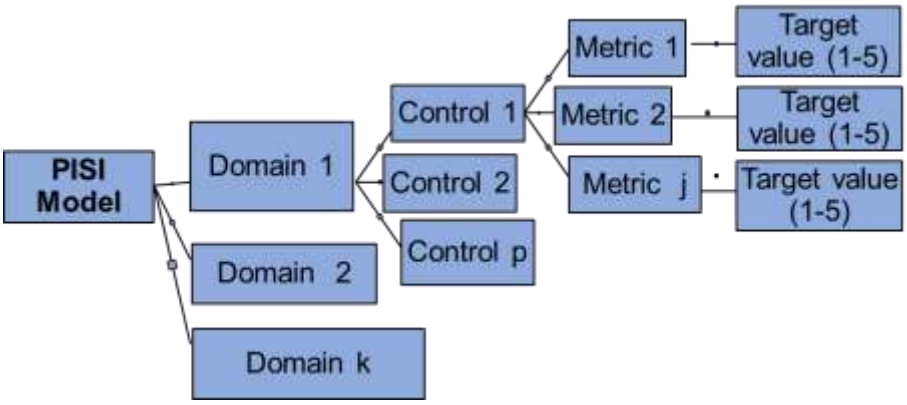


Figure 12. A PISI profiles vision

Typically, the characteristics of standard models for various industries (PSITI) are formulated in specific standards and regulations, such as *PCI DSS, GDPR*, globally applicable acts like *HIPAA*, and local regulations from supervisory bodies. The PSITI maturity profile might specify these requirements to meet the needs of management.

The PSITI model is not intended to provide a definitive answer to how good an individual ISMS is, but rather serves as a framework for structuring an individual ISMS or a specific CS profile, or for comparing the maturity of various typical entities.

Since security measures and controls are derived from the specific static and/or dynamic operational situations of the organization and the evaluation mission, PISI should be customized/interpreted on a case-by-case basis based on a PSITI or a similar PISI. Each specific

entity will create its own PISI profile according to its specific context, which will take into account the SMSI/SoA area and the established targets. Examples of PSITI and PISI can be seen in *(Fig. 13, Fig. 14).*

ID	Nume Control	Descriere	Risk	Niveluri de Maturitate	Actiuni
1	+ Cadrul de organizare a securității informației				
2	+ Managementul resurselor informaționale				
3	+ Securitatea Resurse Umane				
4	- Securitatea fizică și a mediului de lucru				
4.1	Zone de securitate	să prevină accesul fizic neautorizat, distrugerile și pătrunderile în interiorul băncii, precum și accesul la resursele informaționale.		1. Controalele sunt doar partial definite si/sau executate intr-un mod inconsecvent 2. Controalele sunt in vigoare si executate doar intr-un mod structurat si consecvent, dar informal 3. Controalele sunt documentate si executate intr-un mod structurat, formal si dovedit 4. Eficacitatea controalelor este evaluata si verificata periodic pentru calitate 5. A fost creat un sistem ecologic care sa asigure un control continuu si eficient si sa rezolve riscurile	Editeaza Sterge
4.2	Securitatea echipamentelor	să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI și întreruperea proceselor de activitate ale băncii.		1. Controalele sunt doar partial definite si/sau executate intr-un mod inconsecvent 2. Controalele sunt in vigoare si executate doar intr-un mod structurat si consecvent, dar informal 3. Controalele sunt documentate si executate intr-un mod structurat, formal si dovedit 4. Eficacitatea controalelor este evaluata si verificata periodic pentru calitate 5. A fost creat un sistem ecologic care sa asigure un control continuu si eficient si sa rezolve riscurile	Editeaza Sterge
5	+ Managementul comunicațiilor și operațiunilor				
6	+ Controlul accesului la resursele informaționale				
7	+ Achiziționarea, dezvoltarea și mentenanță sistemelor de aplicații				
8	+ Managementul incidentelor de securitate a informației				
9	+ Managementul continuitatii activitatii				
10	+ Conformitatea				
11	+ Auditul intern al securității informației				

Figure 13. A fragment of PSITI for banking activity in the Republic of Moldova

ID	Nume Control	Descriere	Nivel curent	Evidente
1	- Cadrul de organizare a securității informației		3.25	
1.1	Politica de securitate a informației	să asigure orientarea generală de management și sprijinul pentru securitatea informației în conformitate cu cerințele de afacere, legislația și actele normative aplicabile.	3	lista
1.2	Organizarea SMSI	să asigure cadrul intern adecvat pentru managementul securității informației.	4	lista
1.3	Relația cu terțele părți	să asigure securitatea informației în relația cu terțele părți care prestează sau beneficiază de servicii ce implică informația băncii	3	lista
1.4	Externalizarea serviciilor TI	să asigure securitatea și continuitatea serviciilor TI externalizate către furnizori externi de servicii.	3	lista
2	- Managementul resurselor informaționale		2.67	
2.1	Responsabilitatea pentru resurse	să asigure stabilirea și asumarea responsabilității pentru protecția corespunzătoare a resurselor informaționale ale băncii.	3	lista
2.2	Clasificarea informației	să asigure faptul că informația beneficiază de un nivel de protecție adecvat, proporțional importanței ei, reglementărilor aplicabile și amenințărilor aferente	2	lista
2.3	Managementul riscurilor	să asigure faptul că banca isi gestioneaza riscurile intr-o maniera eficace si eficienta	3	lista
3	- Securitatea Resurse Umane		3.00	
3.1	Înainte de angajare	să asigure faptul că noii angajați, terțele părți, precum și reprezentanții acestora sunt corespunzător verificați înainte de acordarea accesului la sisteme, iar responsabilitățile pentru securitatea informației sunt adecvat stabilite, comunicate și asumate.	4	lista
3.2	Instruirea	să asigure faptul că cerințele de securitate sunt cunoscute în măsură suficientă de către angajații băncii, terțele părți, precum și reprezentanții acestora.	3	lista
3.3	Pe perioada angajării	să asigure faptul că cerințele de securitate sunt respectate necondiționat de către angajații băncii, terțele părți, precum și de reprezentanții acestora, iar responsabilitățile și răspunderea juridică ale acestora sunt stabilite și conștientizate corespunzător.	3	lista
3.4	Încetarea contractului sau schimbul locului de muncă	să asigure faptul că angajații, terțele părți, precum și reprezentanții acestora încetează relația cu banca într-o manieră controlată din punct de vedere al riscurilor de securitate.	2	lista
4	- Securitatea fizică și a mediului de lucru		3.50	
4.1	Zone de securitate	să prevină accesul fizic neautorizat, distrugerile și pătrunderile în interiorul băncii, precum și accesul la resursele informaționale.	4	lista
4.2	Securitatea echipamentelor	să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI și întreruperea proceselor de activitate ale băncii.	3	lista

Figure 14. A fragment of PISI for a hypothetical bank

In addition to *Domains/Areas* and *Controls*, PISI also includes: *the expected maturity level; the identified maturity level; a list of rigorous proofs and arguments attached,* documenting the

identified maturity level. Ultimately, the evaluation result according to PISI enables the identification of steps for continuous improvement of information security. Additionally, it is possible to accumulate a history of domains and incremental improvements, which may occur in the analyzed entity from month to month, quarter to quarter, or year to year, depending on the frequency imposed by business requirements.

The M^{3}SI application is designed to meet the challenges and complexities of InfoSec and qualitatively differs from other common tools by:

a) **Synthesizing and systematizing** knowledge about various InfoSec frameworks and assessment tools/questionnaires, including defining the five maturity levels in a single adaptable and extensible cumulative database;

b) **The universal applicability of the application,** starting from the ISO/IEC 27001:2022 controls, which can be expanded/reduced, e.g., to the Top 20 CIS Controls [11], predominantly internet-oriented; CMMC, predominantly cybersecurity-oriented; PCI DSS, focused on bank card transactions, etc.

c) **Accumulating the history** of the entity's maturity levels assessments according to specific PISI and missions, tracking progress, dynamics, etc.;

d) **Ensuring evaluation comparability** due to the formalization of evaluation criteria and InfoSec metrics.

To use the application integrating the generic M3SI model, PSITI, and PISI, the user must:

1. **Define the scope** of the ISMS or the evaluation mission, starting from the industry-typical model, by removing/adding/modifying, as needed, specific controls in M^{3}SI and PSITI, dictated by the needs and constraints of the organization;

2. **Generate the individualized** information security maturity **profile** PISI (Possibly by identifying a similar/close PISI and adapting it, or by initially constructing a PISI by combining control domains and corresponding controls in accordance with the risks and threats characteristic of the industry and entity);

3. **Complete the responses to the list of questions** and/or select the metrics of the respective criteria (from the dropdown menus on the pages of each control included in PISI). Based on the responses to each question *(choices from dropdown lists or input of measurement results of evaluation criteria),* the application automatically determines the maturity level scores according to the metrics provided on controls and domains, and then displays the resulting "Report" as **radar charts and/or detailed bar charts on the control domains** according to the scale/colors of the risk analysis matrix [23].

4. **Implement the improvement recommendations** based on the conducted evaluation/ report. The obtained scores are used either to measure the organization's progress, to formulate objectives/tasks for improvement, to mitigate risks according to the needs and constraints of clients and the organization, or to ensure an evolutionary transition from an ad-hoc individual effort (initial maturity level) to a consistent and optimizable organizational approach of continuous CS improvement (highest level of maturity).

The M^{3}SI usage scenario steps include updating PISI (possibly the knowledge base as well) according to the mission, conducting the evaluation, documenting, and displaying the evaluation results. The M^{3}SI web application interface is intuitive, easy to use, and after the initial launch displays two operating areas, Zone 1 and Zone 2, which is structured into three sub-zones 2.1-2.3 *(Fig. 15).*

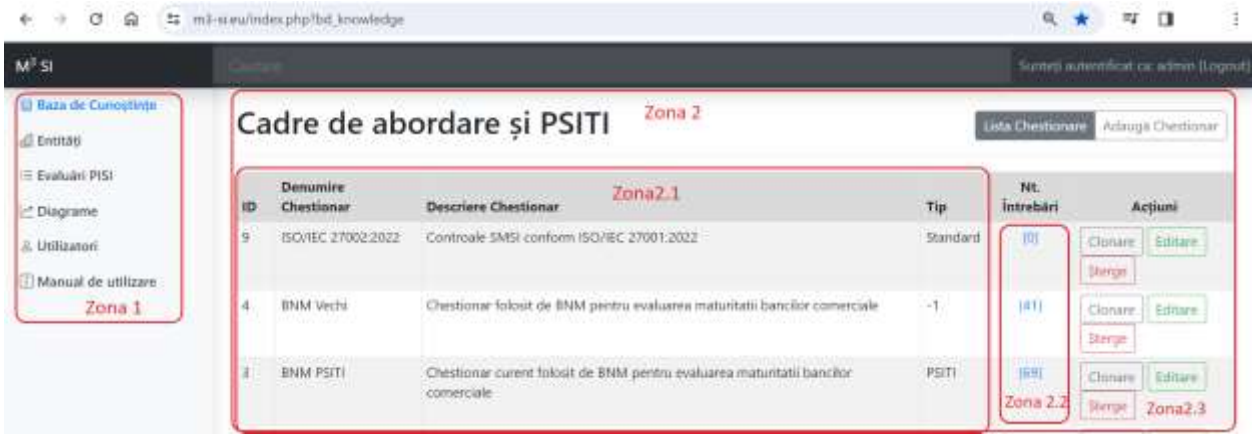


Figure 15. The M^{3}SI interface overview

The first area *(Zone 1, on the left)* contains a list of functional menus. These can be accessed by traditionally selecting and activating them with a ***Click*** when the cursor is placed over the selected object or by pressing ***Enter***. The selected object is highlighted in blue text. **Zone 2**, the workspace, is the main screen area where all instances of the selected object and the options for manipulating them are displayed. This area has three subzones: the list of objects with some identification characteristics *(Zone 2.1)*, the manipulation/action options such as cloning, deleting, editing with the selected object, also highlighted by color *(Zone 2.3, Fig. 15):* **Edit** name and type of object - in green and **Delete** - in red, on the right side of the screen. Also in this area, records can be edited, attributes of best practice frameworks can be entered, evaluation data can be input, etc., by activating the blue button with the number of records of the selected object *(Zone 2.2, Fig. 15).*

The database (DB) of the M^{3}SI model encompasses knowledge about the best practices, models, standards, and InfoSec tools that apply at the global, national, and local levels. The main content of the DB consists of knowledge about the areas and controls of InfoSec/CS, drawn from

the most widespread frameworks for addressing InfoSec, such as OISM3:2018, NIST SP:2018, the ISO 27k family including ISO/IEC 27001:2022, ISO/IEC 27004, ISO/IEC 27032:2023, ISO/IEC 27033 (2012-2016), PCI DSS version 4.x, COBIT:2019, ISO/IEC 20000-1:2018, ITIL version 4:2019, and adapted by the author to meet the needs of the application. **The author's significant contribution** in creating the content of the knowledge base lies not only in their synthesis but also in **defining the evaluation criteria across the five maturity levels.**

Examples of displaying reports in charts form can be seen *(Fig. 16).*



Figure 16. Examples of summary evaluation charts for CB "Alpha"

The two-colored areas on the radar chart represent the scores – the current target (blue) and the actual current score (purple) across the control areas. The graphical report is useful in all cases of InfoSec audit missions (internal performance, pre-certification audit) or for visually analyzing gaps and planning improvements in the form of an integrative one-page overview.

On each of the control areas/domains, bar charts are displayed. These are useful for pinpoint analyses, e.g., to justify projects based on gap analysis. *In Figure 17*, two such domains are displayed, each with five controls, with blue bars reflecting the target values and red bars showing the actual values of the controls. As can be seen from *(Fig. 17)*, the entity has significant room for improvement in the control *ID.03 Super Users* within *the Access Management* domain and moderate reserves in *the Governance domain, controls GU.01 Strategy; GU.02 Policies; GU.03 Plan/Roadmap; and GU.04 Enterprise Information Architecture.*

For further details regarding evaluation reports and graphical displays, explore the application. Typically, each PISI has its own metrics, oriented towards achieving specific objectives. The determination of maturity is based on the review of ISMS documentation, staff

interviews, performing measurements, and gap analyses for each of the security domains included in PISI and the measured values.

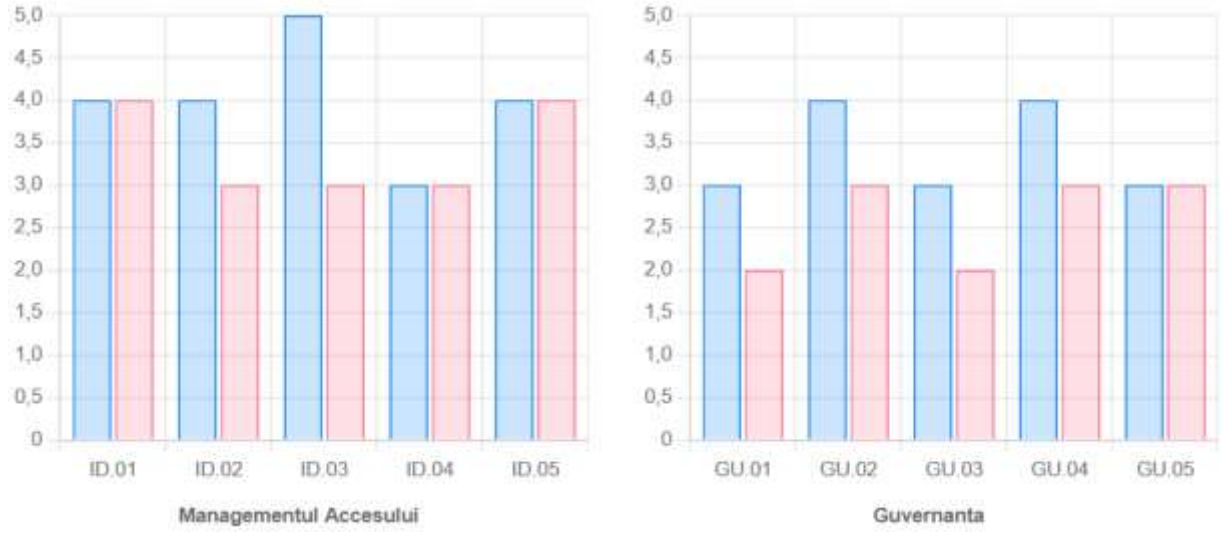


Figure 17. Example of charts on separate domains

The assessment of levels for each of the PISI domains is conducted according to the criteria developed/metrics of the model. For example, the measurement score for fulfilling a criterion can be "Compliant", "Partially Compliant", or "Non-compliant". If a specified criterion has multiple metrics and they are assessed with different values, the aggregate score is typically evaluated at the level of the lowest metric value or an average value.

Ultimately, the M^{3}SI platform has a series of advantages and innovative features:

1. It is an **integrated platform for designing, developing, evaluating, and continuously improving InfoSec;** a practical method and a tool for determining InfoSec risks.
2. **The support application generates and displays the evaluation result in the form of visual charts,** which facilitate gap analysis. Based on these, the board of directors, auditors, and supervisory bodies obtain objective, consistent, and qualitative information on the state of InfoSec and justify their decisions.
3. **InfoSec officers and teams of IT/SI/Cybersecurity professionals** eliminate much of the routine involved in planning future tasks.
4. The M^{3}SI platform allows for **the accumulation of historical data, the evolution of InfoSec domains, and incremental improvements,** which may occur in the analyzed entity from month to month, quarter to quarter, or year to year, depending on the frequency imposed by business requirements.
5. The M^{3}SI platform, accessible at *https://www.m3-si.eu*, enables **comparative analysis of the maturity of typical entities,** such as banks, universities, hospitals, etc.

FINAL CONCLUSIONS AND RECOMMENDATIONS

Within the thesis, **the state of InfoSec/CS in various entities was analyzed, with losses and challenges in CS,** particularly in the banking sector, being identified. Some problems were found that could be overcome by changing the InfoSec approach paradigm, geared towards management.

Various globally recognized InfoSec frameworks were also analyzed to synthesize and justify an integrative maturity model that allows the use of all best practices. The knowledge base of the M3SI model incorporates the most recommended approaches based on globally accepted best practice standards, such as COBIT from ISACA, ISO 27k from ISO, the NIST SP 800.x series, PCI DSS, and the risk-based approach.

In reality, many entities find it difficult to obtain a unique, objective, and comprehensible vision of all cybersecurity risks and capabilities. This requires much time, skills, and special expertise, which not all entities always have. **Complexity is a very important factor in achieving a unique and objective view of InfoSec risks and capabilities.** This is also because risks are continuously increasing, caused by the integration of new ICT applications in virtually all spheres of human activity, the emergence of new vulnerabilities, new threats, and attacks. And because **InfoSec risk management is a continuous process** that should allow the organization to achieve its established business objectives in **a constantly changing environment.**

Although it is a quite complex and routine process, risk management leads to an increase in the level of InfoSec maturity and the organization as a whole. In this sense, **the best practices with the most relevant recommendations are those from the ISO/IEC 27005 standard.** These involve risk assessment based on qualitative analysis of probability with ratings like: *5 – Frequent; 4 – Likely; 3 – Occasional; 2 – Seldom; 1 – Unlikely,* and impact types like *5 – Catastrophic, 4 – Critical, 3 – Serious, 2 – Significant, 1 – Minor,* broadly similar to the five maturity levels. From here, the calculation of risk value as the product of probability and impact follows, sorting risks in descending order of their value and treatment according to adopted strategies.

Implemented correctly, cybersecurity in the conditions of mass teleworking and remote access to sensitive information presupposes a new approach not just based on technical-technological solutions, ICT, and traditional information systems, but also on the security of mobile, home devices, and on the security of IoT, IoB, cloud, etc., including changing the management systems approach, which would allow effective control and monitoring of cyber risks.

Another significant issue is **how cybersecurity information is collected, managed, reported/disseminated, and used** by respective roles within entities, monitoring, and real-time support of which is quite difficult. **Evaluating and tracking cybersecurity by manually collecting and recording information** on spreadsheets or other tools to track numerous threats, initiatives/projects, programs, and security processes, aligning InfoSec to numerous legal frameworks, approaches, and various regulations **are no** longer **efficient.** It becomes extremely difficult not only to collect and evaluate data but also to update and maintain the consistency of numerous documents to obtain a coherent picture of all aspects of information security, to compare and analyze evolution over time and/or between entities.

To solve these problems and not only, within the thesis, a prototype for planning-evaluation of InfoSec was created based on a multi-profile maturity model M3SI, with typical PSITI profiles and individual PISI profiles, with predefined evaluation criteria and procedures, which allows different evaluators to reach approximately the same results. The model is supported by an original software application that reduces the volume of routine work.

All these make managing and ensuring InfoSec within entities or conglomerates of entities from the same activity domain more transparent, simpler, and easier to understand and apply.

Indeed, on the one hand, internal and external contexts can differ significantly for different entities and, as a result, there cannot be a single evaluation model. Each PISI model pursues its objectives and solves its problems according to the mission. On the other hand, it is difficult to apply personalized maturity models without understanding the basic model/general problem statement, typical industry profiles, and approaches. Designed to optimize an entity's security performance in a continuously changing global environment, **the multi-profile M^{3}SI model, typical industry PSITI profiles, specific PISI InfoSec evaluation profiles, and the accompanying application, provide guidance and support for the organization to improve InfoSec processes,** including the ability to manage, develop, acquire, and maintain InfoSec controls, tools, products, and services. All these help the organization to assess the maturity level, establish improvement priorities, and implement these improvements in contexts and processes specific to an entity.

At its core, **M^{3}SI represents a generic, cumulative, adaptable, and extensible** database regarding frameworks, zones, controls, criteria, and InfoSec targets, from which typical industry PSITI profiles are generated (e.g., education, health, banks), which in turn serve as a basis for constructing/generating specific individual PISI profiles, also based on the accumulated experience of similar entities with similar profiles.

With M^{3}SI and its support application, maturity can be systematically evaluated, more broadly or narrowly, more concretely to identify, notice the gaps, "starting points" and to apply the model to a wider range of tasks and situations or more broadly **to plan changes in a more coordinated and reasonable way, including to compare maturity levels at different times and/or maturity levels of different entities** with similar activities, etc.

In reality, **the five levels of maturity signify the stages through which a launched ISMS** passes. PISI refers to the key capabilities of the ISMS, controls, tests/questionnaires, typical templates, and best practices for evaluating and measuring the level of maturity established in various frameworks and globally recognized standards such as ISO, NIST, ISACA, etc. The criteria, also established based on best practices, are intended **for assessing** (measuring and evaluating) and **continuously improving InfoSec**, to meet both the specific needs and particular security policies of the organization, as well as global standards. The accompanying M^{3}SI application provides intelligent support for generating consistent evaluation profiles for InfoSec maturity through continuous improvement, as well as various ways of displaying reports, better suited to the purpose of maturity measurement, such as tracking dynamics over time or conducting internal performance audits or pre-certification audits, etc.

The **"multi-profile model – typical industry profile – specific entity profile"** approach and the corresponding M^{3}SI application (https://www.m3-si.eu) for automated support are useful both for specific security roles that need to be up-to-date with the current state, maintain necessary documents, ensure reporting/information, and for all those who need access to security information, such as auditors, inspectors, and managers.

In perspective, **M^{3}SI could collaborate with other similar tools,** like CIS CSAT, C2M2, etc., including at the level of data import/export and displaying integrated reports obtained from common data.

The results implementation. The developed M3SI model and the support web application have been implemented in NBM, confirmed by an **Implementation Act,** with practical illustration for a hypothetical *"Alfa"* bank *(Illustration based on a real bank would have violated InfoSec for that entity).* However, the M^{3}SI model and the corresponding application can be directly applied to any bank in RM, with the necessary adaptation of the PISI profiles; and also, for any other industries and entities with only minor adaptations of the database content and/or the PSITI and PISI profiles.

BIBLIOGRAPHY

All web sources, including those from the thesis text, were checked as of February 28, 2024.

[1] *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[2] *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

[3] *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls*

[4] *General Data Protection Regulation (GDPR) nr. 2016/679.* Available at: https://gdpr-info.eu/

[5] *The Complete Guide to PCI-DSS 4.0.* Available at: https://colortokens.com/blog/pci-dss-4-0/

[6] *Lege Nr. LP133/2011 din 08.07.2011privind protecția datelor cu caracter personal, adoptată de Parlamentul RM, cu modificări LP52 din 12.03.20, MO84/14.03.20 art.88; în vigoare din 14.03.2020*

[7] *ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*

[8] *239 Cybersecurity Statistics (2023).* Available at: https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/

[9] FLECK, A. *Cybercrime expected to skyrocket in coming years. Dec. 2, 2022.* Available at: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[10] *Cele mai bune teste antivirus gratuite 2024.* Disponibil la: https://top10programeantivirus.com/cel-mai-bun-antivirus-gratuit/

[11] *CIS Controls Version 8. (CIS/SANS TOP 20 Security Controls).* Available at: https://www.cisecurity.org/controls/v8/?utm_source=website&utm_medium=email&utm_campaign=v8_release/

[12] *CIS Controls Self-Assessment Tool or CIS CSAT.* Available at: https://csat.cisecurity.org/

[13] *Cybersecurity Maturity Model Certification v.1.02 (2020).* (CMMC 1.2, 2020) Available at: https://www.acq.osd.mil/cmmc/draft.html/

[14] *Free assessment of your cyber security defenses.* Available at: https://www.itgovernance.co.uk/free-assessment-of-your-cyber-security-defences/

[15] *The NIST Cybersecurity Framework (CSF) 2.0 (2024).* Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf/

[16] *Gartner Magic Quadrant.* Available at: https://www.gartner.com/en/research/methodologies/magic-quadrants-research

[17] *ISO/IEC 27032:2023. Cybersecurity – Guidelines for Internet security*

[18] The Open Group. *Open Information Security Management Maturity Model (O-ISM3, 2017),* Version 2.0. Available at: https://www.opengroup.org/forum/security/infosecmanagement/

[19] MUNEER, A. et al *A Balanced Information Security Maturity Model Based on ISO/IEC 27001:2013 and O-ISM3. International Journal of Innovative Science and Research Technology, Volume 8, Issue 6, June, 2023, p,2444-2450. ISSN No:-2456-2165*

[20] MAYFIELD, R., CVITANIC, J. *Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security*. Information Systems Control Journal, 2, 2001, ISACA. p. 32-35.

[21] *COBIT® 2019 Framework: Governance and Management Objectives*. ISACA, 2019. -300 p. Available at: https://www.iso27001security.com/html/iso27000.html/

[22] National Institute of Standards and Technologies. *Special Publication 800 series, Computer security.* Available at: https://csrc.nist.gov/publications/sp800

[23] *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks*

[24] **BRICEAG, V.**, BRAGARU, T. *Evaluarea riscului securității cibernetice.* Revista Economica, 2(122), SEP ASEM, 2021, pp. 138-147. ISSN 1810-9136

[25] *Amenințări generice la adresa securității cibernetice.* ENISA (2020). Disponibil la: https://dnsc.ro/vezi/document/amenintari-generice-securitate-cibernetica/

[26] *CVE (Common Vulnerabilities and Exposures, 2021).* Available at: https://cve.mitre.org/

[27] *Cybersecurity Maturity Model Certification Guide (CMMC, 2022). Available at:* https://www.varonis.com/blog/cmmc-compliance/

[28] *Cybersecurity Capability Maturity Model (C2M2, version 2.1, 2022).* Available at: https://c2m2.doe.gov/C2M2%20Version%202.1%20June%202022.pdf

LIST OF PUBLICATIONS ON THE THESIS TOPIC

1. BRAGARU, T., **BRICEAG, V.,** MALCOCI, V., GALAICU V. (2019). *Securitatea informației vis-a-vis de securitatea informațională.* Revista Studia *Universitatis* Moldaviae, 2(122), seria „Științe exacte și economice”, CEP USM, 2019, pp. 38-47. ISSN 1857-2073; ISSN online 2345-1033
2. BRAGARU, T., **BRICEAG, V.** *Evaluarea securității informației organizației în baza unui model de maturitate*. IN: Materialele conferinței științifico-practice internaționale „Teoria și practica administrării publice”, Chișinău, AAP, 22 mai 2020, pp.248-252. ISBN 978-9975-3240-9-0
3. BRICEAG, V**., BRAGARU, T.** *Evaluarea riscului securității cibernetice.* Revista Economica, 2(122), SEP ASEM, 2021, pp. 138-147. ISSN 1810-9136
4. **BRICEAG, V.** Inteligent support for assessing the level of maturity of information security. International Conference „Mathematics & Information Technologies: Research and Education” (MITRE - 2021). Abstracts. Chișinău: CEP USM, 2021. -p.94. ISBN 978-9975-158-19-0. Available at: https://ibn.idsi.md/vizualizare_articol/134317
5. **BRICEAG, V.,** BRAGARU, T. Sustainable Curricular assurance of the information security management course. International Conference „Mathematics & Information Technologies: Research and Education” (MITRE - 2021). Abstracts. Chișinău: CEP USM, 2021. -p.118. ISBN 978-9975-158-19-0.
6. BRAGARU, T., **BRICEAG, V**. Sustainable cybersecurity training for modern society. Sustainable cybersecurity training for modern society. Proceeding of International Teleconference of young researchers "Creating the Society of Consciousness" (TELE-2022), 11th Edition, 18-19 March 2022. ARA Journal of Sciences, Nr. 5, 2022, pp.30-41. ISSN: 0896-1018. Available at: https://www.americanromanianacademy.org/_files/ugd/754172_0c407fa356a04c2a8a000f6a3f92bae8.pdf
7. BRAGARU, T., **BRICEAG, V.** Sustainable cybersecurity training for modern society. The thesis of international teleconference of young researchers "Creating the Society of Consciousness" (TELE-2022), 11th Edition of 18-19 March 2022. Society. Consciousness. Computer. Volume 8 (2022). Editorial Office "Vasile Alecsandri University of Bacău”, Romania, Bacău, 2022, p.32. ISSN 2359-7321. Available at: https://ibn.idsi.md/vizualizare_articol/179237
8. **BRICEAG, V.** *Model Multiprofil de Maturitate a Securității Informației (M^3SI).* Revista Română de Informatică și Automatică (RRIA), ISSN 1220-1758, vol. 32, nr. 1, pp. 99-112. ICI București, 2022. Disponibilă la: https://rria.ici.ro/en/vol-32-no-1-2022. ISSN 1220-1758

ADNOTARE

BRICEAG Valentin: „Analiza și creșterea nivelului de maturitate a sistemului de management al securității informației pentru entități din Republica Moldova (pe exemplul băncilor comerciale)”.

Teză de doctor în informatică, Chișinău, 2024.

Structura tezei: teza este scrisă în limba română și constă din introducere, trei capitole, concluzii generale și recomandări, bibliografie 93 de titluri și 4 anexe. Teza conține 141 de pagini cu text de bază, 54 figuri și 10 tabele. Rezultatele obținute sunt publicate în 8 lucrări științifice cu volum total de circa 7 coli de autor.

Cuvinte-cheie: Securitatea Informației (SI), Securitatea cibernetică (CS), Sistem de Management al Securității Informației (SMSI), Model Multiprofil de Maturitate a Securității Informației (M^3SI), Baza generică de date M^3SI, Profil de securitate a informației tipic unei industrii (PSITI), Profil individual de securitate a informației (PISI) pentru o entitate concretă.

Scop: elaborarea unui model multiprofil de maturitate a securității informației cu suport informatic pentru evaluarea și creșterea nivelului de maturitate.

Obiective: Crearea unei baze generice de date M^3SI privind cunoștințele despre cadrele de abordare, cerințe, amenințări, riscuri și controale de securitate a informației; Elaborarea aplicației instrumentale de suport a modelului multiprofil M^3SI, a profilurilor tipice unor industrii PSITI și a profilurilor PISI pentru entități concrete; Generarea, aprobarea și validarea unui profil tipic PSITI pentru activitatea bancară, stabilirea valorilor țintă ale criteriilor de măsurare și evaluarea conform PISI.

Noutatea și originalitatea științifică: modelul generic M^3SI, profilul tipic PSITI și profilurile particulare PISI cu controale, criterii și metrici specifice, instrumentul software de suport pentru M^3SI și procesul de evaluare sunt originale și potrivite pentru diferite entități și contexte diferite de utilizare.

Rezultatul obținut care contribuie la soluționarea unei probleme științifice importante îl constituie baza de cunoștințe despre cadrele de abordare și controalele de securitate a informației și generarea modelelor multiprofil conforme unor cerințe tipice comune și specifice individuale, pentru cazuri particulare, concrete.

Semnificația teoretică este determinată de sintezarea bazei de cunoștințe, a modelelor, profilurilor, controalelor de securitate a informației, a criteriilor de evaluare și măsurare a maturității conform cerințelor tipice și particulare.

Valoarea aplicativă constă în aportul substanțial al modelelor, profilurilor generate și a aplicației de suport pentru măsurarea și evaluarea nivelului de maturitate a securității informației, aplicabile pentru un cerc larg de organizații și utilizatori evaluatori, auditori ai securității informației.

Implementarea rezultatelor: modelele M^3SI, PSITI, PISI și aplicația de suport au fost implementate în NBM pentru activitățile de supraveghere și evaluare a SI a CB din Moldova.

ANNOTATION

BRICEAG Valentin: "Analysis and Enhancement of the Information Security Management System Maturity Level for the Republic of Moldova Entities (Case Study - Commercial Banks)".

PhD thesis in computer science, Chisinau, 2024.

Thesis structure: the thesis is written in Romanian and consists of an introduction, three chapters, general conclusions and recommendations, a bibliography of 93 titles and 4 appendices. The thesis contains 141 pages of basic text, 54 figures and 10 tables. The obtained results were published in 8 papers with a volume of over 7 sheets of author.

Keywords: Information Security (IS), Cyber Security (CS), Information Security Management System (ISMS), Multi profile Information Security Maturity Model (M^3SI), Generic Database M^3SI, Information Security Profile Typical of an Industry (PSITI), Individual Information Security Profile (PISI) for a specific entity.

Research purpose: the development of a multi-profile information security maturity model with TI support for evaluating and increasing the maturity level of information security.

Research objectives: Create a generic M^3SI database of knowledge about IS approach frameworks, requirements, threats, risks and controls; Development of the instrumental support application of the M^3SI multi-profile model, of the typical for an industry profile PSITI and of the individual PISI profile for concrete entity; Generating, approving and validating a typical PSITI profile for banking activity, establishing the target values of the measurement criteria and evaluation according to PISI.

Scientific novelty and originality: The generic M^3SI model, the typical PSITI profile and the particular PISI profiles with specific controls, criteria and metrics, the software tool supporting the model M^3SI and the evaluation process are original and suitable for different entities and different contexts of use.

The obtained result, which contributes to solving of an important scientific problem, is the database with the knowledge about the information security approach frameworks and controls and the generation of multi-profile models conforming to typical common and specific individual requirements, for particular, concrete cases.

The theoretical significance it is determined by the synthesis of the knowledge base, information security models, profiles, controls and their evaluation and measurement of the criteria for evaluating and measuring their maturity according to typical and particular requirements.

The applicative value: it consists in the substantial contribution of the generated models, profiles and the supporting application in the measurement and evaluation of the maturity level of IS, applicable to a wide area of organizations and user's evaluator, auditors of IS.

Implementation of the results: the M^3SI, PSITI, PISI models and the auxiliary application were implemented in the NBM for supervisory activities and assessment of information security of banks in Moldova.

АННОТАЦИЯ

Бричаг Валентин: «Анализ и повышение уровня зрелости системы управления информационной безопасностью для предприятий Республики Молдова (на примере коммерческих банков)».

Докторская диссертация по информатике, Кишинёв, 2024.

Структура диссертации: диссертация написана на румынском языке и состоит из введения, трех глав, общих выводов и рекомендаций, библиографии из 93 названий и 4-ёх приложений. Диссертация содержит 141 страниц основного текста, 54 рисунков и 10 таблиц. Полученные результаты опубликованы в 8-и научных работах с общим объёмом около 7 авторских листов.

Ключевые слова: информационная безопасность (ИБ), кибербезопасность (КБ), система управления информационной безопасностью (СУИБ), многопрофильная модель зрелости информационной безопасности (M^3SI), универсальная база данных M^3SI, типичный для отрасли профиль информационной безопасности (PSITI), Индивидуальный профиль информационной безопасности (PISI) для конкретной организации.

Цель: разработка многопрофильной модели зрелости ИБ с ИТ-поддержкой для оценки и повышения уровня зрелости.

Подцели: создание базы данных M^3SI, содержащее обобщённые знания о подходах к ИБ, о требованиях, угрозах, рисках и средствах контроля ИБ; разработка инструментального приложения для поддержки многопрофильной модели M^3SI, типовых отраслевых профилей PSITI и индивидуальных профилей PISI для конкретных объектов; разработка, утверждение и валидация типового профиля PSITI для банковской деятельности, установление целевых значений критериев и оценка согласно PISI.

Научная новизна и оригинальность: генерирующая модель M^3SI, типичный для отрасли профиль PSITI и индивидуальные профили PISI для конкретных объектов со специфическим контролями ИБ, критериями и показателями, программный инструмент, для поддержки модели M^3SI и процесса оценки – являются оригинальными и подходят для различных объектов и различных конкретных контекстов использования.

Полученный результат, способствующий решению важной научной задачи, является обобщённая база знаний по основным общепризнанным подходам и управлению ИБ и построение на их основе многоуровневых моделей, соответствующих типовым отраслевым и конкретным индивидуальным требованиям, для конкретных частных случаев.

Теоретическая значимость: определяется синтезом базы знаний, критериев оценки зрелости и их измерения в соответствии с типовыми и специфическими/частными требованиями.

Прикладная ценность: заключается в существенном вкладе моделей, профилей и вспомогательного приложения для измерения и оценки уровня зрелости ИБ, применимого к широкому кругу организаций и пользователей оценщиков и аудиторов ИБ.

Внедрение результатов: модели M^3SI, PSITI, PISI и вспомогательное приложение были внедрены в НБМ для надзорной деятельности и оценки ИБ банков Молдовы.

BRIACEAG Valentin

ANALYSIS AND ENHANCEMENT OF THE INFORMATION SECURITY MANAGEMENT SYSTEM MATURITY LEVEL FOR THE REPUBLIC OF MOLDOVA ENTITIES
(Case Study - Commercial Banks)

232.02 Technologies, products and information systems

Summary of the doctoral thesis in Informatics

Aprobat spre tipar: 02.05.2024
Hârtie ofset. Tipar ofset.
Coli de tipar: 2.0

Formatul hârtiei 60×84 1/16
Tiraj 25 ex.
Comanda nr. 60/24

Centrul Editorial-Poligrafic al USM
Str. Al. Mateevici, 60, Chișinău, MD-2009
Email: cep1usm@mail.ru, usmcep@mail.ru