# Critical Success Factor for Integration of Cyber Security in Context of Managed Services

**Georg Sven Lampe[1], Marieta Olaru[2], Teodora Elena Fogoros[3] and Stephan Massner[4]**
*[1)2)3)4)] The Bucharest University of Economic Studies, Bucharest, Romania.*
E-mail: lampe@compliance-docs-group.com; E-mail: olaru.marieta@gmail.com
E-mail: massner@compliance-docs-group.com; E-mail: teodora.elena@icloud.com

**Please cite this paper as:**
Lampe, G.S., Olaru, M., Fogoros, T.E. and Massner, S.,2022. Critical Success Factor for Integration of Cyber Security in Context of Managed Services. In: R. Pamfilie, V. Dinu, C. Vasiliu, D. Pleșea, L. Tăchiciu eds. 2022. *8th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Graz, Austria, 25-27 May 2022. Bucharest: ASE, pp.741-748.
**DOI: 10.24818/BASIQ/2022/08/098**

**Abstract**
The increasing frequency of cyber security attacks and their impact on value-added business processes requires companies to appropriately address cyber security risks in the Risk Management Process (RMP). In the context of cybersecurity risks, companies can identify, assess and manage their business aims by applying 4C (Consultation, Communication, Coordination, Cooperation).
With this paper an increase in the efficiency of the RMP is proposed through an adaptation of the management activities by means of categorization of the information and group consolidation as well as the prioritization of measures. Trough adaptation it possible to establish a Cyber Security RMP (CS-RPM). The result is a predicted balancing of the benefits of the technology with the potential consequences of a CS risk threat event that drives proactive CS risk management. A system of guidelines for an information security-, cyber security- and data privacy-specific document structure of the managed services (MS) is also considered and be looked. The use of risk registers to map CS risks and the application of risk metrics is considered in more detail. Risk values to be quantified and their determination from risk measurements are explained in parts.

**Keywords**

Cyber security management, risk management process, cyber risk, managed services

**DOI: 10.24818/BASIQ/2022/08/098**

## Introduction

The ISO/IEC 27002:2013 provides best-practice requirements for ISO/IEC 27001:2013 and is therefore the second most important international standard when it comes to introducing an ISMS in a company. In combination with ISO/IEC 27005:2018, which describes the RMP for information security, the criteria for assessing, prioritizing and accepting risks are dealt with. The applying of RMP is applied by the risk managers, who assume responsibility for the residual risks, e.g. for the "supporting assets". If risks are not correctly managed since the beginning, a project may encounter issues even before it starts (Fogoros et al., 2021). The RMP is mostly limited to statistical threat catalogues and one-off risk assessments (Lampe et al., 2021). This also affects the risk assessments for the asset register. The financial impact increases due to cyber-attacks on vulnerabilities in information technology systems (Proofpoint, 2021). Due to the limited perspectives, relevant risks are out of focus and lead to a high willingness to take risks. Therefore, the RMP management activities for Information Security (IS) and Data Privacy (DP) related measures must be adapted. According to previous research (Ande et al., 2020; Bhamare et al., 2020; Ganin et al., 2020; Pandey et al., 2020), the RMP approaches to information security are indispensable for the application and management of cybersecurity (Fuertes et al., 2017). The paper is intended to present the management of cyber security risks using an RMP and to show a method for quantifying the risks. It can be assumed that there will be an improvement in risk measurement and risk analysis methods. The consultation as an iterative process causes a constant conditioning of the participants through communication, coordination and cooperation. In particular, the addressing of risks is addressed in order to more clearly delineate the involvement of those responsible for risk in cyber security risk management.

## 1. Literature review

Strategies, methods and their application of measures regarding Information Security (IS), Cyber Security (CS) and Data Privacy (DP) are challenges for every company. Cyber-attacks are increasing due to the digital transformation, opening up new areas of attack in all fields (Senol and Karacuha, 2020; World Economic Forum, 2021). The risks posed by digital globalization in the transport and traffic industry has made keeping business processes running a struggle for companies (Bakator, Đorđević and Ćoćkalo , 2019). In addition to these dynamic conditions, the COVID-19 pandemic has put additional strain on companies (Juergensen, Guimón and Narula, 2020). Besides to the globalization of markets, the modern business environment is characterized by constant changes in the field of Information and Communication Technology (ICT) (Sunday and Vera, 2018). Furthermore, it should be noted, that international framework conditions are constantly renewed or redefined, such as the revised ISO/IEC 27002 standard, which was newly adopted in February 2022. ISO/IEC 27002:2022 lists new controls, which are also indicators for the new thematic priorities. It is advantageous that the topics of avoiding, detecting and reacting to cyber-attacks as well as the protection of data come to the fore.

An understanding for risks and adapting efficiently to business changes are essential for the companies to maintaining a stable position within the industry. Through the requirements, companies have to consider the implementation of different management systems, which may bring additional risks to business performance (Vulanovic et al., 2020). Those responsible roles must establish management activities, which are necessary to identify and prioritize supporting applications, business processes and measures in order to conduct a business and risk impact analysis. In addition, these are linked to their probability of occurrence and their impact on the business process and must be quantified in order to adequately deal with cybersecurity problems due to the rapidly increasing attacks and vulnerabilities (Štitilis et al., 2020).

The TOP management of the companies must consider the trend changes as well as the risks in order to face the sustainable achievement of business goals (Popescu et al., 2020). This implies the need for effective decision-making and an adequate supporting information system (Elbashir et al., 2020; Rahimnia and Molavi, 2021). For a structured management, it is essential to better manage cyber security risks at the system and enterprise level. The responsible roles are to describe the technical and organizational measures in terms of processes in order to establish preventive and reactive measures for business processes relating to information technology. In addition, cyber security risks must be categorized in cyber security risk registers and the measures must be consolidated, prioritized and tracked in groups. The current literature addresses the mentioned business metrics and factors in different contexts however these do not describe how the RMP approaches to information security can be implemented for the application and management of cybersecurity for managed services.

## 2. Research methodology

Qualitative research as a process of analysis and interpretation was applied to achieve an appropriate combination of theoretical approaches and practical implementations. Based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013 (latest version published in 2022), the generic requirements for the ISMS were formulated as questions. The industry-specific requirements for companies in transport and traffic were selected from the main part and the associated ANNEX A, which contain more than 140 controls. Company-related individual questions ensured that the focus was on information and cyber security. Existing management systems were questioned with regard to their process orientation and risks. In addition, questions were created to obtain further and supplementary information (Stake, 1995; Yin, 2008). The evaluation on which this study is based only includes transport and traffic companies with a turnover of more than 100 million euros, whose questions are largely congruent. Only congruent questions were evaluated. Their results were processed for the practical implementation of suitable measures (Walsham, 1993; Strauss and Corbin, 1994). Overall, the results of seven Europe-based companies in the logistics sector were included.

## 3. Results and discussion

### 3.1. Interviews and roles

The interviewees, who are located at the strategic and operational level in the respective company, were guided through a standardized and predefined questionnaire. The fact that within the organizations the interviewees have different roles regarding information and cyber security (CS) and data protection was taken into account as shown in Table no. 1.

**Table no. 1. Specific roles in organizations - transport and traffic - rail transport company**

| Case | Employees | Responsibilities (interviewees) | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | *Roles* | | | | | | | *Other roles* | | | | | | | | | | |
| | | *TOP mgmt..* | | *Management* | | | *Administration* | | *TOP mgmt.* | | | *Management* | | | | | | *Administration* | |
| | | *Chief Executive Officer* | *Head of IT* | *Information Security Officer* | *Data Privacy Officer* | *Logistic support manager* | *IT system administrator* | *database administrator* | *Head of IT infrastructure* | *Head of digitization* | *Head of management systems* | *Risk manager* | *Information systems manager* | *Innovation manager* | *Systems support engineer* | *Logistic engineering manager* | *Project manager* | *Product manager* | *Solution architect* | *ICT system owner* |
| *1* | *>10k* | *x* | *x* | *x* | *x* | *x* | *x* | *x* | *x* | *x* | - | *x* | *x* | *x* | *x* | *x* | *x* | *x* | *x* | *x* |
| *2* | *>1k* | *x* | *x* | *x* | *x* | *x* | *x* | *x* | - | - | - | - | - | *x* | *x* | *o* | *x* | *o* | *x* | - |
| *3* | | *x* | *x* | *x* | *x* | *x* | *x* | *x* | - | - | *x* | - | - | - | *x* | *x* | - | *x* | *x* | - |
| *4* | | *x* | *x* | *x* | *x* | *x* | *x* | *x* | *x* | - | - | - | - | - | *x* | *x* | - | *o* | *o* | - |
| *5* | *<1k* | *x* | *x* | *x* | *x* | *x* | *x* | *x* | - | - | - | - | *x* | *x* | *x* | - | - | *x* | - | - |
| *6* | | *x* | *x* | *x* | *x* | *x* | *x* | *x* | - | - | - | - | *x* | *x* | *o* | - | - | *x* | - | - |
| *7* | | *x* | *x* | *x* | *x* | *x* | *x* | *x* | - | - | - | - | - | - | *x* | - | - | *x* | - | - |
| *Legend: mgmt. management, **x** present, **o** partially, - not present* | | | | | | | | | | | | | | | | | | | | |

Any conflicts of interest were treated separately. The roles with the comparable field of activity were assigned. The roles that cover a more extensive field of activity were identified. The tasks of the risk manager employed by a company include recognizing, analyzing and evaluating as well as monitoring, managing and controlling risks of all kinds. This means that the risk manager focuses on technical and financial risks as well as software /System and environmental risks. In the other companies, the tasks are distributed more individually, so that relevant risks are out of focus due to a limited perspective and can lead to a higher willingness to take risks.

In addition, additional internal company documents were viewed. These consisted of business process and system documentation as well as guidelines and procedural descriptions. The data collection was limited to supplementary information on the results of the interviews. If there were differences between the interviews and the documents viewed, an additional consultation was carried out.

### 3.2. Structured policy system

Formal and structured management of responsible roles is crucial for the successful use of technical and organizational measures. Therefore, the use of a hierarchical framework with clear definitions of relevant roles and responsibilities is necessary to assign and systematically implement the measures. A structured policy system should include preventative, detective, and corrective actions and controls, ranging from manual to fully automated. These should be developed in the relevant policies and procedures, documented and communicated via a more appropriate board. Structured policy system is recommended as shown in Figure 1. It is made up of three levels, the abstract level, a level with overarching concrete valid specifications and the level with implementation specifications for each area. The IS guideline is to be seen as an entry point into the document structure. This includes the overarching aims and principles for IS and CS as well as DP.

The management aims are to be agreed with the management, published internally and checked regularly. Based on the IS guideline and the Statement of Applicability (SoA) according to ISO/IEC 27001:2013, a large number of guidelines (topic-specific guidelines) and supporting documents must be established, which detail the regulations and instructions regarding information and cyber security as well as data protection describe and specify.

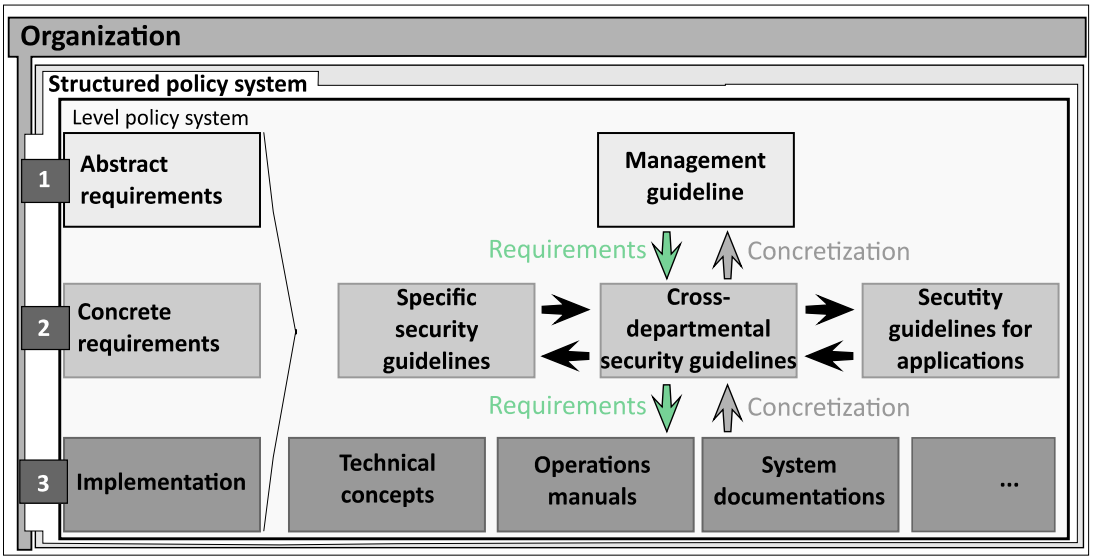


**Figure. no. 1. Elements of structured policy system**

On top of that, the use of further process-oriented specifications through area-specific or topic-specific guidelines is required. For example, the guideline for ensuring the information security (IS) of managed services is aimed in particular to

- customers and interested parties (stakeholders),
- the manager and executives responsible for information technology and information security,
- IS- and DP-officers, IT-coordinators, key-user as well as
- all employees regarding to or activities related to IS, CS, DP.

IS, CS and DP classified documents must be marked as such (e.g. public, internal, confidential, strictly confidential). All guidelines are to be aligned in a systematic and structured manner in order to enable a holistic approach to information and cyber security as well as data protection. These documents are subject to document control, regular review and are communicated to the relevant target groups after each change. Process-oriented reviews and approvals of documents as well as archiving and deletion must be defined. The associated processes are to be used in a goal-oriented manner, checked, cyclically trained and documented. In addition to the technical aspects, the guidelines also have to consider infrastructural, organizational and personnel issues in order to identify and implement the necessary security measures. Under these conditions, the structured system of guidelines with the associated measures is regularly checked, adjusted and can be used as part of an internal/external audit in accordance with ISO/IEC 27001:2013 certification.

### 3.3. Objectives of Managed Services (MS)

The ISMS regulates the security objectives as well as the general technical and organizational measures to ensure IS. An important part of the ISMS for MS is the description of the IS objectives and the comparison with the requirements for CS and DP.

The principles for dealing with IS, CS and DP are to be transferred to the structured policy system and assigned to the Managed Services division. One of the objectives is to continuously improve the security level of all aspects that are necessary for the operation of the customer's services or that affect this operation in any way. In addition, the systematic examination of risks, weak points and threats is seen as an essential part of establishing targeted technical and organizational measures and proactively avoiding threats. In general, these aims for MS can be summarized as follows:

- the highest priority is the protection of integrity and confidentiality of customer data as well as the authenticity of customers;
- another is to ensure the availability of the service according to the agreed service and operation level;

- the systematic examination of risks, weak points and threats is an essential part of the ISMS and a prerequisite for targeted technical and organizational measures with the aim of proactively avoiding threats and being able to ward off threats quickly if necessary;

- the basic objective of the ISMS is the continuous improvement of the security level of all aspects that are necessary for the operation of the services for customers or that influence this operation in any way.

With regard to the measures used for the scope, these are focused and goal-oriented procedures, definitions and regulations that are compared with the requirements of ISO/IEC 27001:2013 Annex A and ISO/IEC 27018:2019.

### 3.4. Pro-active management of cyber risk

Cybersecurity risk management means

- to weigh the benefits of applying information and technology against the potential negative impacts;

- to estimate their likelihood of the consequences resulting from the deployment of this application at the system, organizational or corporate level.

Risks are defined in terms of the likelihood of an event occurring and the potential adverse consequences of such an event (Kendrick, 2009). These estimates are often made subjectively. Therefore, it is often difficult to reach a consensus between the stakeholders involved. In addition, care must be taken not to ignore the risks (Kutsch and Hall, 2010). Since the responsible roles usually have limited resources, these are only used when the risks become hazards and occur. Therefore, proactive management of cybersecurity risks is recommended. Proactive management involves balancing the benefits of the technology with the potential consequences of a threat event within the RMP and is to be established within the organization. The following must be observed:

- the responsibility of a Cybersecurity Risk Officer (CRO) must be defined;

- the impact of cybersecurity risks in the RMP must be objectively assessed;

- the economic consequences as well as strategic and operational IS-, DP-aims must be taken into account in the risk treatment plan. Other dependencies such as relevant political decisions and regulatory implications must also be considered;

- a cybersecurity register is to be created so that the content of the register can be classified, aggregated with the IS and DP risk register (ISO/IEC 27005:2018), prioritized as follows and fed into the RMP for IS, CS and DP.

### 3.5. Adapted risk management activities

In many companies, the assessment of cyber security risks is largely spontaneous (ad hoc) and not process-oriented in the sense of ISO 27005:2018. The risk assessments only partially related to the protection goals and there were insufficient risk treatments. Applying a cybersecurity risk register, based on the organization's cybersecurity objectives, allows for the alignment of cybersecurity risk data with the organization's risks. Furthermore, the transfer of cyber security risks and knowledge into IS and DP-related risk management is made possible. With this cyber security risk register, the standardization of risks and their associated measures are compared with the addition of the IS- and DP- risk register. The risk reduction measures are controlled and communicated by the RMP. This is an advantage because it allows the risk owners to take the risk-treating measures expeditiously. The classification in the CS risk register was based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013, taking IS/DP aims into account. In addition, the cyber security risks were quantified to create IT budgeting for TOP management.

### 3.6. Cybersecurity risk register template

Cybersecurity risks shall be documented and tracked in cybersecurity risk registers to enable better management of cybersecurity risks at enterprise level. The following template, table 2, lists the most significant elements of a cybersecurity risk register.

**Table no. 2. Elements of cyber risk register**

| Elements of risk register | Description in detail |
|---|---|
| ID | Identifier number used to reference a risk in the risk register, which is continuous. |
| Priority | Criticality within the risk register (number or scale-related). |
| Description | Short explanation of the impact of the cyber security risk including root cause analysis. |
| Category | Multiple risk register entries are grouped together, such as for the Access Control (AC) category. Significant for comparison between individual risk registers during the grouped risks. |
| Valuation — Likelihood | Estimation of the probability of the risk occurring before any immediate action (first iteration of the risk cycle). |
| Valuation — Effects | Analysis of potential consequences or opportunities |
| Valuation — Risk level | The risk level is calculated on the basis of the probability estimate and the identified benefit/consequences of the risk. |
| Risk treatment | Dealing with the identified risk. Values for risk treatment are 3x3, 4x4 or 5x5 matrix (very low, low, moderate, high, very high). |
| Risk response | Short description of how to deal with the identified risk. Listing and comparison of measures for consolidation of measures (checklist). |
| Risk owner | Responsible and accountable for managing and monitoring the risk response. |
| Risk-status quo | Tracking the current state of this risk and any next activities. |
| Cost Risk treatment | Estimated cost of applying the risk treatment measures. |

By applying the above template, the CS risk management methodology for risk measurement and risk analysis as well as the register entry for CS risks is adapted. The approach ultimately leads from the assessment of potential consequences or opportunities of cybersecurity risks to the application and management of measures in which the cybersecurity risks are fully quantified. In addition, the results of the risk treatment are fully traceable and can be reproduced retrospectively.

### 3.7. Conditioning to Cyber Security RMP (CS-RMP)

Through a targeted transfer of treatment measures to cyber security risks, these can be conditioned by the responsible person in such a way that these measures have a more coordinated and more effective effect on specific risks for risk reduction. The following steps apply to the conditioning of cybersecurity risks from the cyber security risk register:

1. Information categorization: Categorized information and its consistent presentation within the company creates a uniform understanding: a) to measure cybersecurity risks, b) their negative impact on company aims; and c) the required measures treatment.

2. Redundancy reduction: Is the elimination of information/data duplication.

3. Grouping of measures: Risks that exploit the weak points of the "supporting assets" through generic threats and endanger sensitive and/or comparable information (information objects) are to be grouped in the first step.

4. Consolidation of measures in groups: The compromised information/data that lead to system failures are consolidated. i.e. the grouping of similar or related measures leads to a consolidation in which redundancies of measures are eliminated.

5. Prioritization of measures: The measures that are taken immediately (ad hoc) and/or at different times (change) to deal with operational risks must be assigned to a security program. Any necessary budgeting must be prepared for the approval process.

The consequence of the above conditioning is therefore an efficient and effective Cybersecurity RMP (CS-RMP). The CS-RMP is intended to help companies realize these added values while meeting the requirements of corporate aims, compliance with IS and DS-related topics (e.g. ISO/IEC 27001:2013) and the expectations of interested parties in relation to meet the protection objective. For this it is necessary to establish an internal and active control system as a process with the associated responsibilities in order to offer an appropriate guarantee for the achievement of goals and requirements. The concrete security controls serve the management for information, cyber security and data protection to establish, check and

condition the technical and organizational methods for reacting to cyber security risks. The detection, prevention or correction of security gaps and vulnerabilities is imperative for maintaining operational security.

## Conclusions

The impact of cyber risks on business processes can vary within a company's industry. If protective measures for the information to be protected are based on the organizational and technical RMP approach for IS, then a structured system of guidelines can be applied procedurally. This results in a reproducibility of the partial results and consequently a complete transparency for the risk assessment and risk treatment, which can be operated sustainably. If the process of applying the structured system of guidelines is cyclical, an iterative minimization of the residual risks can be achieved in the sense of a successive approximation to the minimal residual risks. The quality of the risk information can be improved by adapting the methods of the CS-RMP for risk measurement and analysis, including and using the cyber security risk register template with the assessment specifications. In this way, the cyber security risks within the organizations are analyzed and their impact quantified, and the risk-reducing measures are determined and implemented. As a result, system-level cybersecurity risk management is consolidated at the enterprise level. This means that the cyber security risks are collected and analyzed at the system level in order to align them with the strategic aims of the company. That promotes the entrepreneurial understanding of cyber security risks and has a positive effect on the definition of strategic company aims and associated operational measures. Based on RMP steps – Identify, Protect, Detect, Respond and Recover – that organize the basic cybersecurity activities, conditioning can support the responsible person in designing, assessing, managing and responding as well as reporting risks within the business units. This also means that CS analyzes can lead to missing or incorrect risk information that CS professionals are confronted with. It is therefore important to identify and eliminate the incorrect risk information within the CS-RMP. By consulting those responsible, a constant conditioning of those involved is brought about. Through comparing the endangered "supporting assets" they are assigned to the relevant risk category. In addition, it could be shown whether risk consequences can be measured by cyber security risk indicators and whether the integration of a cyber security risk management process (CS-RMP) brings advantages. Finally, the understanding and awareness of risk officers directly impacts risk and performance outcomes, and hence the "duty of care and proof" of vulnerabilities and exposures within the organization.

## References

Ande, R., Adebisi, B., Hammoudeh, M. and Saleem, J., 2020. Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, 54(07), p.101728.

Bakator, M., Đorđević, D. and Ćoćkalo, D., 2019. Developing a model for improving business and competitiveness of domestic enterprises. *Journal of Engineering Management and Competitiveness*, 9(2), pp.87–96. https://doi.org/10.5937/jemc1902087B.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K. and Meskin, N., 2020. Cybersecurity for industrial control systems: A survey. *Computers and Security*, 89, p.101677.

Elbashir, M.Z., Sutton, S.G., Mahama, H. and Arnold, V., 2021. Unravelling the integrated information systems and management control paradox: enhancing dynamic capability through business intelligence. *Accounting & Finance*, 61(S1), pp.1775–1814. https://doi.org/10.1111/acfi.12644.

Fogoroș, T.E., Olaru, M., Bitan, G.E., and Dijmărescu, E., 2021. The Risks ofAgile Methods in the Context of Digital Transformation. In: R. Pamfilie,V. Dinu, L. Tăchiciu, D. Pleșea, C. Vasiliu eds. 2021. *7th BASIQ International Conference on New Trends in Sustainable Business and Consumption*. Foggia, Italy, 3-5 June 2021. Bucharest: ASE, pp.756-764.

Fuertes, W., Reyes, F., Valladares, P., Tapia, F., Toulkeridis, T. and Pérez, E., 2017. An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence. *Systems*, 5(4), p.52. https://doi.org/10.3390/systems5040052.

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D. and Linkov, I., 2020. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, 40(1), pp.183–199.

International Organization for Standardization, 2013a. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO, [online] Available at: <https://www.iso.org/standard/54534.html> [Accessed 12 April 2022].

International Organization for Standardization, 2013b. *ISO/IEC 27002:2013 Information technology —*

*Security techniques — Code of practice for information security controls*. Geneva: ISO, [online] Available at: <https://www.iso.org/standard/54533.html> [Accessed 12 of April 2022].

International Organization for Standardization, 2022. *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. Geneva: ISO, [online] Available at: <https://www.iso.org/standard/75652.html> [Accessed 12 of April 2022].

International Organization for Standardization, 2018. ISO/IEC 27005:2018 *Information technology — Security techniques — Information security risk management.* Geneva: ISO, [online] Available at: <https://www.iso.org/standard/75281.html> [Accessed 12 of April 2022].

International Organization for Standardization, 2018. ISO/IEC 27018:2019 *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.* Geneva: ISO, [online] Available at: <https://www.iso.org/standard/76559.html> [Accessed 12 of April 2022].

Juergensen, J., Guimón, J. and Narula, R., 2020. European SMEs amidst the COVID-19 crisis: assessing impact and policy responses. *Journal of Industrial and Business Economics*, 47(3), pp.499–510. https://doi.org/10.1007/s40812-020-00169-4.

Kendrick, T., 2009. *Identifying and managing project risk*. 2nd ed. New York, NY: Amacom.

Kutsch, E. and Hall, M., 2010. Deliberate ignorance in project risk management. *International Journal of Project Management*, 28(3), pp.245–255. https://doi.org/10.1016/j.ijproman.2009.05.003.

Lampe, G.S., Olaru, M., Maftei, M. and Ilie, C., 2021. Information Security Management System and Cyber Security Strategy implementation in the context of SCRUM. In: R. Pamfilie, V. Dinu, L. Tăchiciu, D. Plești, C. Vasiliu eds. 2021. *7th BASIQ International Conference on New Trends in Sustainable Business and Consumption*. Foggia, Italy, 3-5 June 2021. Bucharest: ASE, pp.811-819.

Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A., 2020. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, 13(1), pp.103–128.

Popescu, L., Iancu, A., Avram, M., Avram, D. and Popescu, V., 2020. The Role of Managerial Skills in the Sustainable Development of SMEs in Mehedinti County, Romania. *Sustainability*, 12(3), p.1119. https://doi.org/10.3390/su12031119.

Proofpoint, 2020. *Quarterly Threat Q4*, [online] Available at: <https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes> [Accessed 12 April 2022].

Rahimnia, F. and Molavi, H., 2021. A model for examining the effects of communication on innovation performance: emphasis on the intermediary role of strategic decision-making speed. *European Journal of Innovation Management*, 24(3), pp.1035–1056. https://doi.org/10.1108/EJIM-10-2019-0293.

Senol, M. and Karacuha, E., 2020. Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering*, 2020, pp.1–19. https://doi.org/10.1155/2020/5267564.

Stake, R.E., 1995. *The art of case study research*. Thousand Oaks, CA: Sage Publications.

Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S. and Khorunzhak, N., 2020. National cyber security strategies: management, unification and assessment. *Independent Journal of Management & Production*, 11(9), pp.2341–2354. https://doi.org/10.14807/ijmp.v11i9.1431.

Strauss, A. and Corbin, J., 1994. Grounded theory methodology. In N. K. Denzin & Y. S. Lincoln Eds. *Handbook of qualitative research*. Thousand Oaks, CA: Sage Publications, pp.273–286.

Sunday, C.E. and Vera, C.C.-E., 2018. Examining information and communication technology (ICT) adoption in SMEs: A dynamic capabilities approach. *Journal of Enterprise Information Management*, 31(2), pp.338–356. https://doi.org/10.1108/JEIM-12-2014-0125.

Vulanovic, S., Delic, M., Kamberovic, B., Beker, I. and Lalic, B., 2020. Integrated management systems based on risk assessment: Methodology development and case studies. *Advances in Production Engineering & Management*, [online] 15(1), pp.93–106. https://doi.org/10.14743/apem2020.1.352.

Walsham, G., 1993. *Interpreting information systems in organisations*. Chichester, UK: John Wiley & Sons.

World Economic Forum, 2021. *The Global Risks Report 2021, Insight Report*, 16th Edition. Geneva: World Economic Forum. [pdf] Available at: <http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf> [Accessed 15 Apr. 2021].

Yin, R. K., 2008. *Case study research*. Thousand Oaks, CA: SAGE Publications, Inc.