TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 61, Issue Special, September, 2018

INTEGRATION OF THE GDPR REQUIREMENTS INTO THE REQUIREMENTS OF THE SR EN ISO/IEC 27001:2018 STANDARD, INTEGRATION SECURITY MANAGEMENT SYSTEM IN A SOFTWARE DEVELOPMENT COMPANY

Mirabela Luciana GAŞPAR, Sorin Gabriel POPESCU

Abstract: *Information security in general and personal data security in particular is one of the major challenges in today's business arena. It implies specific reactions both from the technological point of view and from the management point of view and specific international regulations and standards set the boundaries between which it operates. This paper presents a managerial approach on information security, which combines the GDPR (General Regulation regarding Personal Data Protection) requirements and those of the ISO 27001 standard, validated by a study case on a software development company. It suggests stages, the identification of the critical ones, it defines directions and actions related to information security and it describes the methodology for applying certain support techniques and instruments.*
Keywords: *GDPR, ISO 27001, ISO 27005, personal data, information, confidential information, information security management, data security, information security, risk, risk evaluation*

1. INTRODUCTION

In a society and economy based on knowledge, information and its flows is the main factor of economic growth. Information is important at all levels of organisation in a contemporary society, starting with unions between states as the European Union, getting to a national level, that of an organisation/company and ending at a personal level. Information is considered a resource, which, as all other important business resources, is vital in the organization's competitivity [6], and thus the need for it to be properly protected. No matter the form of the information or the channels it is being transmitted through, it needs a proper protection. The management of a company's information depends on the support technology used, usually, ICT. This makes technology the key element in creating, analysing, storing, transmitting, protecting and destroying a company's information. [4]

The interconnected global business environment has a critical impact on information security, by generating new multiple threats and vulnerabilities [6]. Information on its own, does not mean knowledge: it is just its raw material, from witch one can create a product, a meaning, an explanation, a strategy, etc. On the other hand it is widely known and quoted that "Scientia potentia est" information means power (Francis Bacon), and for companies it is an important competitivity factor, being desired by competitors and protected by the company that owns it. For a company, information is not just the one generated by it, but it may belong to customers, suppliers or other interested parties and has gotten under the company's ownership by running their own processes. The company is responsible for this information and as the situation of Cambridge Analitica illustrates, where personal data of over 80 million users has been given to third parties and then used for less honest purposes, there is a need for better

protection of third party's information that is being handled by the company.
Information protection and security is the main topic of ISO 27001:2013 (SR EN ISO/IEC 27001:2018) standard, now at his second edition. GDPR (General Data Protection Regulation) Regulations came into force in May 2018 in the EU and they impose a rigorous approach while dealing with the management and protection of the personal data being used by any organisation. This paper offers a methodology for risk identification, description and integration regarding information security from the point of view of GDPR and ISO 27001 standard requirements. The stages have been identified, their content defined and it has also been described the use of particular support techniques and instruments. The strategic directions regarding information security and the necessary specific actions have been defined in order to ensure success. The exemplification and validation of the methodology is performed on a study case in a software development company.

2. BACKGROUND

2.1 Information

Information is a communication process, a message containing new elements as compared to what its user previously knew, related to the characterization of a particular situation, phenomena, fact, economic process, etc. As such, information is a research instrument of the processes that take place in different systems, reflecting cause and effect relationships from the surrounding environment [3].
Information can be stored in different ways including: digital format (data files saved on optical or electronic storage), material format (ex. paper) and also information that cannot be represented, such as the employees' knowledge. Information can be transmitted in different ways including: courier service, electronic communication or verbally [6].
It is mandatory that all information be classified, no matter where it is used. Thus, in the EU, information is classified [2] as: strictly secret, secret, confidential and restricted. Governments start from a broader classification of information, such as: subjective information and objective information (as compared to classified and non-classified).
ISO 27001 [7] standard does not mention the way information is classified but allows all companies to implement their classification strategy. The classification systems have to consider the essential characteristics of information: confidentiality, integrity, availability. Most methods used have 4 security levels:

- Public or unrestricted information
- Internal or protected information
- Confidential information
- Secret or restricted information

This model can be improved according to the company's objective needs. It is worth mentioning that inside a classification model, placing information in a classification category is not final and that it can undergo changes according to the company's policies.
According to [8] information must be classified according to its value, legal requirements, importance, and critical level for the organisation. ISO 27002 standard recommends the following for information classification:

- Information classification must take into consideration the objective needs of protecting the information which is a result of the company's area of activity and the impact, the disclosure, unauthorized use or even destruction of any type of information might have on the company.
- The level of protection of information should be analysed in the context of the CIA (Confidentiality, Integrity, Availability) profile.
- The rules for using and controlling the information should be based on information classification
- The company's management should periodically review the information classification according to the already decided access policies.
- The responsibility for placing the information in a particular category and for its review belongs to the owner of the information.
- When information is shared with third parties, it should be decided on measures that can

eliminate any misunderstandings related to its use.

- The owners of the information should supervise the use of the information from every classification category and should take into consideration the following types of processing: creation/ modification, copy, storage, transmission by mail, fax, electronic mail, verbally, including by phone, voicemail, answering machine, declassification, destruction.

2.2 Information security

Information security consists of three major aspects: confidentiality, availability and integrity [6]. In order to unsure the business's success and continuity and to minimize impact, information security implies the use and management of proper security measures which means taking into consideration a large variety of threats.
According to [7], information security is performed by implementing a series of control measures selected based on the risk management process and managed by using an ISMS which includes policies, processes, procedures, organisational structures, software and hardware, in order to protect the identified informational resources [6]
A survey of ISO [5] mentions, for 2016 only, over 27 thousand companies that certified their Information Security Management System (ISMS) according to ISO 27001, 21% more than in the previous year.

2.3 Risks and approaches regarding information security

Today's society is permanently faced with a wide variety of risks: natural risks, professional risks, health risks, information security risks, risks that affect the environment and have negative effects on future generations etc., whose action is permanent.
One of risk's numerous definitions shows it as being a threat, a possibility of occurrence of a damage causing event, characterised on one hand by the severity of its consequences and on the other hand by its occurrence probability.

SR EN ISO/CEI 27001:2018 standard explicitly requires that the company, that wants the implementation and certification of an information security management system, defines and applies an information security risk evaluation process by:

- Establishing and maintaining information security risk criteria, meaning risk acceptance criteria and risk evaluation criteria
- Making sure that continuous and repeated risk evaluation generates consistent, valid and comparable results
- Identifying risks, that is risks associated with information confidentiality, integrity and availability loss and by identifying risk owners
- Risk analysis, that is potential consequences if the identified risk was to occur, the real possibility of occurrence of the identified risk and the identification of the level of risk
- Estimating risks

2.4 Norms and standards regarding information security management

2.4.1 GDPR

The GDPR norms, debated a lot lately, require all companies (commercial enterprises, administrative institutions, etc.) which use personal information be obligated to comply to strict rules regarding the way they collect, use, process and store this type of information, whether it is digital data or physical documents [13].
GDPR was created to offer citizens a better control over their personal data and establishes an implicit confidentiality [10]. The objective of this regulation is to offer safety, a safe way of data sharing between data controllers and to protect consumers from being stuck with one special supplier [11].
In Romania, the GDPR norms are basically an update to an already existing legislation, 677/2001 law. This law regulates aspects regarding personal data processing since 2001, so the current European norms just extend, complete and apply it more vigorously.
Personal data

The awareness of the impact of this wave of new regulations is raised by taking into consideration that the expression "personal data" refers both to the company's customers (individuals) and to its employees [1].
This expression refers to any type of information related to an individual (no matter that it identifies itself or not): name, PIN, telephone number, email address, home address, possessions, copy of the ID card, CV, facial photo, work contract, etc. [11]. This means that all processes within an organization that uses this type of data can be affected by the measures that GDPR obligate companies to implement in order to protect it.
There are very few companies that are not affected by the GDPR. Most companies should make a substantial effort to secure the data of their own employees and also of their customers. A non-governmental organization that does not collect any data from individuals will never targeted by NAPDSP (National Authority for Personal Data Processing Surveillance), authority that applies both law Nr. 677 and the GDPR directions. Commercial enterprises with natural persons as customers (banks, insurance companies, consumer goods producers, telephone operators, etc.) or public institutions (administrative, hospitals, financial, educational, etc.) are obligated to go through all the internal changes required by the new personal data security legislation.
Consent
The most significant aspect of this personal data protection process is the fact that the company needs to explicitly or implicitly obtain the consent of every person involved by collecting and processing personal data [11]. This means that all means of collecting personal data must explicitly contain the request of consent from the person involved.
Personal data security
Taking into consideration the risk from the company's area of expertise with different degrees of probability and severity for the rights and freedom of individuals, the company (operator) and the person empowered by it have to implement adequate technical and organizational measures in order to ensure a level of security specific to risk, including, according to the situation [13]:

- Pseudonymization and encryption of personal data
- The ability to ensure the confidentiality, integrity, availability and continuous resistance of the processing systems and services
- The ability of restoring the availability of personal data and access to it on time in case of a physical or technical incident
- A process for periodical testing, evaluation and appreciation of the efficiency of the technical and organizational measures in order to ensure the data processing security

When evaluating the adequate level of security, one must take into consideration the risks generated by the processing system, especially generated, accidentally or illegally, by the destruction, loss, change, unauthorised disclosure or unauthorised access to personal data, transmitted, stored and processed differently [11].
The surveillance authority must be notified in case of a breach in personal data security.

Evaluation of impact on data protection
The company (operator) performs, before the processing stage, an evaluation of the impact of the processing operations on personal data protection and asks for the approval of the data protection responsible [11], if assigned one. A single evaluation may approach a set of similar processing operations which show similar high risks.
The evaluation of impact on data protection [13] is mandatory especially in the following situations:

- The systematic and extensive evaluation of personal aspects related to natural individuals, which is based on automatic processing and which is the basis for decisions that lead to legal effects regarding the individual or that significantly affect it in a similar way
- The processing at a large scale of specific data categories or personal data regarding legal sentences and crimes
- Of a systematic monitoring at a large scale of a public accessible area

2.4.2 SR EN ISO/IEC 27001:2018 standard

SR EN ISO/IEC 27001:2018 "Information Technology. Security Techniques. Information Security Management Systems. Requirements", contains the requirements for the establishment, implementation, maintenance and continuous improvement of an information security system in the context of the company [1].
The implementation of the SR EN ISO/IEC 27001:2018 standard helps the company to be able to answer the GDPR requirements, being a framework for information protection.
According to GDPR, personal data is critical confidential information that all companies must protect.

3. RESEARCH METHODOLOGY

For creating the methodology a few stages are being considered:

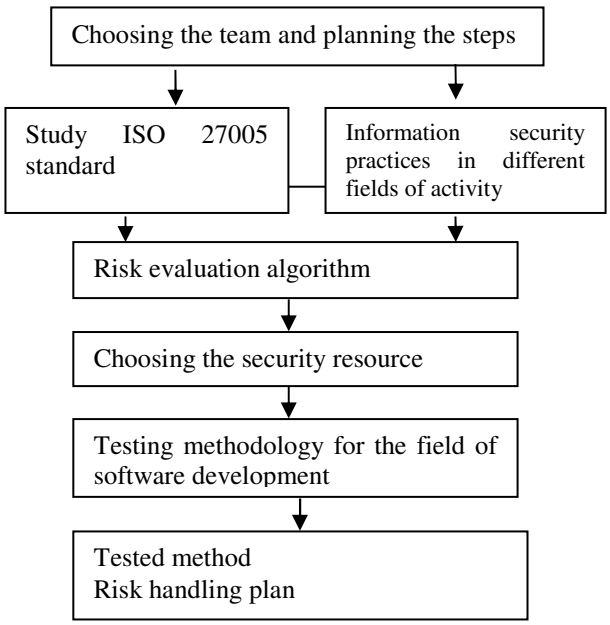


Fig. 1: Risk evaluation methodology

In the first step of the methodology, figure 1:
- The team is chosen from the employees responsible for the management system
- The development of the process is planned (desired outcome, time, resources, methods)
- Primary information collecting and processing

The second step consists of the analysis of the SR ISO/ IEC 27005:2016 standard "Information technology. Security Techniques. Information security risk management" and the practice in information security of the analysis team.

The algorithm for performing the process, according to which the methodology in a software development company is tested for confidential information resource (personal data), is chosen.

4. RESEARCH

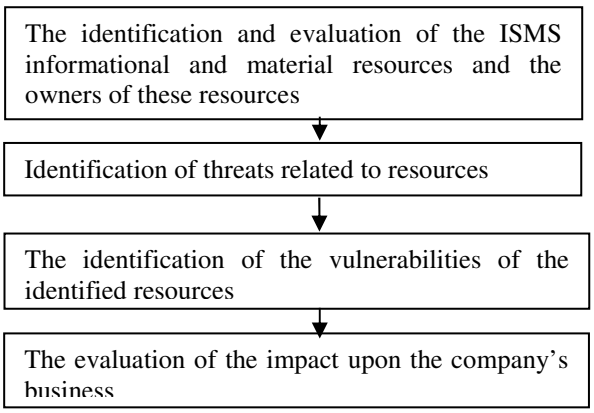
4.1 Study regarding information security resources identification

The information security management system keeps information confidentiality, integrity and availability [7] by applying a management process, it offers trust to the interested parties and it proves that risks are properly handled. Chapter 6.1 of SR EN ISO/IEC 27001:2018 standard contains the requirements related to information security risks evaluation and treating. A reference standard for information security risk evaluation and treating is SR ISO/ IEC 27005:2016 "Information technology. Security Techniques. Information security risk management".
Thus, resource identification in a software development company is done for two types of resources:
- Primary resources: business processes and activities, information
- Support resources: hardware, software, network, personal, location, company structure.

Personal data can be included in the information type of primary resources category.

4.2 Risk handling plan and methodology

The risk management methodology used in a software development company is based on the regulations of the international SR ISO/IEC 27005:2016 standard and it consists of the following stages:



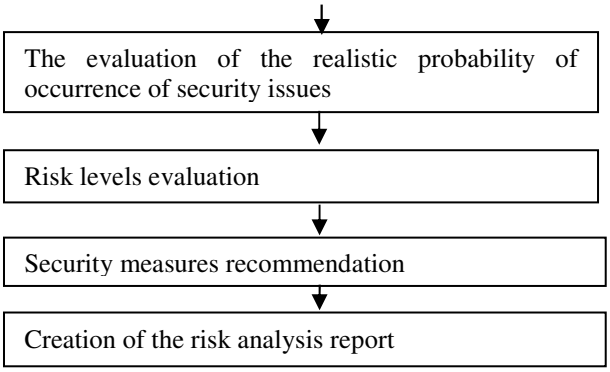


Fig.2: Stages of risk evaluation process

4.2.1 Stage 1 Resources' identification

In this stage we identify: the ISMS' operational boundaries together with the system's material resources, the services offered by it and the information handled, which can be subject to risk. The values of the informational and material resources, which can be revealed, changed, made unavailable or destroyed, are determined. In order to identify the informational resources belonging to ISMS that can be subject to risk, one needs a deep understanding of the system's processing environment, an identification of the applicability field and its operational limitations. For this, the risk analysis team has to get information about the ISMS that should include:

- ISMS purpose and mission;
- ISMS' architecture (hardware, software, system's interfaces, network's diagrams)
- The importance of the ISMS and that of the processed information
- Informational flow
- Information classification level
- Security policies that apply to ISMS
- ISMS' functional requirements
- ISMS' users

Any other relevant information about ISMS

4.2.2 Stage 2 Threat identification

Threat can be defined as the possibility of accidentally or deliberately compromising of an ISMS, through loss of information's confidentiality, integrity or availability in an electronic format or by affecting the functions which ensure information authenticity and annulment [16].

The purpose of this stage is to identify the potential threat sources towards the analysed ISMS and to create a list with possible threats that could affect the company.

Related to the type of source, the threat categories [16] being analysed are:

- Natural threats (force majeure)- caused by natural phenomena such as floods, earthquakes, storms, landslides, avalanches, thunders etc
- Human threats – favoured or caused by people, through unintentional actions
- Technical/technological threats – caused by the improper functioning of the ISMS' informatics systems, of the auxiliary installations etc.
- Organizational threats – favoured by organizational shortages or shortcomings
- Deliberate acts- favoured or caused by people or their deliberate actions

4.2.3 Stage 3 Vulnerabilities identification

Vulnerability is a breach or a weakness in ISMS' security design and implementation or in the security measures, and it could be exploited accidentally or intentionally by a threat to the system, identified according to the results of stage 2 [16]. The purpose of this stage is to identify the vulnerabilities inside the ISMS and to create a list of these vulnerabilities.

Vulnerabilities identification and the method used for it depend on the ISMS's operational environment, and also on the stage that the system is at:

- If the system is in the planning stage, the identification of vulnerabilities is based on the analysis of the security policies of the company, on the analysis of the security requirements and of the security operational procedures suggested for the ISMS and on the analysis of the security characteristics of the equipment that can be used in the system.
- If the system is in the implementation stage, the identification of the vulnerabilities is based on the analysis of the security requirements and on the approved security operational procedures and also on the results of security testing and evaluation.
- If the system is in the operational exploitation stage, the identification of vulnerabilities is

based on the analysis of the way the system's equipment and software is used and also on the analysis of the efficiency of the technical and non-technical security measures, used for ISMS' protection.

4.2.4 Stage 4 Impact analysis when an undesired event occurs

Before starting the impact analysis it is necessary to get the following information:

- Processes run in the ISMS;
- The system and data importance and criticability;
- The level of classification of information.

The impact of an undesired event represents the loss or degradation of one or a combination of the three security objectives, ISMS' confidentiality, integrity and availability [16].
The analysis of the impact that the occurrence of an undesired event has on the ISMS' purpose, determines its classification according to the effect on the company's goods and resources. .
The impact's ranking is based on a qualitative and quantitative evaluation of the sensitivity or importance of the informational resources.
Certain impacts can be evaluated from the quantitative point of view through:

- Financial loss;
- The cost for repairing the system;
- The level of necessary effort to repair the effects of a successful attack etc.

Other impacts such as loss of credibility and the damage of the company's interests cannot be appreciated in specific units but they can be evaluated from the qualitative point of view (very big, big, medium, small, very small).

4.2.5 Stage 5 Determination of the probability of occurrence of an undesired event

During this stage, the team that performs risk analysis has to determine the probability of occurrence of an undesired event, more exactly, the probability of a vulnerability of the ISMS to be exploited [16].
The following basic factors have to be taken into consideration:

- The motivation of the threat source and its ability, more exactly, access means, abilities and opportunities;
- The nature of the vulnerabilities;
- The existence and efficiency of the implemented security measures.

In order to determine the probability of the occurrence of an undesired event, the threats addressed to the ISMS have to be analysed strictly related to the possible vulnerabilities and to the security measures already implemented in the ISMS.

4.2.6 Stage 6 Qualitative determination of risks and of the associated levels

The purpose of this stage is risk determination and the levels associated to it, for the ISMS' resources.
The risk of occurrence of an undesired event is defined as being the probability that a threat addressed to the ISMS to be able to exploit one of the system's vulnerabilities, leading to its compromise or to that of its resources.
The level of risk is a function given by the occurrence probability of an undesired event and by its impact upon the ISMS.

$$R = P \times I$$

The identification of the level of risk for every undesired event that may have an impact on ISMS or on information, is done according to the risk level matrix presented in Table 1.
Risk level is situated at the intersection of the column representing the probability of occurrence on an undesired event with the line indicating the impact of the occurrence of that event.

Table 1.

Risk level matrix

		Probability				
		Very low	Low	Medium	High	Very high
Impact	Very high	5	10	15	20	25
	High	4	8	12	16	20
	Medium	3	6	9	12	15
	Low	2	4	6	8	10
	Very low	1	2	3	4	5

These risk levels are:
- Very low risk (grades 1-2);
- Low risk (grades 3-6);
- Medium Risk (grades 8-10);

- High risk (grades 12-16);
- Very high risk (grades 16-25)

As it can be seen from the risk level matrix, security risk may have different values, from very small risk to very big risk. In case of a very small or small risk, the company's management has to decide if any extra security measures are necessary or if this level of risk is acceptable

For a medium risk, extra security measures are necessary and a plan that would allow the implementation of these measures in a reasonable amount of time has to be created.

If risk is big, there is a need for extra security measures that have to be implemented as soon as possible, and the system may or may not be functional until these security measures are being implemented.

For a very high risk, in most of the cases, it is decided to forbid the use of the ISMS until extra security measures are being implemented, that would lead to a smaller risk.

In the study case company, the acceptable risk level is of Small and Very small. The medium risk level means a financial loss of over 15 000 €. A financial loss greater than this amount is considered unacceptable.

4.2.7 Stage 7 Security measures recommendations

The purpose of this stage is to recommend security measures that can reduce at an acceptable value the identified risks [16]. Factors that influence the choice of the specific security measures in SR ISO/CEI 27002:2018

- The efficiency of the recommended security measures
- Legislation and the ongoing regulations
- Information security policy
- The operational impact on the system's performances;
- The system's protection and reliability.
- If the threat changes affecting the information security characteristics, the information in written down in table 3. Besides the loss of information confidentiality threat, there might appear other threats such as: the loss of information integrity and availability. The last step in risk evaluation is creating the information security risk evaluation report and the risk handling plan.
- Reducing the informational risk
- Reducing risk means ranking, evaluation and implementation of security measures, recommended during the risk analysis stage [16], which took place at a previous time, in order to reduce the identified risks.
- The 7 stages in figure 3 are followed:

4.2.8 Stage 8 Risk analysis report

After the risk analysis has been ended, meaning that the threat and vulnerability sources have been identified, the risks and the levels associated with them have been identified and there were given recommendations regarding the choice and implementation of the security measures, the results have to be written down in an official document called Risk Analysis Report, according to SR ISO/CEI 27001:2018 requirements.

Risk analysis report helps the upper management to take fundamental decisions regarding the change of security policy for the ISMS, the change of the security operational procedures and also to ensure the necessary budget for the implementation of these changes.

The risk analysis report has to be presented in an analytical and systematic manner of risk evaluation, so that management can understand the risks related to ISMS and to create a budget for the necessary financial resources in order to reduce and correct the potential losses.

4.3 Method validation in a study case in a software development company

The resource for which risk analysis was performed is information, classified as confidential and which contains employees' personal data. This data, according to GDPR has to be processed and protected through its own methods by the software development company.

Table 2 contains the risk analysis for the loss of information confidentiality threat and for three vulnerability options identified during a brainstorming session of the company's security group. The members of this group are: Physical Security Manager, IT Manager, Quality Manager, Delivery Directors, HR Manager.

Table 2:

Risk evaluation for confidential information resource- personal data

	1	2	3	4
Threat	Loss of confidentiality	Loss of confidentiality	Loss of confidentiality	Loss of confidentiality
Vulnerability	Theft	Insufficient infrastructure	Non-conform handling	Improper setting of access rights
Previously implemented measures	M1 Confidentiality clause M2 Inserting contractual confidentiality clauses in all contracts M3 The definition of the specific clauses in the job descriptions M4 Internal procedure Nonconformities control	M1 Restricted access to work areas with confidential information M2 identification and creation of a documents archive area M3 acquiring office furniture with locks in order to restrict access to documents	M1 Defining the procedure Safeguarding the information security M2 Making the employees responsible through the confidentiality agreement M3 Training employees regarding the correct handling and classification of information	M1 Setting the access rights M2 constant review of access rights
Impact Probability	Very high medium	medium low	Very high medium	High Low
Level of risk Affected characteristics: confidentiality: integrity: Availability:	High risk 80% 0% 20%	Low risk 80% 0% 20%	High risk 60% 0% 40%	Medium risk 90% 0% 10%
Suggested measures	Documentation and implementation of the GDPR requirements inside the company	Minimized risk because of the implemented measures. Safeguarding the implemented measures	Cryptographic keys throughout information communication Risk evaluation related to information migration to cloud	Risk dropped after implementing M2 Safeguarding M2

Table 3:

Risk evaluation for confidential information resource - personal data

	1	2	3	4
Threat	Loss of information integrity	Loss of information integrity	Loss of information availability	Loss of information availability
Vulnerability	Introducing wrong data	sabotage	Documents destruction	The degradation of the data base where documents and emails are stored on computers
Previously implemented measures	M1 Employ qualified personnel M2 Train personnel, defining the	M1 Level of access to information by using different applications	M1 Organizing activities according to legal regulations M2 documents stored in fire resistant safe or in places with a minimum fire risk	M1 computers' Backup M2Data base Backup using NAS for emails M3 Move NAS to a different location from that of the email server.

	training plan		M3 scanning confidential documents	
Impact Probability	Low Low	Low Low	Low Low	High Very low
Level of risk Affected characteristics: confidentiality: integrity: Availability:	Low risk 10% 70% 30%	Low risk 10% 70% 30%	Low risk 20% 20% 60%	Low risk 0% 20% 80%
Suggested measures	No measures necessary Keep the already implemented measures	No measures necessary Keep the already implemented measures	No measures necessary Keep the already implemented measures	No measures necessary Keep the already implemented measures

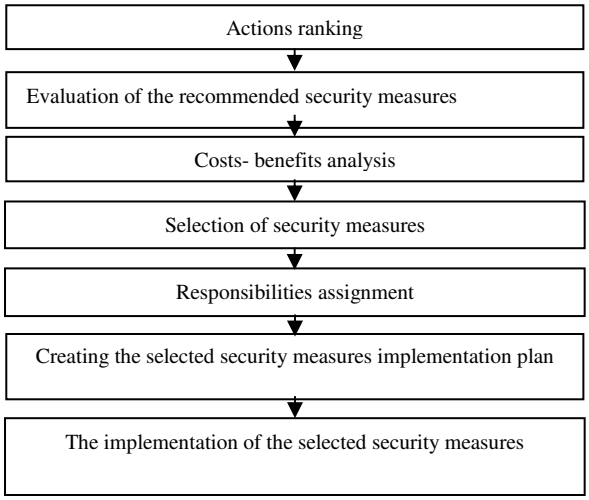


Fig.3 Risk reduction stages

If the threat changes affecting the information security characteristics, the information in written down in table 3. Besides the loss of information confidentiality threat, there might appear other threats such as: the loss of information integrity and availability. The last step in risk evaluation is creating the information security risk evaluation report and the risk handling plan.

Reducing risk means ranking, evaluation and implementation of security measures, recommended during the risk analysis stage [16], which took place at a previous time, in order to reduce the identified risks.

The 7 stages in figure 3 are followed were necessary.

According to every particular situation, the implementation of security measures may reduce the level of risk but it may not entirely eliminate it. The remaining risk is defined as residual risk [9].

The implementation of the selected security measures or the improvement of the already existing ones may reduce risk by:

- Eliminating some of the system's vulnerabilities (breaches or weaknesses), reducing this way the number of possible pairs, the source of threat/vulnerability;
- Adding a new specific measure to reduce the capacity or motivation of the threat source.
- Reducing the impact of producing an undesired event. The risk remained after the implementation of the new methods or after the improvement of the already existing ones is residual. Practically, no ISMS is lacking risks and not all the implemented security strategies can eliminate the risks they are addressed to or reduce the level of risk to zero.

If the residual risk was not reduced to an acceptable level, the cycle of risk management has to be repeated in order to identify a new possible way to reduce the residual risk to an acceptable level.

The residual risk has to be accepted by the upper- management [16] by signing the Risk Handling Plan.

Table 4 describes the risk handling plan for confidential information resource- personal data.

Table 4:

The risk handling plan for: confidential information resource- personal data

Influenced resource	Confidential information	Confidential information	Confidential information
Measure	Documents and the implementation of the GDPR requirements in the company	Cryptographic keys throughout information communication	The consistent review or access rights
Risk responsible	ISMS responsible	ISMS responsible	ISMS responsible
Measure implementation responsible	Security group	IT Manager	IT Manager
Ticket number	INSEC-49	INSEC-95	INSEC-98
The control reference from ISO 27001/ Appendix A	A 10.1.2	A 10.1.2	A 9.2.5

The measures mentioned in table 4 need to be implemented by the assigned responsible in no less than 3 months from the analysis, so that there is no suspicion regarding the affected resource. The tickets that are not solved in the previously mentioned time interval, reach the

5. CONCLUSIONS

The integration of the GDPR requirements into the requirements of the ISO 27001 standard is a contemporary subject and leads companies who implement is, to performance. It is true that not all companies can afford to implement an ISMS because of lack of resources (financial, personal, business), but if they want a protection of information regarding personal data, they need to implement a particular beneficial strategy and which can help them reach their goal.

In order to obtain an efficient and adequate result there is need for a structural and algorithmic approach that requires specific competencies in the company's field of activity. The techniques, instruments and methods characteristic to ISMS that were suggested in this paper were intended to structure, filter, selection, information ranking, facilitating the work of the team who undertook these steps. The results need to bring added value for the company through lines of action, specific actions, objectives and measures.

The purpose of this study was to present the integration of a resource chosen by the authors as being the most frequently encountered in modern companies, whether they have implemented or not the ISO 27001 standard. The authors want to meet the companies interested in this process so as to get to performance by respecting the GDPR requirements and even implement the information security standard.

The final purpose of this paper is the creation of a plan to handle risk related to information protection - personal data, through the methodology described, measures related to the increase of performance of the management system. Having this in mind, this study tried to identify the main resources used by the software development company in its efforts to respect the requirements of the European norms who entered into force in Romania on the 25th of May 2018, to overcome their competition through security measures implemented as a result of evaluation and to reach the position as top leader on the software market.

6. REFERENCES

[1] ASRO. (2018, February 19). Retrieved from GDPR și SR EN ISO/IEC 27001:2018: www.asro.ro

[2] Council, E. (2017, september 11). Protection of European Union classified information (EUCI). Retrieved from European Council: http://www.consilium.europa.eu

[3] Dinte, Constantin. (2016). Informatia si rolul acesteia in management.

[4] ENISA. (2017, November). Retrieved from Cyber Security Culture in organisations: https://www.enisa.europa.eu

[5] ISO. (2017, september). ISO Survey. Retrieved from International Organization for Standardization: www.iso.org

[6] ISO27000. (2018). Information technology. Security techniques. Information security management systems. Overview and vocabulary.

[7] ISO27001. (2013). Information technology. Security techniques. Information security management systems. Requirements. iso.org.

[8] ISO27002. (2013). Information technology. Security techniques. Code of practice for information security controls. iso.org.

[9] ISO27005. (2016). Information technology. Security techniques. Information security risk management. iso.org.

[10] OECD. (2018). Retrieved from The-digital-economy-multinational-enterprises-and-international-investment-policy.pdf: http://www.oecd.org

[11] ParlamentulEuropean, ș. C. (2016). Regulamentul (UE)2016/679 al Parlamentului European și Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Dir 95/46. Jurnalul Oficial al Uniunii Europene.

[12] Reguli de buna practica privind securitatea informatiei. (2016, martie 25). Retrieved from InterManagement Consulting: http://www.intermanagement.eu

[13] Rentrop&Straton. (2018). Protecția datelor cu caracter personal. Bucuresti: Rentrop&Straton.

[14] SRENISO27001. (2018). Tehnologia informatiei. Tehnici de securitate.Sisteme de management al securității informației. Cerinte.

[15] ASRO.

[16] SV. (2015). Metodologia de evaluare a riscurilor.

Integrarea cerințelor GDPR în cerințele standardului SR EN ISO / IEC 27001:2018, Integrarea Sistemului de Management a Securității Informaţiei într-o companie de dezvoltare software

Rezumat: Securitatea informației în general și a datelor cu caracter personal în particular constituie una dintre provocările majore ale vremurilor actuale. Ea presupune reacții specifice atât pe dimensiune tehnologică cât și pe cea managerială, în privința căreia operează standarde şi reglementări internaționale specifice.

Lucrarea prezintă o abordare managerială privind asigurarea securităţii informaţiei, care combină cerințele GDPR (Regulamentul General privind Protecția Datelor Personale) și ale standardului ISO 27001, validarea fiind realizată pe un studiu de caz într-o companie din domeniul dezvoltării de software. Sunt propuse etape, identificate cele critice, definite direcții și acțiuni pe domeniul securităţii informației și descrisă aplicarea unor tehnici și instrumente suport.

Mirabela Luciana GAŞPAR, Department of Design Engineering and Robotics, Technical University of Cluj-Napoca, 103-105 Muncii Blvd., 400641 Cluj-Napoca, Romania, mirabela.gaspar@yahoo.com

Sorin Gabriel POPESCU, Department of Design Engineering and Robotics, Technical University of Cluj-Napoca, 103-105 Muncii Blvd., 400641 Cluj-Napoca, sorin.popescu@muri.utcluj.ro