Information Security Management System and Cyber Security Strategy implementation in the context of SCRUM

Georg Sven Lampe[1], Marieta Olaru[2], Mihaela Maftei[3] and Cristian Ilie[4]
[1)2)3)4)] *The Bucharest University of Economic Studies, Bucharest, Romania.*
E-mail: georg.sven.lampe@gmail.com; E-mail: olaru.marieta@gmail.com;
E-mail: mihaela.maftei@ase.ro; E-mail: dgaeur@gmail.com

Please cite this paper as:
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. Pleşea, 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
DOI: 10.24818/BASIQ/2021/07/102

Abstract

A cyber security strategy based on information security is the key to a trusted and sustainable digitization. To meet different regulatory requirements, the cyber security strategy must map a wide variety of frameworks. To manage specific cyber security threats, many organizations present different approaches to protecting critical data, software, and systems as part of an integrated cybersecurity strategy. However, the strategic potential of the scrum methodology for the sustainable management of global risks such as cyber-attacks within the Information Security Management System is largely unexplored. The paper aims to present how the implementation of ISMS and a cybersecurity strategy could be achieved by using the scrum framework. The authors of the paper would like to examine the current model of information processing by the Information Security Management System for cyber situations and to reconcile it with extended measures through an integrated cybersecurity strategy. Thus, a literature review on IT, Cybersecurity and Agile is conducting to identify the application of scrum in ISMS and cybersecurity strategy implementation. The findings show that the scrum framework supports ISMS and Cybersecurity strategy implementation, being used by many IT professionals and organizations.

Keywords

Information security management, cyber security strategy, scrum, risk management, risk processes, digitization.
DOI: 10.24818/BASIQ/2021/07/102

Introduction

The research carried out by the authors propose to investigate the extension of the existing risk management process (RMP) within the Information Security Management System (ISMS) and its effects on the measures due to the threat of cybercrime. 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). However, the RMP is mostly limited to statistical threat catalogs and one-off risk assessments. In addition, the use of technical and organizational measures only reduces risks to an economically appropriate level.

The distribution of the measures to operational teams is necessary, but a different understanding may lead to insufficient prioritization of security tasks and a limited perspective. Relevant risks are outside the focus and due to the different understanding of information security, the reporting in the annual management review is excessively positive. The ISMS must not only be operated to satisfy auditors (Todorovic, Todorovic and Tomas, 2020), but the basic ISMS security measures must be expanded. The corresponding measures are to be described in more organizational and technical details for the different areas of the organizations (Järvsoo, et al., 2018; Niemimaa and Niemimaa, 2017). In addition, the prioritization of business processes enables implementation in the correct order. Strategically, the ISMS must be supplemented by the "Cyber Security Operation" (CSO) category and operated more agile (Gomero-Fanny, Bengy and Andrade-Arenas, 2021; Kammergruber and Durner, 2018).

The paper aims to present how the implementation of an ISMS and a cybersecurity strategy could be achieved by using the scrum methodology. The first part of the paper presents the literature, standards and legal framework review on IT and cyber security fields at EU and Germany level. Results and discussion section describes the application of Agile approach, specifically scrum methodology, in IT and cybersecurity strategy implementation in ISMS.

Literature Review

The analysis of the specific literature shows that various standards have been issued for the regulation of cybersecurity, which the cybersecurity strategy shall fulfill. Below is a short overview of the most important uniform standards for cybersecurity, information security management systems and security frameworks.

Cyber Security Strategy (CSS)

The increasing digital networking simplifies joint communication, coordination, and cooperation (3C) and increases the competitiveness of companies (Lampe, et al., 2020). At the same time, malicious actions and cyber-attacks are increasing due to digital change and technological developments in ICTs and are opening new areas of attack in the fields of processing, hosting, transmitting, and using data in all domains (Senol and Karacuha, 2020; World Economic Forum, 2021). The areas of threat are constantly changing and expanding, while most resources and financial means of defense are stagnating, especially for SMEs (Teufel, et al., 2020), due to low financial investments in the field of cyber security (Zec and Kajtazi, 2015). Larger companies have the resources to solve cybersecurity problems, while small businesses often do not have the appropriate resources (Berry and Berry, 2018). This implies that common assumptions such as the availability of qualified workers, documented processes, or the planning of the IT budget must be changed in the security discussion. According to the Cyber Security Workforce Study 2019 (International Information System Security Certification Consortium, 2019), it is estimated that around 4.07 million cyber security experts are missing. Additionally, organizational IT security research has largely neglected the SME context (Heidt, Gerlach and Buxmann, 2019). The background to this is that cybersecurity is a young and immature area that is constantly evolving and whose skill requirements are changing rapidly (HM Government, 2018). SMEs should improve the ICT capabilities and digital technologies to acquire knowledge about standards, standardization, and management systems, since those are missing the chance to benefit from the implementation of management systems (Mijatovíc, Tošíc and Jovanovíc, 2019).

Cyber - attacks are not specific only to companies, but to the entire national, regional, and international security system at the level of critical defense, nuclear, energy, water supply, medical, cybercrime, and scientific research infrastructures (Štitilis, Pakutinskas and Malinauskaite, 2017). In this context, cyber security has become an important issue on the national and EU level, being perceived as a part of national and EU security. Thus, it is necessary to create and implement national and EU cybersecurity strategies to properly handle cybersecurity issues due to the fast growing of attacks and vulnerabilities (Štitilis et al., 2020). Implementing an adequate cybersecurity strategy in a changing cyber-physical operating environment requires an anticipatory attitude toward strategic decision-making and a toolset to support agility in strategy implementation (Kuusisto and Kuusisto, 2018). Legal and regulatory requirements present operators of critical and noncritical infrastructures with the challenge of protecting the existing IT structure and organization, where cyber-attacks could inject false measurement data that cause real overloads (Li and Hedman, 2020), affect industrial vital digital assets (Kim et al., 2019), and industrial control systems (Choi et al., 2016). To fulfil different regulatory requirements, the cyber security strategy must be able to map a wide variety of legal frameworks. Information security management systems and security frameworks form the basis for designing a CSS, because this ensures comprehensive protection of business processes and information objects across all supporting assets in the SoA. Cybersecurity must ensure existing and evolving IT systems and infrastructures in all business areas. The dynamic development of the business areas and organizational structures of organizations require agile ISMS teams that organize themselves and can adapt to agile Security Operations (SecOps). An adapted Development Operation (DevOps) approach is recommended for the operation and continuous development of IT systems because this describes the agile cooperation between development and IT operations (Kim et al., 2016). A "one-size-fits-all" principle is only partially effective as there are different security requirements for the various business areas in the organization. A cross-functional CSS is necessary that identifies and evaluates weak points, defines organization-wide aims, and how these can best be implemented in the organization. For the analysis and implementation of the risk management process (RMP) within cybersecurity, practical principles are presented drawing attention to key values and improved value retention. Particular attention is paid to the fact that the specific complexity of these frameworks listed above can be translated into a practical, user-friendly environment.

Strategic framework at EU level: Network and Information Security (NIS), Cybersecurity Act (CSA), General Data Protection Regulation (GDPR)

The first EU-wide cybersecurity law, the NIS Directive, came into force in 2016 to achieve a high EU-wide security level for networks and information systems (Directive (EU) 2016/1148 of The European Parliament and Of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union). The NIS guideline is currently being revised and will have measures for a high common level of cybersecurity in the future. NIS2 is a response to increasing threats through digitization as well as its connectivity and will affect medium-sized and large enterprises (SMEs) across the EU. Increased security requirements are being placed on supply chains and the relationships between providers, providing for simplified reporting requirements as well as stricter supervisory measures and enforcement requirements. The expansion of the SoA (e.g., public management, district heating, etc.) as well as the determination of the requirements for cybersecurity risk management including notification obligations of companies is planned. More uniform sanctions regulations are planned in the member states to achieve mandatory cooperation and a greater exchange of information in the management of cyber crises at the national and EU level. The EU Cybersecurity Act (CSA), which came into force in 2019, provided Europe with a framework for the cybersecurity certification of products, services, and processes (Štitilis et al., 2020). The current regulation is intended to help ensure that IT products, services, and processes, consider and implement cybersecurity requirements as early as the conception and development phase (Regulation (Eu) 2019/881 of the European Parliament and of the Council). The EU-wide GDPR regulates the handling of personal data in organizations, with the requirements for the protection of personal data being specified in ISO/IEC 27701:2019. However, there is currently no independent ISO/IEC 27701 certification. An ISMS certification according to ISO/IEC 27001:2013 and 27002:2013 in connection with ISO/IEC 27701 is not GDPR-compliant according to Article 42 GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council).

Strategic framework in Germany: IT Security Act (IT-SA) IT-Grundschutz catalogues

The IT-SA came into force on July 25, 2015, with the aim of significantly improving the security of information technology systems in Germany (IT Security Act - Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme IT-Sicherheitsgesetz). It is directly linked to other laws, such as the Federal Office for Information Security Act (BSIG), the Telecommunications Act (TKG), and the Telemedia Act (TMG) and should be amended accordingly NIS Directive from 2016 (Foulks, 2018). Currently, there is a legislative procedure for a second law IT-SA that contains expanded powers for cyber security authorities and expanded requirements for critical infrastructures (IT Security Act 2.0 Draft - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme). Federal Office for Information Security (BSI) standards contain technical and organizational measures (Federal Office for Information Security - BSI, 2021). The effort and costs for certification according to ISO 27001:2013 based on IT-Grundschutz catalogue are significantly higher than for certification according to ISO 27001 (Ionescu, Olaru and Sargut, 2019). The BSI standard is also cited as a reference model in EU guidelines but is only recognized to a limited extent internationally. Specific standards and guidelines have been issued that define the requirements for ISMS in accordance with ISO 27001:2013 for operators of business processes within telecommunications and energy services as well as for the operators of critical infrastructures. In Germany, the legislation (§ 11, Paragraphs 1a, 1b of the Energy Industry Act, 2005) stipulates an “appropriate security” against threats to the network control connection (German Bundestag, 2005). In the IT security catalog (SICAT) of the Federal Network Agency (BNetzA), the security requirements for "adequate security" are specified (German Federal Network Agency - Bundesnetzagentur, 2015). A functioning and certified ISMS in combination with ISO 27002:2013 and ISO 27019:2017 has been implemented since 2018. Thus, the critical infrastructures’ operators are legally obliged to report IT security incidents to the BSI (Federal Office for Information Security, BSI, 2016). There is no obligation to report outside the critical infrastructure.

Information security and cybersecurity standards

Many standards and norms regulate security management, such as ISO/IEC 27001:2013 and ISO/IEC 27100:2020. ISO/IEC 27001 is the internationally recognized standard for ISMS and contains specifications and requirements. The ISMS begins with a Business Impact Analysis and Risk Impact Analysis (BIA-RIA) that identifies the events which could disrupt business operations and processes. Once the threat has been identified by the treatment of incidents, a risk assessment must be carried out. The business impact, the likelihood of occurrence, and the recovery time must be determined, being required for critical business processes and applications. This evaluation considers only the business processes related to the information technology in the SoA and includes preventive and reactive measures. ISO/IEC 27100:2020 describes in general cybersecurity and relevant concepts, including its relationship to

information security and how it differs from ISO/IEC 27001:2013. However, the international standards for ISMS and cybersecurity do not describe which strategy should be implemented in combination.

Research Methodology

To achieve the research objectives, it is necessary to analyse the current state of knowledge of research on cybersecurity and existing threats as well as information security, into the context of legal frameworks and international standards. In addition, the theoretical aspect also focuses on studies on management systems and best practice approaches in order not only to confirm the empirical theoretical part, but also to illustrate the practical implications of this study. For this purpose, quantitative descriptive approaches have been used to strategically identify organizational approaches for the organizations that can explain the success or failure of technical and organizational implementation efforts. Business success requires controllable and resilient digitally supported business processes. Therefore, the existing model of information processing is to be extended to include the strategic elements to be implemented. As a result, the strategic organizational requirements of the ISMS are examined in the second part. The development of a conceptual approach is necessary to show that the ISMS plays a central role for critical and non-critical infrastructures. As part of the analysis of the organizational measures used, supplemented by a specific literature search, the authors want to examine how the ISMS could be expanded through the integration of a Cyber Security Operation (CSO) and information security management processes could be combined and improved, which ultimately affect the level of maturity.

Results and Discussion

Agility through an adapted DevOps approach from Scrum

Agility is an approach of developing solutions based on software applications and use that is focused on projects with changing requirements and provides the cooperation and interaction in the foreground. The main purpose is to deliver high-quality software, providing its users with features that include usability, utility, accessibility and others (Morandini et al., 2021). The agile software development is evolving in an emerging Software Engineering approach being currently practiced by many software companies (Marques and Da Cunha, 2019).

The use of valuable resources and time for documentation is limited to what is necessary and not to carefulness. An agile method divides projects into short development cycles (sprints), which normally last up to a maximum of four weeks. This enables agile ISMS teams to develop individual processes and test their functionality while taking changing requirements into account at the same time (Reyes et al., 2019). Agility defines the core values and principles for the project team, while Scrum defines and further develops the development process. Almost 75% of the software teams depend on Scrum or Scrum-Hybrid (digital.ai, 2020). The Scrum Sprint consists of several events (Brechner, 2015; Project Management Institute and Agile Alliance, 2017):

- *Planning:* The activities that will be carried out in each sprint.
- *Daily meet:* The team discusses which activities have been carried out, which activities they want to carry out and which activities exist that could prevent the continuation of the work.
- *Review:* Results against the requirements that are completed during each sprint. If necessary, acceptance or back to the product backlog.
- *Retrospective:* The aim is to improve the way people work when using the Scrum method (process improvement, not the product). The improvements are documented.

Product owners establish the aims of the requirements and are responsible for quality assurance. The development teams are responsible for implementing the requirements and independently organizing the processing through so-called sprints. A Scrum master plays a central role in the coordinated flow of sprints Morandini et al., 2021. Table 1 shows the practical approaches as scrum elements in the context of the ISMS:

Table no. 1. Specific security elements associated with the processes of ISMS

Product-Backlog	*Sprint-Backlog*	*Sprint-Review*
- Risk treatment measures; - Results of the effectiveness test; - Continuous improvement process through reviews (adapted security concepts, security quality gates, vulnerability scans, pen tests, etc.).	- Refinement of the risk assessment; - Detailing and implementation of the measures, - Maintenance of the current implementation status.	- Examination of effectiveness, achievement of objectives and results; - Security approvals; - Security acceptance.

The central principle of Scrum is the timing procedure of sprints, which are determined by the team as a sprint plan in terms of the process and duration. Planning and control of the sprint is then done with the help of the backlog, in which the elements are defined as tasks and implemented in a subordinate manner. Due to the responsible position, the product owner and scrum master determine the functions of the tasks and the successive sprints. After completion of the sprint planning, an overview of the completed and still open tasks from the sprint is created, on the one hand to recognize the progress of the task planning and on the other hand to be able to carry out continuous evaluation (Stellman and Greene, 2014). In addition to the sprint planning, there is a short daily meeting in which the team reports which tasks are being worked on the previous day and currently. In addition, problem areas that prevent progress are discussed. The Scrum Master supports team in solving these obstacles. Each sprint is followed by a detailed sprint test and a sprint retrospective. The productive teamwork in terms of time, work content, results, and effort in fixed processes ensures that function-oriented and deliverable work results are created. The team checks the effectiveness for weaknesses and successes during the retrospective. At the same time, the aim-oriented control with the help of the backlog enables integrated, efficient, and qualitative process management (Wysocki, 2019). This procedure can be mapped to the interaction between the ISMS and cybersecurity, as shown in Figure 1 below.

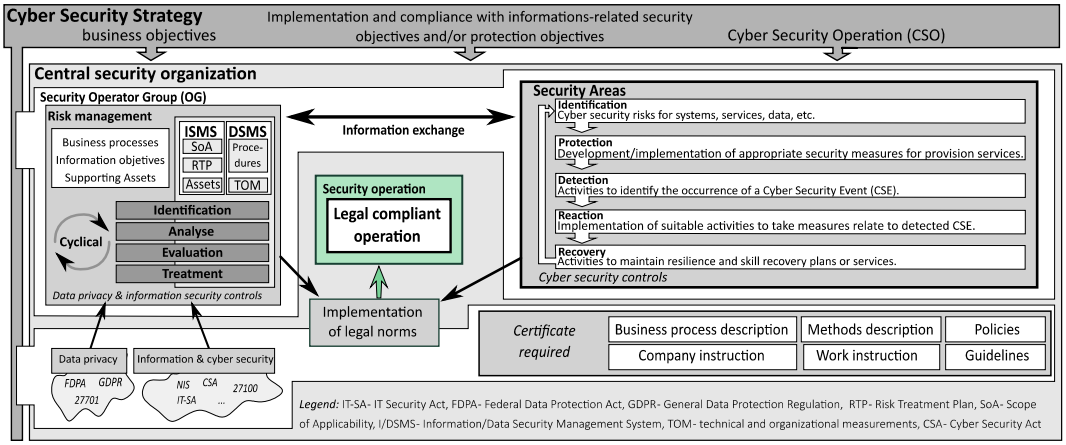

Fig. no. 1. Cyber Security Strategy related to ISMS

Agile cyber security

An established ISMS is evolving through the continuous PDCA cycle (Plan-Do-Check-Act). Similarly, the creation and implementation of a cybersecurity strategy could be approached through a PDCA cycle model (Senol and Karacuha, 2020). A continuous improvement of the security of the ISMS is similar to the results of agile methods. The iterations as short sequences of successive cycles of activity ensure that the results are checked immediately and that the actions are corrected in good time. The ISMS is certified according to the ISO 27000 standard published rules and safety catalog. The accreditation requirements apply to the audit process. For sole proprietorships with one or more locations, certification is carried out using a random sampling procedure with a specified time expenditure and interval. In addition, the organization processes and security measures are checked for conformity for the scope and not for the specific industry. Uniform information security for a legally secure operation is only possible if all cooperating operator groups (OGs) of the respective organization locations align their activities to achieve comparable security. As part of the ISMS, the existing processes shall be renewed, and new aims shall create as wells as implemented (operationalized) and centralized. It is therefore recommended to appoint a central ISMS and data protection officer from the top management for both OGs. Furthermore, those involved and cooperating operator groups can maintain a common IT security organization (roles, reporting channels, reporting).

Cyber security must deal with the connected systems and infrastructures of the customer (CIT) and process IT (PIT) as well as the newly emerging IoT (Internet of Things) systems of the entire organization. CIT and PIT each form security areas. It is therefore recommended to use appropriate security in complex IT systems and structures by agile ISMS teams in various areas of organizations. In comparing the IS policies of the OG, the ISMS teams in the area define generally applicable rules and processes for compliance with Information Security (IS) governance, the realization of synergies, and their cooperation. This establishes a decentralized responsibility and an agile security structure for the area. The implementation and further development of the area-oriented ISMS requirements are subject to binding and target-oriented and agile. All risk decisions using the RMP can be standardized for the security measures and then standardized. The escalation process does not end with the respective operator group, but with the security organization of the ISMS team (Marquardt, et al., 2018; Olaru, et al., 2017).

Conclusions

In this paper, first, we analyze the cyber security and ISMS scientific literature, standards and regulations and then we discussed the major research from industry and academia towards the implementation and development of a Cyber Security Strategy related to ISMS by using an innovative agile tool, respectively scrum methodology, which is a novelty in the information security research field. The implementation and operation of an ISMS in a diverse and complex business and IT environment within an organization ensures information security. An integrated cybersecurity strategy can be well represented based on ISMS information processing. Although the daily management activities derived from the Plan-Do-Check-Act are assigned to the ISMS management framework, combinations with more advanced tools such as Scrum, which promote innovation and digital transformation are possible. This extension shows the direction of agile information and cybersecurity organizations, adding value for the organizations, because essential business procedures have been tried and tested. For this, only the Scrum-specific elements must be added, which leads to a secure operation for information and cybersecurity. The ISMS carried out the RMP methodology in critical infrastructures to guarantee information security. On the one hand, this is due to the fact that the IT Security Act (IT-SA) (IT Security Act) in relation with the BSI-Critis Regulation (BSI-Critis Regulation) provides certification in accordance with ISO/IEC 27001:2013 mandatory for operators of critical infrastructures. On the other hand, the ISMS are only operated to create an appropriate level of security for the Scope of Applicability (SoA).

Cyber-attacks are on the rise and can become the greatest threat to the entire organization. The RMP is no longer based on static threat catalogs and one-time event, but the organizational and technical processes adapt to the security requirements and are continuously developing. The effects can vary depending on the sector, industry, and individual context in terms of the SoA of the business processes, the range, and importance of the information to be protected. A consistent structure in which the technologies optimally meet the security requirements and complement each other is necessary. Applications, business processes, technology structures and protective measures against cybersecurity must be based on the organizational and technical ISMS approach, in which the protection of critical information resources has priority. Therefore, organization-wide efforts must be made to protect critical data, software, and systems as part of the integrated CSS. If this is used sustainably as a CSO in companies, it enables the effects of threats to be worked out continuously, the uncertainties to be recorded, and the complexity to be reduced.

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(July), Article number: 101728.

Berry, C.T. and Berry, R.L., 2018. An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, 8(1), pp.1–10.

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, Article number: 101677.

Brechner, E., 2015. *Agile Project Management with Kanban*. Redmond: Microsoft Press.

BSI-Critis Regulation (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz BSI-Kritisverordnung - BSI-KritisV.

Choi, S.M., Kim, R.H., Kim, G.Y., Lee, H.K., Gim, G.Y. and Kim, J.B., 2016. A study of effective defense-in-depth strategy of cyber security on ICS. *International Journal of Security and its Applications*, 10(5), pp.235–242.

digital.ai, 2020. *14th annual State of Agile Report*, [online] Available at: <https://explore.digital.ai/state-of-agile/14th-annual-state-of-agile-report> [Accessed 15 March 2021].

European Parliament, 2016. Directive (EU) 2016/1148 of The European Parliament and Of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1.

European Parliament, 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

European Parliament, 2019.*Regulation (Eu) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52*

Federal Office for Information Security (BSI), 2021. *IT-Grundschutz*, [online] Available at: <https://www.bsi.bund.de> [Accessed 12 February 2021].

Foulks, J.A., 2018. German IT Security Law. *Journal of Law & Cyber Warfare*, 6(2), pp.165–190.

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.

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.

German Bundestag, 2005. *Energy Industry Act (Energiewirtschaftsgesetz - EnWG)*. Germany: BGBl I 2005, 1970.

German Bundestag, 2015. *IT Security Act (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme IT-Sicherheitsgesetz*.

German Federal Network Agency (Bundesnetzagentur), 2015. *IT security requirements catalog in accordance with Section 11 (1a) of the Energy Industry Act (IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz)*.

Gomero-Fanny, V., Bengy, A.R. and Andrade-Arenas, L., 2021. Prototype of Web System for Organizations Dedicated to e-Commerce under the SCRUM Methodology. *International Journal of Advanced Computer Science and Applications*, 12(1), pp.437–444.

Heidt, M., Gerlach, J.P. and Buxmann, P., 2019. Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, 21(6), pp.1285–1305.

HM Government, 2018. *Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views*, [online] Available at: <https://www.gov.uk/government/publications> [Accessed 5 January 2021].

International Information System Security Certification Consortium, 2019. *Strategies for Building and Growing Strong Cybersecurity Teams*, [online] *(ISC)2 Cybersecurity Workforce Study*, Available at: <https://www.isc2.org/Research/-/media> [Accessed 10 February 2021].

International Organization for Standardization, 2013a. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO.

International Organization for Standardization, 2020. *ISO/IEC TS 27100:2020 Information technology — Cybersecurity — Overview and concepts*. Geneva: ISO.

Ionescu, R.C., Olaru, M. and Sargut, K., 2019. Study of the Information Security Impact on the Business Continuity. In: K. Soliman, ed., *Proceedings of the 34th International Business Information Management Association Conference (IBIMA)*. Norristown, Pa: IBIMA, pp.4279–4287.

IT Security Act 2.0 Draft (Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme), [online] Available at: <https://www.bmi.bund.de> [Accessed 14 March 2021].

Järvsoo, M., Norta, A., Tsap, V., Pappel, I. and Draheim, D., 2018. Implementation of information security in the EU information systems: An Estonian case study. In: *Lecture Notes in Computer Science*. Cham: Springer International Publishing AG, pp.150–163.

Kammergruber, R. and Durner, J., 2018. Laboratory information system and necessary improvements in function and programming. *Journal of laboratory medicine*, 42(6), pp.277–287.

Kim, G., Humble, J., Debois, P. and Willis, J., 2016. *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. Portland: IT Revolution Press, LLC.

Kim, S., Kim, S., Nam, K.H., Kim, S. and Kwon, K.H., 2019. Cyber security strategy for nuclear power plant through vital digital assets. *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*, pp.224–226.

Kuusisto, R. and Kuusisto, T., 2018. Cyber Security Strategy Implementation Architecture in a Value System. In: P. Lehto, M and Neittaanmaki, ed., *Cyber Security: Power And Technology*, Intelligent Systems Control and Automation Science and Engineering. Cham: Springer International Publishing AG, pp.49–62.

Lampe, G.S., Maftei, M., Surugiu, I. and Ionescu, R.C., 2020. Study on Information Security Management System and Business Continuity Management in the Context of the Global Crisis. In: R. Pamfilie, V. Dinu, L. Tachiciu, D. Plesea and C. Vasiliu, eds., *6th BASIQ International Conference on New Trends in Sustainable Business and Consumption*. Bucharest: ASE, pp.942–949.

Li, X. and Hedman, K.W., 2020. Enhancing Power System Cyber-Security with Systematic Two-Stage Detection Strategy. *IEEE Transactions on Power Systems*, 35(2), pp.1549–1561.

Marquardt, K., Olaru, M., Golowko, N. and Kiehne, J., 2018. Study on Economic Trends, Drivers and Developments of the 21 St Century. In: R. Pamfilie, V. Dinu, L. Tachiciu, D. Plesea and V. Cristinel, eds., *BASIQ The 4th international Conference on New Trends in Sustainable Business and Consumption*. Heidelberg: ASE, pp.65–73.

Marques, J. and Da Cunha, A.M., 2019. ARES: An Agile Requirements Specification Process for Regulated Environments. *International Journal of Software Engineering and Knowledge Engineering*, 29(10), pp.1403–1438.

Mijatovíc, I., Toší, B. and Jovanovíc, M., 2019. The acquiring of the knowledge about standards in the digital era. *Amfiteatru Economic*, 21(51), pp.427–441.

Morandini, M., Coleti, T.A., Oliveira, E. and Corrêa, P.L.P., 2021. Considerations about the efficiency and sufficiency of the utilization of the Scrum methodology: A survey for analyzing results for development teams. *Computer Science Review*, 39, Article number: 100314.

Niemimaa, E. and Niemimaa, M., 2017. Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, 26(1), pp.1–20.

Olaru, M., Ionescu, R.C., Maftei, M. and Ilie, C., 2017. Application of Six Sigma tools for improvement of Information Security Management System. In: K. Soliman, ed., *Proceedings of the 30th International Business Information Management Association Conference, IBIMA 2017* - Norristown, Pa: IBIMA, pp.5779–5784.

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.

Project Management Institute and Agile Alliance, 2017. *Agile Practice Guide*. Newtown Square, Pa: Project Management Institute, Inc.

Reyes, F., Fuertes, W., Tapia, F., Toulkeridis, T., Aules, H. and Pérez, E., 2019. A BI solution to identify vulnerabilities and detect real-time cyber-attacks for an academic CSIRT. *Advances in Intelligent Systems and Computing*, 857, pp.1135–1153.

Senol, M. and Karacuha, E., 2020. Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering (United Kingdom)*, 2020.

Stellman, A. and Greene, J., 2014. *Learning Agile. O'Reilly*. Sebastopol: O'Reilly Media, Inc.

Štitilis, D., Pakutinskas, P. and Malinauskaite, I., 2017. EU and NATO cybersecurity strategies and national

cyber security strategies: A comparative analysis. *Security Journal*, 30(4), pp.1151–1168.

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), Article number: 2341.

Teufel, S., Teufel, B., Aldabbas, M. and Nguyen, M., 2020. Cyber Security Canvas for SMEs. In: H. Venter, M. Loock, M. Coetzee, M. Eloff, J. Eloff and R. Botha, eds., *Information and Cyber Security. ISSA 2020. Communications in Computer and Information Science*. Cham: Springer International Publishing, pp.20–33.

Todorovic, Z., Todorovic, B. and Tomas, D., 2020. The role of internal audit in the fight against cyber crime. *Economy and Market Communication Review*, 10(2), pp.514–529.

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

Wysocki, R.K., 2019. *Effective project management. Traditional, Agile, Extreme, Hybrid*. 8th ed. Indianapolis: John Wiley & Sons, Inc.

Zec, M. and Kajtazi, M., 2015. Examining how IT Professionals in SMEs Take Decisions About Implementing Cyber Security Strategy. In: *Proceedings Of 9th European Conference On Is Management And Evaluation (ECIME 2015)*, Proceedings of the European Conference on Information Management and Evaluation. Reading: Acad Conferences LTD, pp.231–239.