Information risk management in SME sector enterprises

Paweł Kobis
Czestochowa University of Technology, Faculty of Management, Częstochowa, Poland
pawel.kobis@wz.pcz.pl
ORCID: 0000-0003-0714-1888

Abstract: *The article attempts to determine the level of use of methods increasing the security of information resources among the SME sector enterprises declaring the use of information security risk management methods. Research was carried out to determine the scope of use of risk management methods in the aspect of actions taken in the area of security of the intangible assets. Also the so-called "human factor" in the information protection process was taken into account. An attempt was made to determine how business entities use risk assessment in any form and how many of them use (and to what extent) the recommendations described in the ISO/IEC 27005 standard.*
Keywords: *INFORMATION, SECURITY MANAGEMENT, RISK, SME ENTERPRISES*

1. Introduction

The majority of enterprises operating on the market process information in digital form. Data stored in paper form currently are a negligible part of all processed information and constitute rather an "analog copy" of a digital record. In addition, information is the company's most valuable resource. Processing information in a digital form involves the risk of its loss, destruction or takeover by third parties. This is primarily due to the fact that virtually every information system of a business entity operates in a local network with a direct connection to the Internet. Thus, potentially unsecured data and information resources can be accessed from virtually anywhere in the world. Therefore, it becomes necessary to develop appropriate principles of information management, implementation of specific safeguards, and identification, analysis and assessment of information risk. The risk management process is particularly important. Identifying the weaknesses of both the company's IT system and ways of securing digital content is a starting point in determining potential threats and the occurrence of unwanted incidents.

2. Theoretical outline of risk management in the area of information security

Risk management is the main area in the information security management system in business entities. This process can be divided into six main stages forming a closed loop [1,2]:

- Context Establishment;
- Risk assessment consisting of:
  - Risk identification;
  - Risk analysis;
  - Risk evaluation
- Risk treatment;
- Risk acceptance;
- Risk communication and consultation;
- Risk monitoring and review.

Closed loop proves that this process is being repeated successively in entities, and security management is continuous. Any, even the slightest change in the information system should generate the need to re-perform the risk management procedure. A detailed theoretical description of the individual stages of risk management together with the methods currently used in organizations for estimating the appropriate quantities could successfully constitute material for a separate book publication. In this article, in the theoretical part, only definitions of elements of this process are provided. The stages of risk management are graphically presented in Figure 1. This is a model contained in the international standard ISO/IEC 27005 [3].

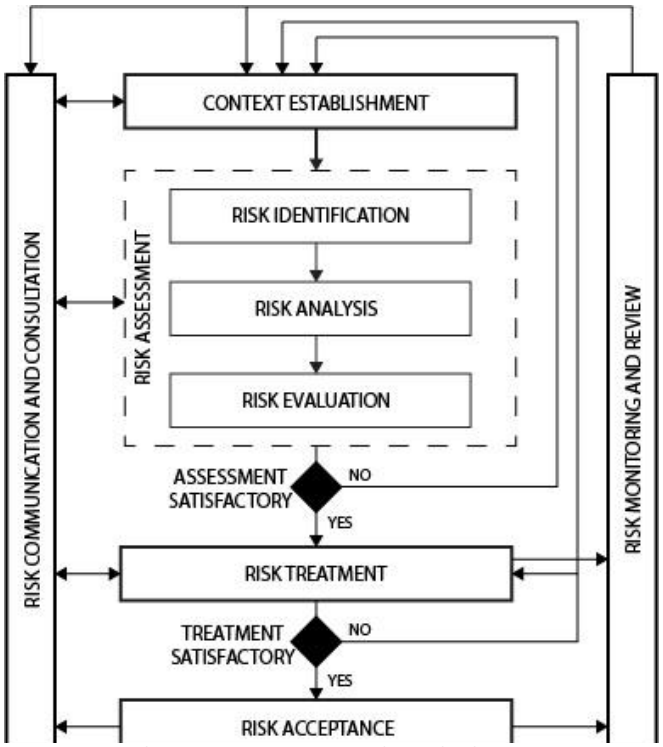

Fig. 1 *Stages of risk management in the field of information security in business entities.*
Source: [4]

These stages are a logical sequence of actions aimed at minimizing or, in exceptional cases, eliminating potential risks affecting the security of digital resources [5]. They "recognize" potential information threats, allow you to accurately determine the structure of your own information system - identify its strengths and weaknesses. They allow the company to be identified as part of a wider, regional, national and perhaps even global information exchange system. The individual stages of risk management can be briefly characterized as follows:

1. Context Establishment - involves analysing the business and organizational environment of the enterprise. It consists in a detailed separation of external and internal factors affecting information processing in the enterprise [6]. In the case of external factors, the most common ones include: competition of the business entity, relations with clients and business partners, political and cultural environment, technological environment in the aspect of the possibility of using the existing potential [7]. The legal environment and related rights and obligations of the organization associated with the processing of information resources are also important. In the case of internal factors, we are talking about: organization of information processing within the enterprise, organizational structure, strategy and goals of the economic entity, the potential of the organization (technical, resource, knowledge, etc. potential).

2. Risk assessment - a key element of the information security management system. The first stage is to determine the causes and ways of materializing unwanted incidents. As part of risk identification, it is necessary to list all database resources, all security measures used and usable and to list all possible threats and vulnerabilities [8]. An inventory of assets should be made, in particular: software, hardware, technologies used, locations and people. It is very important to identify individual thematic areas in the field of information processing, specification of groups, teams, people who have access to information areas in a specific way and scope. It is important here to take into account the human factor, i.e. the human impact on information security - identification of strengths and weaknesses in the aspect of information security. Thus, it is necessary to determine the level of knowledge and experience of individual employees. This is a difficult task, but necessary in the times of continuously emerging social engineering techniques. In terms of the human factor, it is also necessary to specify the level of possibilities for conducting possible trainings for employees of the business entity - training facilities. Many techniques [9] are used to identify risk. The most important of them include [10]:

- review of the documentation;
- information gathering techniques, which include: brainstorming, Delphi technique, surveys and root cause analysis (RCA);
- checklists based on an analysis of similar projects from the past;
- analysis of project assumptions;
- techniques based on diagrams: cause and effect diagram, impact diagrams, block diagrams;
- SWOT analysis;
- expert assessment.

The second stage of risk assessment is its analysis. It allows with a certain approximation or probability to estimate the occurrence of a threat and its impact on information security.

Many methods of risk analysis are used in management theory and practice (CRAMM, COBRA, MARION, FMEA, OCTAVE, MEHARI, ISACA and others) [11, 12]. Many business entities develop their own proprietary methods. Generally, they can be divided into 3 groups [13]:

- Quantitative methods - in which attempts are made to quantify the probability of their occurrence and potential losses;
- Qualitative methods - based on the assessment of threats, their significance and possible losses associated with them, based on good practices and experience of a person or group of assessors;
- Mixed methods - using elements of the above two methods.

The third stage is risk assessment. It allows us to answer the question: is the risk acceptable? Whether any consequences of its occurrence constitute, or not, serious problems for the enterprise. At this stage, the risks are prioritized and in case of their occurrence the priorities for action are defined. The so-called residual risks are also specified, i.e. risks that remain after all possible or economically reasonable steps have been undertaken to avoid those risks. Risk assessment is an introduction to the stage of risk management.

3. Risk management means a specific set of actions to be undertaken in relation to the estimated risks [14]. It aims to provide certain options that will reduce or eliminate the risks if they occur. Risk management should take into account the effects of the risk (be proportionate to them) and should be cost-effective. The most common risk procedures include:

- Risk avoidance - implemented through resigning from certain actions that cause risks, replacing some actions with other, less risky ones, etc.
- Risk transfer - consisting in transferring responsibility for the effects of risk to another entity. This includes, for example, insurance, guarantees, employment of subcontractors (separate business entities) for selected risk-taking activities.
- Risk mitigation - a set of methods that reduce the likelihood of risk occurrence to an acceptable level.
- Risk acceptance - means the fact of knowingly accepting the risk and not taking any action to reduce it. It occurs most often in case of the absence of appropriate countermeasures despite access to all possible information related to the subject. It should be noted that accepting risk without first thoroughly investigating the phenomenon with as much information as possible can be considered as ignoring risk. We distinguish active and passive acceptance of risk. Active acceptance assumes creating a contingency plan in the event of a risk. In the case of passive acceptance, there is no contingency plan and no actions are taken [10].

4. Risk acceptance is the stage at which decision makers accept the risks developed in previous points of risks, their possible effects and established actions. Dealing with risk seems to be satisfactory [15].
5. The risk communication and consultation stage is a kind of stage covering all 4 previous stages. It runs in parallel and allows communication between decision-makers and other interested parties within the scope of the exchange of information on the risk and reaching agreement on the risk management [16].
6. The risk monitoring and review stage is a continuous process of tracking the risks and effectiveness of the security measures implemented by the organization [17]. It involves assessing the procedures developed as part of risk management and estimating their timeliness. It enables the analysis of the state of the information system - its possible changes, needs for updating and, as a consequence, conducting a new risk management procedure, taking into account all its stages.

The risk management scheme according to ISO 27005 is quite flexible and allows decision-makers of business entities to repeat any given stage of the process. At the same time, it is consistent in their implementation, not giving the opportunity to bypass any of them [18]. Thus, the authors of the scheme indicate that risk management is not a "rigid" process. Its course largely depends on the business entity, its needs and experience in the field of risk management. The authors of the scheme and other provisions of the standard also do not divide business organizations depending on risk management. Thus, specific guidelines are equally valid for small, medium and large enterprises. Certain 'framework' of proceedings is identical, however: the scope of analysed issues and the way of functioning of information systems in enterprises are changing.

3. Research results and discussion

Research using the CAWI (Computer-Assisted Web Interview) method was conducted in the period from January 2019 to June 2019 in 117 enterprises of the SME sector in the Silesian Voivodeship in Poland. The selection of enterprises for research was made using the purposive sampling method, taking into account the following condition: the business entities carried out to any extent the risk analysis of information security. People directly involved in business organizations in information security processes were asked to complete the survey. The survey was placed on the website of the author of this article. Requests for completing the survey were sent by e-mail to companies' email addresses and were communicated directly by phone.

The first question (Table 1) concerned the definition of resources and areas taken into account when assessing risk in business entities. The question includes traditional areas of information processing as well as those related to the human factor. All respondents declared here the area of hardware resources - thus

recognizing them as the most important in the information management system. Most of the respondents (98%, 99%, 98% and 99% respectively) also included: software resources, database resources, used security measures, and potential threats. Slightly less, because 87% also include technologies used in risk assessment. The above areas constitute a classic canon in the probed business entities in determining potential risk. Only slightly more than half of enterprises identify vulnerabilities in their information systems. This is quite surprising, since the vulnerability area should be one of the starting points when assessing risk. It follows that the potential effects of a threat are determined without establishing a precise genesis of the possibility of their occurrence. This is a methodological error showing the fundamental lack of knowledge among those responsible for the protection of intangible resources.

Table 1 *Answers of the respondents to the question: Please indicate which areas of risk identification do you include in the process of risk estimation*

1	hardware resources	100%
2	software resources	98%
3	database resources;	99%
4	locations of information resources	26%
5	used security measures	98%
6	technologies used	87%
7	potential threats	99%
8	identified vulnerabilities	54%
9	level of training	14%
10	employee susceptibility to social engineering methods	29%
11	employee knowledge	38%
12	employee experience	18%

Source: own study

Most business entities surveyed do not take human factors into account when estimating risk [19]. The highest result obtained in this group of areas is employee knowledge of 38% and social engineering methods with a result of 29%. Employee knowledge significantly affects information security. Knowledge of new techniques and technologies of protection as well as used attack techniques allows for an appropriate response from the employee. In addition, having knowledge about information security, the employee properly organizes the workplace (also in the virtual space) so as to minimize the risk of any incident. Therefore, it is surprising that only 38% of respondents pay attention to this. The training aspect is completely negligible (only 14% of responses). The pace of development of information management methods in digital form and the pace of development of more and more new techniques of digital aggression force continuous expansion of knowledge in this area. This applies not only to people who are formally responsible for security, but to any employee who processes any information. Therefore, when estimating risk, special attention should be paid to e.g. the planned frequency of training - this will reduce the likelihood of multiple incidents.

The next question concerned methods used by company representatives when assessing the risk of information security breach (Fig. 2).

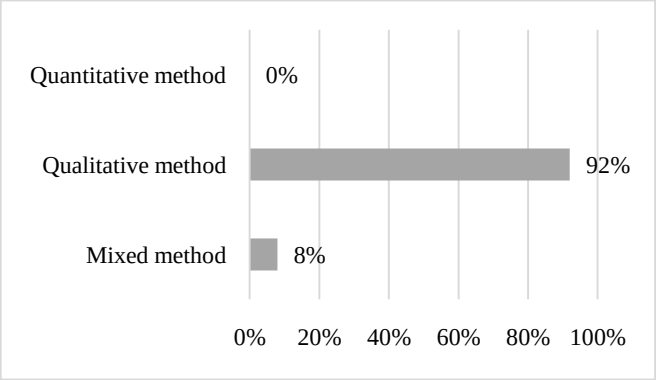

Fig. 2 *Answers of the respondents to the question: Please specify which methods of risk assessment do you use in your company?*
Source: own study

Most respondents indicated qualitative methods. Only 8% of the surveyed entities use mixed methods and none of them uses only quantitative methods. Where do these proportions come from? This probably results first of all from the specificity of the area in which the risk is determined, and secondly from the level of difficulty of individual methods. The area of information and the associated risk of security breach and, consequently, the area of resulting effects is sometimes difficult to quantify. Example: how to quantify the level of loss of reputation among customers of a business entity after occurrence of a specific incident? It seems to be very difficult; or: how to quantify the level of confidence of business partners in an enterprise that has a given information protection system. There are more examples of this type. That is why economic organizations very often lean towards qualitative methods in which (to simplify) the level is expressed subjectively on a descriptive scale (low, medium, high). The benefits of qualitative methods are [20] as follows:

• no need to value information (its availability, confidentiality, integrity) - it is very difficult and sometimes impossible - the value of information is a relative and variable concept;
• no need to estimate the costs of recommended risk management methods or calculate potential profit / loss;
• the possibility to identify general, significant risk areas;
• the possibility to consider and take into account, when estimating risk, the aspects that are very difficult to measure, such as company image, organizational culture, etc.;

Qualitative methods are more understandable to most people - they do not contain a complicated mathematical apparatus. For example, considering the answers in Figure 3, almost half of the respondents carried out a risk analysis only because of a certain requirement dictated by the introduction of the provisions of the GDPR. As much as 26% also perform the analysis less than once a year. Therefore, it should be assumed that all these business entities take up decisions guided by the choice of less work effort.

Going back, however, to risk assessment methods, despite the fact that none of the entities declared to use only quantitative methods, 8% declared mixed methods in which there are elements of methods containing a mathematical apparatus. Quantitative methods bring several benefits [20]: estimation and results are objective and comparable, the value of information is expressed in money and the results of risk estimation are expressed in to dimensions: financial and percentage. It should be assumed that 8% of business entities have more objective risk assessment results than the rest.

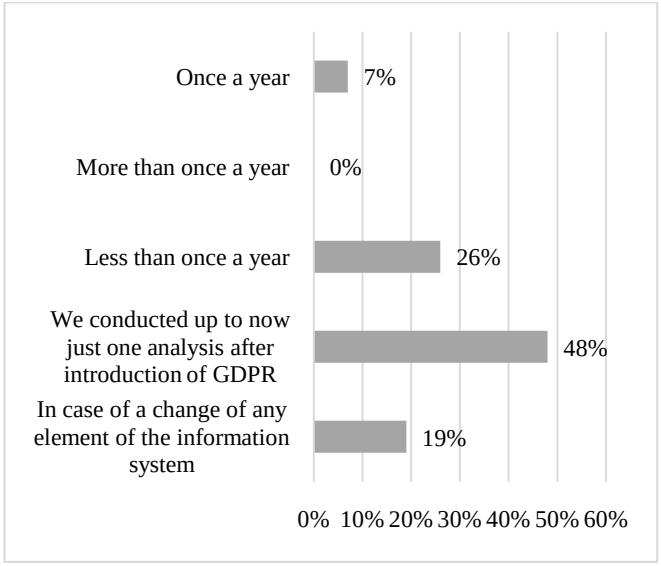

Fig. 3 *Answers of the respondents to the question: How often do you carry out the various stages of the risk management process*
Source: own study

As mentioned in the theoretical part of the study, risk management processes in the aspect of information security should be carried out in full whenever any element of the information system is changed. In the case of the surveyed business entities, only 19% declare this type of practice (Fig. 3). This may be due to the fact that only 28% of the surveyed enterprises take into account the recommendations of the ISO/IEC 27005 standard and 11% only part of the recommendations described in that standard (Fig. 4).

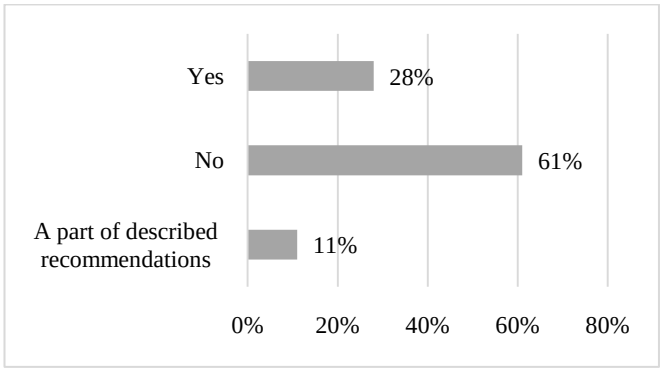

Fig. 4 *Answers of the respondents to the question: Do you include ISO/IEC 27005 recommendations in the information security risk management process?*
Source: own study

The majority of respondents (61%) admit that they do not apply the recommendations of an international standard during risk management. In a sense, this coincides with the answer to the question about the frequency of risk management. Entities that implement these procedures only because of the entry of the GDPR probably use ready-made (template) solutions offered by commercial companies for risk analysis. This, of course, does not mean that the lack of consideration of the ISO standard is equivalent to poor quality of the analyses. However, it should be assumed that they may slightly differ from standards generally accepted in the world.

The next, and last question asked to the respondents concerned the awareness of the respondents about the impact of the human factor on the security of information resources (Table 2).

Table 2. *Respondents replied to the question: Please specify to what extent (1- smallest, 5-largest) in your enterprise the information security may be influenced by the following factors*

1	social engineering activities	1.9
2	lack of knowledge	3.8
3	lack of experience	3.2
4	indifferent attitude to the work performed	1.6
5	fatigue	1.4
6	intentional, harmful actions of employees	1.1

Source: own study

Persons responsible for information security were asked to estimate the likelihood of factors having a negative impact on intangible assets directly related to employees. Thus, an attempt was made to answer the question: is the human factor in business entities treated equally seriously with other threats? According to respondents, the biggest threat is the lack of appropriate knowledge and experience among employees. This is the right approach - taken into account in 38% of process in the area of risk identification (Table 1). This may not be a highly satisfactory result, but quite optimistic compared to the other answers. In the adopted Likert scale from 1 to 5, the respondents estimated below the value of 2 the impact on information security of such factors as social engineering activities, indifferent attitudes to their work, fatigue or deliberate, harmful activities of employees. This is a surprising result, because IT security specialists officially confirm that cybercriminals use fraudulent tricks on a large scale to gain access to confidential company information and manipulate employees, and the human factor is the biggest challenge for companies in ensuring the expected level of security [21]. So how to justify the answers received? - perhaps respondents speaking about their own companies do not believe that these factors occur in their companies and employees are properly prepared in this aspect. But if one adopts this way of reasoning, the question should be asked: on what basis do they make such assumptions, since training in such a dynamically changing area of knowledge is marginalized at the stage of risk assessment (14% - Table 1).

4. Conclusions

Information security is currently one of the most dynamically developing areas of information management. Risk management is the crucial from the point of view of protecting intangible assets. It allows, as a result of the conducted identifications, analyses and assessments, to implement an effective information security policy in a business entity. Risk management is a process and as such it requires special diligence at every stage carried out. Each stage is the result of the previous one and contributes to the next one. That is why it is very important to follow specific guidelines described in detail in international standards: the guidelines to guarantee the best possible results.

This article includes research conducted in 117 business entities of the SME sector. The results obtained outline the overall picture of how the risk management process works in practice. Both strengths and weaknesses of this process are highlighted. Little interest of enterprises in the human factor in risk assessment and in identifying potential dangers caused by employees has been revealed. The research results encourage further observation of enterprises in the field of risk management, which will allow in the future to estimate the rate of growth of the awareness of business entities within the scope of use of recommendations of international standards.

5. References

1. M. Ghazouani, H. Medromi, A. Sayouti, S. Faris, *Information Security Risk Assessment - A Practical Approach with a Mathematical Formulation of Risk*, International Journal of Computer Applications, **103**(8), 36–42, (2014).
2. T. Peng, *ISO 27005 Information Security Risk Management* [Online]. SlideShare, (2016), [access date: 14.01.2020], URL: https://pt.slideshare.net/thomaspeng30/iso-27005-information-security-risk-management-download-free-template/7
3. V. Agrawal, *A Framework for the Information Classification in ISO 27005 Standard*, 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 264–269, (2017).
4. *ISO/IEC 27005:2014-01 Standard*, [Online], 2014, [access date: 14.01.2020], https://sklep.pkn.pl/pn-iso-iec-27005-2014-01p.html
5. B. Barafort, A.L. Mesquida, A. Mas, *Integrating risk management in IT settings from ISO standards and management systems perspectives*, Computer Standards & Interfaces, **54**, 176–185, (2017).
6. M.A. Fikri, F.A. Putra, Y. Suryanto, K. Ramli, *Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency*, Procedia Computer Science, **161**, 1206–1215, (2019).
7. C. Yang-Ngam, T. Chankoson, P. Aodton, *Influence of internal and external factors on supply chain information system risk management implementation*, International Journal of Supply Chain Management, **8**, 612–623, (2019).
8. A. Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet, *Taxonomy of information security risk assessment (ISRA)*, Computers & Security, **57**, 14–30, (2016).
9. L. Pan, A. Tomlinson, *A systematic review of information security risk assessment*, International Journal of Safety and Security Engineering, **6**, 270–281, (2016).
10. K. Zielosko, *Analiza ryzyka*, [Online], Encyklopedia Zarządzania, (2019), [access date: 14.01.2020], URL: https://mfiles.pl/pl/index.php/Analiza_ryzyka
11. J. Łuczak, *Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001*, Zeszyty Naukowe Akademii Morskiej w Szczecinie, **19**, 63–70, (2009).
12. G. Wangen, *Information Security Risk Assessment: A Method Comparison*, Computer, **50**(4), 52–61, (2017).
13. J. Stanik, M. Kiedrowicz, *Metoda analizy i szacowania ryzyka zasobu informacyjnego*, Roczniki Kolegium Analiz Ekonomicznych, Szkoła Główna Handlowa, Warszawa, **49**, 371–390 (2018).
14. K. Mersinas, B. Hartig, K. Martin, A. Seltzer, *Measuring Attitude towards Risk Treatment Actions amongst Information Security Professionals: An Experimental Approach*, Conference: Workshop on the Economics of Information Security, At Berkeley, CA, (2016).
15. S. Snedaker, C. Rima, *Chapter 6 - Risk Mitigation Strategy Development*, [in:] S. Snedaker, C. Rima (Eds.), *Business Continuity and Disaster Recovery Planning for IT Professionals*, Syngress, 337–367, (2014).
16. R.J. Chapman, *Simple Tools and Techniques for Enterprise Risk Management*, John Wiley & Sons, New Jersey, (2011).
17. C. Martani, *Risk Management in Architectural Design: Control of Uncertainty over Building Use and Maintenance*, Springer, Cham, (2014).
18. S. Ariyani, M. Sudarma, *Implementation Of The ISO/IEC 27005 In Risk Security Analysis Of Management Information System*, Journal of Engineering Research and Application, **6**(8), pp.01-06, (2016).
19. P. Kobis, *Human factor in the aspect of digital information in business enterprises*, Proceedings of the 9th International Conference on Management (ICOM) vol. II, Gödöllő, Hungary, 35–42, (13-14 June 2019).
20. P. Kawczyński, *Analiza ryzyka – metody szacowania ryzyka – cz. 2*, [Online], PortalODO by Lubasz i wspólnicy, (2014), [access date: 15.01.2020], URL: https://portalodo.com/analiza-ryzyka-metody-szacowania-ryzyka-cz-2/
21. KPMG, (2019). Report: *Barometr cyberbezpieczeństwa. W obronie przed cyberatakami*, [Online], KPMG, (2019), [access date: 17.01.2020], URL: https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-obronie-przed-cyberatakami.pdf