CRITICAL SUCCESS FACTORS FOR INTEGRATING A CIRCULAR INTERACTION MODEL FOR SECURITY PROCESSES IN DIGITAL TRANSFORMATION

Georg Sven LAMPE
The Bucharest University of Economic Studies, Romania, Romania
lampe@compliance-docs-group.com
Stephan MASSNER
The Bucharest University of Economic Studies, Romania, Romania
massner@compliance-docs-group.com

Abstract
A circularity of Information and Communication Systems (ICT) implies a sustainable design of associated management systems to comply with Cyber Security (CS), Information Security (IS) and Data Privacy (DP). Due to the rapidly changing of IT infrastructure and the variety of software systems, changes to the workflow processes in activities are becoming more complex in terms of content. At the same time, global and local threats to electronic information and data processing systems are increasing. An effective protection of the information to be protected for the business processes and business practices is of decisive importance for the success of the organization. Against this background, the strategic potential for a sustainable management of global and local risks in combination with a flexibly designed exchange of information within the management systems is largely unexplored. This paper proposes increasing the efficiency of the Risk Management Process (RMP) by adapting the management activities for IS, CS and DP. Through adapted risk management activities, the assessment of potential consequences or opportunities of risks can be quantified towards the application and management of measures. This includes the combination and expansion of implementing strategic elements for the categorization and group consolidation of management systems as well as the prioritization of secure and sustainable measures. Their dependencies are examined to show that the IS, in combination with the other management systems, plays a central role in the model-based standardization of the information elements. In addition, industry-independent and sustainable security disciplines are proposed in order to model the specific security processes or individual security-relevant process steps within existing company processes.

Key words: *Circularity; information security management; interaction model; risk management process; digitization*

JEL Classification: *D81, G32; M15, M41; O32;*

I. INTRODUCTION

The digitization is now the basis for local and global competitiveness for organizations. In concrete tems, the digital transformation of business models and processes offers new opportunities and risks for the progress of organizations. Parallel, global and local threats to electronic information and data processing systems are increasing. At the same time, management systems used today are heavily dependent on ICT-based services and the associated risks. Existing cyber vulnerabilities in Information and Communication Systems (ICS) can be exploited by extortionate ransomware attacks (Proofpoint, 2022). Business processes and sustainable management systems for Information Security (ISMS), Cyber Security (CSMS), Data Privacy (DSMS) and Quality (QMS) can not only be negatively influenced by the increasing risks (e.g. cybercrime, crises, etc.), they can also threaten the economic situation and the existence of organizations. Due to the increasing expansion of the information technology infrastructure with new „intelligent" technologies and automated applications, the continuous further development of the technical and organizational adaptation processes to the security requirements is indispensable. It is therefore becoming more urgent to face the challenges of IS, CS and DP in the digital transformation in order to protect and secure the communicating information (IO – Information Objects) via the supporting values (SA – Supporting Assets) and to make the circulating processes sustainable. If risks are not correctly managed since the beginning, a project may encounter issues even before it starts (Fogoros et al, 2021).

For the achievement of strategic and operational business objectives, the operationalization of business processes is indispensables for every organization. To do this, the requirements for security, quality and sustainability must be integrated into the business processes with the associated information flows or into the implementation of the measures, optimized and operated in an agile and sustainable manner due to rapidly

changing requirements. Core of this activity is the establishment, evaluation and further development of the current business model within digitization and the management systems in compliance with the specific requirements for information and cyber security as well as data protection in order to make the organization future-proof and sustainable. This requires a deeper understanding of current mechanisms, identification of new opportunities and risks as well as more systematic analysis of successes and failures as well as the development and implementation of sustainable solutions-oriented measures (best practices). In this context, the study focuses on the analysis of management activities for CS, IS and DP in order to categorize, to prioritize and to sustainable them by adapting them to the Risk Management Process (RMP). Therefore, was carry out the analysis of current approaches regarding the dependencies of the management systems (IS, CS, DP), the reference to global and local risks (RMP - Risk Management Process) related to process-oriented management activities and the closer consideration for a circularity and the continuous improvement in the context of critical success factors for management systems.

The analysis of the existing information processing model and the combination and expansion of the strategic elements to be implemented, such as protection objectives, are necessary in order to show that the ISMS in combination with the other management systems plays a central role in the model-based standardization of the information elements.

In addition, an organizational framework must be analyzed that incorporates the minimum legal requirements of the relevant ICT-based services (critical, non-critical) in terms of adequate protection and compares them with the strategic and operational aims for CS, IS, DP and sustainability. The most recent changes to security standards at EU level must also be taken into account. In particular, the interactions of business processes are to be highlighted in order to present the systematic examination of risks, weak points and threats. Within the organizations, different roles are taken regarding IS, CS and DP, which have to be taken into account. As an iterative process (3C – Communication, Coordination, Cooperation) in addition through the consultation with those responsible causes a constant conditioning of the participants. It can be assumed that there will be an improvement in risk measurement and risk analysis methods (Lampe et. Al., 2021). In particular, the addressing of risks is dealt with in order to more clearly define the participation of those responsible for risk in risk management. Optimized and appropriate information flows also require agile flexible business process structures. In this context, the categorization and group consolidation of strategic elements of the management systems as well as the prioritization of secure and sustainable measures are also dealt with. In addition, the risk management process (RMP) of the ISMS is usually limited to static threat catalogues and one-off risk assessments for the Scope of Applicability (SoA) (Lampe et al., 2022). Therefore, the RMP management activities for the CS, IS, DP-related measures must be adapted, then 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).

For this purpose, this research work deals with industry-independent security disciplines in order to model the specific security processes or individual security-relevant process steps within existing company processes. Through adapted risk management activities, the assessment of potential consequences or opportunities of cybersecurity risks can be quantified towards the application and management of measures.

II. LITERATURE REVIEW

Globalization and digitization have created a dynamic environment in which processes cannot be planned in detail due to the dependence on information and events. In addition, modern business environment is characterized by constant changes in the field of Information and Communication Technology (ICT) (Sunday and Vera, 2018). The increasing digital networking simplifies joint communication, coordination and cooperation (3C) and increases the competitiveness of companies, but at the same time, security threats (e.g. phishing are increasing (Lampe et al., 2020; World Economic Forum, 2022).

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). Currently, the main challenge for public administration is to ensure greater flexibility and competitiveness, and at the same time, support the rapid transformation into sustainable and digital companies (Grigorescu & Mocanu (Niculae), 2020). In addition, an innovative digital transformation of systems and processes in organizations puts the ability to absorb change to the test because many shows signs of overloading (Cho et al., 2016; Järveläinen, 2012). Organizations adopt management practices that are considered legitimate by others, irrespective of their real usefulness (Carpenter and Feroz, 2001). However, legal concerns and

requirements for data security and protection are perceived as obstacles in digital transformation (Marquardt et al., 2018) and a security awareness program and a security culture should be developed (Da Veiga et al., 2010) in the organisation. It should therefore be noted that international standards are being renewed, such as the revised ISO/IEC 27002 standard (February 2022). The new controls for avoiding, detecting and responding to cyber-attacks, as well as data protection, are at the same time indicators of the new thematic priorities. 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).

Every organization have the challenge that many IT system solutions are used for different purposes and that the interactions of business processes and information flows are constantly changing or expanding. In order to meet various regulatory, organizational and technical requirements, the management systems must not only be able to map the most varied of legal frameworks, but also flexibly adapt, combine and improve the diverse and complex business processes and their information flows to the constantly changing requirements. 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). The COVID-19 pandemic with the dynamic conditions has put an additional burden on companies (Juergensen et al., 2020). All organizations faced the challenge of organizing teleworking ”as a work arrangement to keep their employees safe and to ensure continuity in delivering critical public goods and services” (Grigorescu & Mocanu (Niculae), 2020). Through the risks, which posed by digital globalization within the energy and IT/telecom industries have made it a struggle for companies to maintain business processes (Bakator et al., 2019). Efficient adaptation to changes in companies is essential for a stable position within the industry. A deeper understanding of the current mechanisms for identifying new opportunities and risks is imperative to ensure a more systematic analysis of successes and failures as well as the development and implementation of sustainable solution-oriented measures (best practices). Organizations should consider implementing different management systems, which may pose additional risks to business performance (Vulanovi´c et al., 2020). For an analysis of the business and risk effects, those responsible must establish management activities that lead to the identification and prioritization of sustainable measures. In addition, these must be quantified with their probability of occurrence and their effects using Key Performance Indicators (KPI) in order to appropriately deal with security problems due to the rapidly growing attacks and vulnerabilities (Stitilis et al., 2020). Those responsible for the company must take into account the trend changes as well as the risks in order to face the sustainable achievement of business goals (Popescu et al., 2020). This means that the responsible roles must 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. This implies the need for effective decision-making and an adequate supporting information system (Rahimnia et al., 2021; Elbashir et al., 2020).

The current literature deals with the mentioned business metrics and factors in different contexts, however these do not describe how the RMP approaches to information security for the application and the sustainable and qualitative management in combination with CS and DP. Practical principles are presented for the analysis and implementation of management activities, which draw attention to factors critical to success and improved value retention. Particular attention is paid to transferring the organizational processes and frameworks listed above into a practical, user-friendly environment in order to ultimately enable the integration basis for cross-company and agile risk management.

III. RESEARCH METHODOLOGY

1. Purpose and objectives of the research

Qualitative research as a process of analysis and interpretation was applied to achieve an appropriate combination of theoretical approaches and practical implementations. In addition, the authors research serves to improve the understanding of behaviour and decision-making for business process and Risk Impact Analysis in the area of Information Security (IS), Cyber Security (CS), Data Privacy (DP) and quality within digital transformation. For this purpose, the theoretical aspect also focuses on studies from the various management systems (ISMS, CSMS, DPMS, QMS) and the requirements for standards and legal norms as well as best practice approaches for sustainability of research is analysed, on the one hand to illustrate the practical effects of this study and, on the other hand, to confirm the empirical theoretical part. The main following hypotheses are to prove by the research:

H1) Due to a constant convergence of organizational structures, the various management systems (IS, CS, DP) pursue specific purposes and aims in the digital transformation that must be taken into account in legal and

organizational terms.

H2) An organizational and process-oriented framework can be defined that shows the adaptation of management activities by means of categorization of information and group-wise consolidation as well as the prioritization of measures in order to achieve an increase in the efficiency of the risk management process (RMP).

H3) An organizational and process-oriented framework can be defined that shows the adaptation of management activities by means of categorization of information and group-wise consolidation as well as the prioritization of secure and sustainable measures in order to achieve an increase in the efficiency of the risk management process (RMP).

Controllable and agile and resilient as well as digitally supported business processes and information flows are of great importance for business success. Therefore, quantitative descriptive approaches are used to identify the strategic organizational approaches for the organizations. According, the existing model of information processing is to be expanded to include the strategic elements to be implemented, in order to show that the ISMS plays a central role in combination with various management systems. As a result, the strategic organizational requirements of the IS, CS, DP and quality as well as the sustainability within the digital transformation are examined in the further part. In addition, the research conditions are differentiated in order to create the prerequisites for business and process analysis. Furthermore, the research conditions are considered in a differentiated manner in order to create the prerequisites for business and process analysis for the information or process interactions to be protected. Only then is it possible to carry out the Business Impact Analysis (BIA) and the Risk Impact Analysis (RIA) as well as the process optimization.

The main research analyses the correlations between the dependencies of the various management systems (IS, CS, DP, Quality) in context of sustainability and the changes caused by business-critical risks within digitization. In addition, the reduction of demonstrable risks through suitable corporate strategies and behaviour within the ISMS is analysed in more detail in order to achieve an increase in the efficiency of the Risk Management Process (RMP) by adapting management activities. The applying of RMP is applied by the risk managers, who assume responsibility for the residual risks, e.g. for the "SA - Supporting Assets". 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 IS, CS, DP, quality and sustainability related measures must be adapted. Through the iterative process of consultation, communication, coordination, cooperation (4C), a constant conditioning of the participants is brought about and a proactive management is forced (Lampe et al., 2021). As a result, the business processes (technical and organizational) have to be assessed with regard to quality and risk parameters for IS, CS, DP, Quality and sustainability and the interactions of the processes have to be analysed. Only in this way can the effects and the associated risks be identified, assessed and reduced through specific measures.

In this context, the business processes and their information flows can be combined and improved, which ultimately forms the integration basis for the cross-company security disciplines. Digitization creates partially or fully automated processes for companies as service providers with critical and non-critical ICT-supported infrastructure. It is important to protect these processes against attacks on their infrastructure. Concrete IT security standards and the establishment of an ISMS in accordance with ISO 27001:2013 are required for the value-adding business processes of companies

2. Data collection

As part of the analysis of the organizational measures used, supplemented by a targeted literature search, the current status of information security in companies and how it can be improved is also examined. Based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013, ISO/IEC 27002:2022, the generic requirements for the ISMS were formulated as questions. The decisive factor here is the consideration of the legal conditions and standards for mandatory compliance with information security. These questions or the list of questions were created to enable data collection on the current status of information security for companies from various industries and to analyse, evaluate and make the effects of the established organizational and technical measures on IS, CS, DP, quality and sustainability.

The interviewees, who are located at the strategic and operational level in the respective company, were guided through a standardized and predefined questionnaire. In addition, internal company documents were viewed. This included guidelines, business and process descriptions and system documentation. The data collection on CS, DP, quality and sustainability was limited to supplementary information on the results of the interviews. A supplementary consultation took place as soon as differences between the interviews and the documents examined became apparent. The evaluation on which this study is based only includes organizations within sectors energy, information and telecommunication with a turnover of more than 500 million euros. It was

ensured that the questions were mostly congruent and that 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 8 Europe-based companies in the energy branch and 7 Europe-based companies in the information- and telecommunication branch were included. The industry-specific requirements for companies in those sectors 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 IS, CS, DP, quality and sustainability. Existing management systems were questioned with regard to their process orientation and risks. In addition, questions on quality and sustainability were created to obtain further and supplementary information (Stake, 1995; Yin, 2008).

IV. RESULTS AND DISCUSSION

1. Categorization of management systems in the context of security, privacy, quality

In modern companies, the work and business processes are based on corresponding IT solutions with reliably functioning information processing and are essential for maintaining secure and sustainable operations. Every insufficiently protected component in the context of ICT (Information and Communication Technology) often represents an underestimated risk factor that can even threaten the existence of some organizations. Information security, data privacy and quality are often defined via protection objectives without anticipating a specific technical implementation, as shown in figure 1.

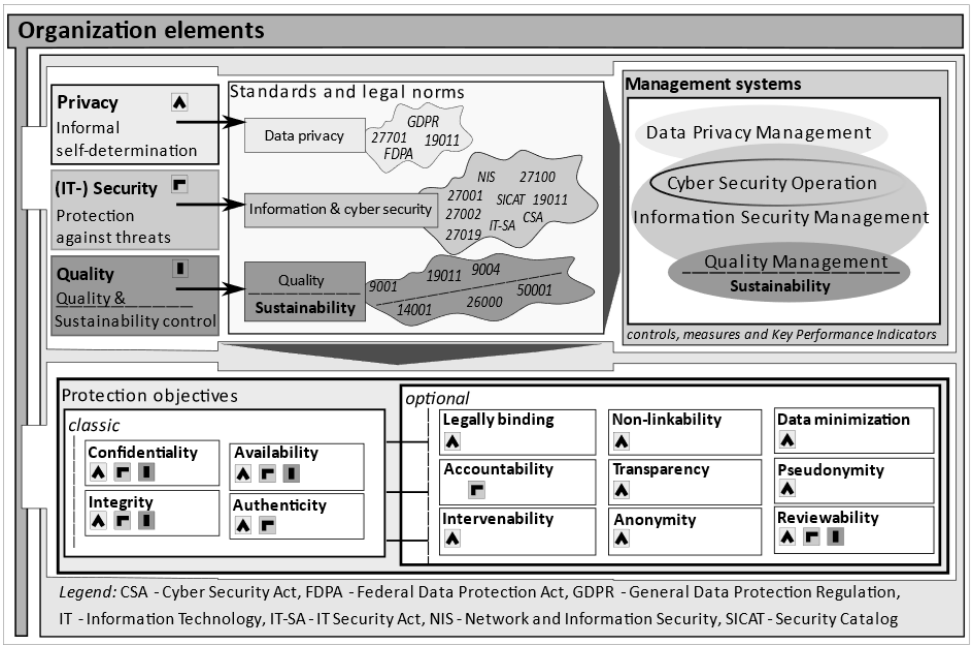

Figure 1 - Elements privacy, security and quality related to protection objectives
Source: Authors, 2022.

The fact that security is linked to protection objectives makes it easier to derive specific requirements and measure their implementation more objectively and easily. The focus here is on the ISMS, which is intended to ensure the protection objectives (confidentiality, integrity, availability, etc.) of information, applications and IT systems and is the part of general risk management. The process management of ISMS is continuous according to the PDCA-cycle (Plan-DO-Check-Act) in which the internal strategies and concepts are constantly checked for their efficiency and effectiveness and updated if necessary. An active ISMS can contain risks and prevent damage, which minimizes the overall residual risk. The same process management applies to the objective-oriented security of information within the DPMS. Data protection is the protection of personal data and secures the basic right of persons to informational self-determination. This gives people the freedom to determine how their data is handled. Personal rights and privacy should be preserved. Due to the advancing development of information technology and digital technology, the importance of data protection has changed and increased. Modern IT makes it possible to collect, analyse and save more and more data more easily. Data protection laws (e.g. GDPR) regulate the collection, use, storage and transfer of personal data. Depending on the organization

that collects, stores, processes or publishes data, different data protection regulations can be used. The legal requirements and guidelines for ISMS and DPMS implementation in the organization are often delegated to responsible managers for Information Security and Data Privacy.

A certified quality management system (QMS) according to ISO/IEC 9001:2015 requires a PDCA control loop that ensures constant further development in the sense of a Continuous Improvement Process (CIP). Environmental protection certification according to ISO/IEC 14001:2015 stands for sustainable corporate management. The aim of the standard is that all environmentally and energy-related processes and processes in a company are analyzed and optimized. In addition, a company can audit an Energy Management System (EnMS) in accordance with ISO/IEC 50001:2018 for sustainable climate protection. In order to control the environmental impact of the administration and storage locations, every company can record and analyze the main energy consumption.

The most recent changes in security standards at the EU level, which regulate the management of information security, cyber security, data protection, are ISO/IEC 27002:2022 and the Telecommunications Telemedia Data Protection Act (TTDSG). 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. However, the implementation of the new measures is not enough, because new or expanded requirements have been added to the known measures. The main new features of the version consist of an improved and updated structure and 11 other measures. ISO27001:2013 (Annex A) counts 114 measures in 14 different areas. The new version divides 93 measures into four areas (organizational controls - 37 measures, people controls - 8 measures, physical controls - 14 measures, technological controls - 34 measures). In addition, the new standard also explicitly defines the goals of the measures and lists other attributes, such as how they work. The focus is now on the purpose of the measure. Due to the change in ISO 27002, ISO 27001 will also be adapted promptly in order to restore the alignment of the standards.

The TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz) - combines the regulations of the Telecommunications Act (TKG) and the Telemedia Act (TMG). However, the TTDSG not only contains rules on data protection, but also regulations on the areas of tele media and telecommunications. This also results in different areas of application and protection purposes compared to the GDPR. As is well known, the GDPR is intended to guarantee the protection of personal data and thus protect the right of personality and the right to informational self-determination of natural persons. With the TTDSG, on the other hand, the purpose of protection is the integrity of the user's end device. The information involved does not necessarily have to be personal data.

Those responsible carry out cyclic audits (internal, external) to identify tampering or prevent it. The implementation is carried out by an "internal control system", which can consist of organizational and technical measures and therefore places important demands on the "integrity" of IT systems and IT services. It should ensure that processes run properly and that the laws are complied with.

2. Minimum requirements for operators of critical infrastructures

The minimum requirements of the relevant ICT-based services with regard to adequate protection are specified in the sector

1) Energy (BSI-Critis, §2, 2016): in §11 Paragraph 1a, 1b and 1c (mandatory notification) of the Energy Industry Act (EnWG), IT security act and IT security catalogs;

2) Information technology and telecommunication (BSI-Critis, §5, 2016): in § 109 Paragraph 1 - 5 (obligation to report) of telecommunication act (TKG) by the Federal Network Agency (BNetzA) represented and regulated.

Critical infrastructures are organizations and facilities of major importance to the state community, the failure or impairment of which would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences. The requirement in the energy sector is the evidence (from 2018) of a functioning and certified ISMS in accordance with ISO / IEC 27001 (2013) in conjunction with ISO / IEC 27002 (2013) and ISO / IEC 27019 (2019). For the information technology and telecommunications sector, there is no obligation to provide evidence of a functioning and certified ISMS in accordance with ISO / IEC 27001 (2013) in conjunction with ISO / IEC 27002 (2013). Only a security concept needs to be drawn up in accordance with the requirements of the Federal Network Agency and submitted for approval. The operators of critical infrastructures in the energy, information technology and telecommunications sector have been given additional reporting obligations regarding IT security incidents to the Federal Office for Information Security (BSI). As a result, an ISMS is always individually adapted to the organizational structure, since the specific characteristics of information security as well as the associated protective measures and the way in which this level of information security is to be achieved can differ in individual cases. A management system for the processing and handling of personal data must be set up in accordance with the EU-wide GDPR (General Data Protection Regulation).

The pre-condition for establishing an appropriate management for information security and data protection are in area of Risk Management (RM). Business risks are identified using the Risk Management Process (RMP), which includes both strategic risks for the organization's development and operational risks. Sustainability and Corporate Social Responsibility (CSR) are important factors for successful corporate development today. However, there is no obligation to provide evidence of a functioning and certified EnMS in accordance with ISO/IEC 50001. With regard to non-European companies, the obligation to submit a sustainability report applies to all companies that achieve net sales of more than €150 million in the EU and at least have a subsidiary or branch in the EU. The obligation to report on sustainability applies to companies that have more than 500 employees on average in a financial year. whose turnover is more than 40 million euros or whose balance sheet total is more than 20 million euros within the EU. The focus is on successful implementation to ensure the balance between economic, ecological and social corporate aims. For a holistic approach to the management systems, the business processes must be aligned with the requirements for IS, CS and DP and expanded to include a sustainability management system. The extension of the RMP from the ISMS with the data protection aspects of the processing activities from the DPMS and the sustainability aspects from the EnMS (Energy Management System) and the CSR-reporting are necessary to enable compliance with the management requirements for secure circularity in the company

3. Management modelling

Any kind of information basically represents an essential value within an organisation. Information assets can be information and data regardless of their form, but also objects (e.g. hard drives, files, etc.) and persons with the associated functions (e.g. TOP management, IS-Officer, DP-Officer, administrators, etc.). In addition to the information types mentioned above, intangible values, reputation and image are also considered as possible information values or categories (ISACA, 2016). Most of the information is created, stored, communicated and processed with the existing IT systems. As a result, information values are an integral part of every company and are viewed as worthy of protection. Because there is a consideration between information which are actually to be secured and the dependent components, a distinction must be made here between specific IT assets, as secondary assets and the actual information assets, as primary assets. The management of information assets worth protecting are also regulated in ISO / IEC 27001 (Appendix A.8) and ISO / IEC 27701 (Point 6.5). The ISO / IEC 27005 (2014) standard also specifies the so-called Supporting Assets (SA) in Part B.

Physical components can have weak points on which a threat acts and becomes an applied threat to the information to be processed and protected. Since it is not the information assets themselves that are exposed to a certain risk, but the supporting assets on which the information assets are based, the threats within the RMP must be dealt. The starting point is an overview model of the processes in which all significant interactions of the process under consideration are listed, as shown in figure 2. The aim of the approach is the detailed description of the information objects to be exchanged using information structure models. The context (organizational, legal, economic, technical) in which the information objects are used is determined by the models of the higher levels. The basis of all model types is a reference library, the elements of which are defined by classes with roles, objects, interactions and channels, as shown in figure 2.

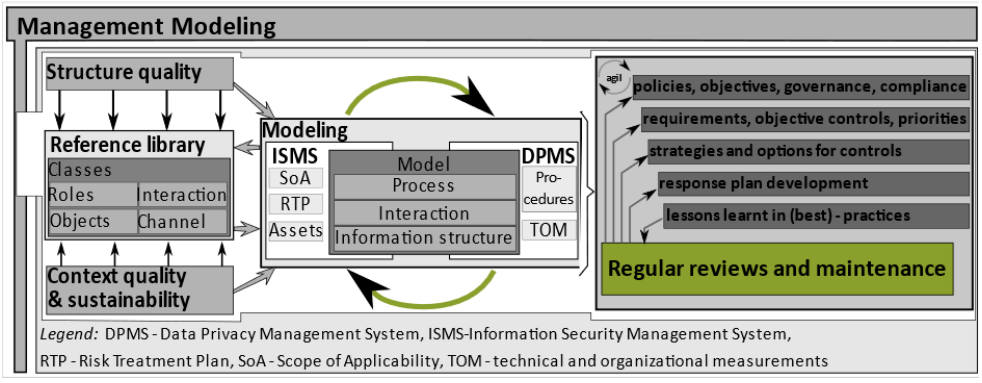

Figure 2 - Management modelling related security, privacy, quality and sustainability
Source: Authors, 2022.

Principle, every process map is an individual representation of the existing business processes of the respective organization, but there are some common rules for creating a process overview model for IS, CS, DP and quality. The determination of primary and support processes and representation as business processes (e.g. according to BPMN - Business Process Model and Notation) are relevant. In addition, the differentiation and separation of the main value-adding processes from management (control) and support processes is required.

Furthermore, the representation of the structural levels (management, main and support processes) and the inclusion of the interfaces and associated information attributes as well as delimitation of the interfaces to outsourced processes (e.g., third parties).

To answer the question - how are the processes and their delimitation defined, the simple consideration and subdivision of the business processes as primary processes, that make a direct, value-adding contribution to the creation of a product or service and the support processes: which are the necessary prerequisites for carrying out the primary activities. This makes it possible to classify the business processes in process types and to determine the sources of differentiation compared to competitors as well as cost advantages in the organization. In addition, the associated information and measures can be categorized and consolidated in groups and prioritized. The process types can be formally described as follows:

- Management process, specifies the overall strategic direction of an organization and includes all strategic and operational planning, steering and controlling activities for their optimal alignment. That means e.g. the process of continuous improvement is therefore assigned to the management processes.
- Main (core) process, constitutes the “added value” of the organization and is perceived by the stakeholders. Optimally configured value creation processes make up the individuality, profitability and thus also the competitiveness of an organization.
- Support process only contributes indirectly to added value. These are essential to deliver value and ensure high quality fulfilment. External business partners, who also belong to the group of stakeholders, are least aware of the supporting activities. Support processes with defined core processes are often in an internal performance relationship to be provided. Another objective is to continuously improve the level of management for IS, CS, DP, quality and sustainability required for operations. The systematic examination of risks, weak points and threats is to be seen as an essential part. In addition, regular reviews of the business processes ultimately serve to evaluate potential changes with consequences, risks or opportunities in order to establish targeted technical and organizational measures and to proactively avoid threats. A constant analysis of the organizational development regarding IS, CS, DP, quality and sustainability and the risks leads to an improvement and optimization of the measures used as well as the management key figures (KPI - Key Performance Indicator). The points of contact and demarcations to the business processes and the responsibilities are shown and the exact requirements are described by the existing complete and concrete guidelines/standards, which apply as procedural, service or work instructions within the organization. The regulations on the allocation of responsibilities oblige those responsible in the organization to comply with the guiding principles of IS, CS, DP, quality and sustainability and, if necessary, to make additional decisions and agreements. In addition, the measures used can be answered in as much detail as possible by the processors in order to be able to use the information obtained as so-called best practices in a solution-oriented manner throughout the company.

4. Modelled disciplines in context of IS, CS, DP, quality and sustainability

The dynamic development of the business fields and organizational structures of companies require a combined use of management systems and associated agile teams that organize themselves and can adapt to individual needs. As a result, management systems and topic-oriented operational teams to IS, CS, DP, quality and sustainability form the basis for the targeted operationalization of comprehensive protection of business processes and information values across all supporting values within the company or a Scope of Applicability (SoA).

This offers aim-oriented customization options for specific needs such as security, quality and sustainability, which identifies and evaluates risks and weak points. A "one-size-fits-all" principle is only partially effective, as there are different security requirements for the various business areas in the company (Lampe et. Al., 2021). The Figure 3 below shows the defined security disciplines from the reference library, which in their total sum up all the requirements for the ISMS, CSMS, DPMS and their series of standards (ISO/IEC-27001, ISO/IEC-27002, ISO/IEC 27701, ISO/ cover IEC 9001). For example, to achieve the aims for information security and data protection, a security organization must be implemented within the company. The operationally active security organization is formed by the information security officer (ISO), the data protection officer (DPO) and those responsible from the departments who promote the further development of overarching protection of business processes and information values. Those responsible can contribute to sustainability in comparison with the design of measures. The ISMS and the DPMS combine a wide range of technical and organizational measures as well as special security processes or individual security-relevant process steps within existing company processes. The security aspects are an integral part of a large number of different IT service managed processes, such as event, incident or change management, which are controlled and coordinated by the ISO and DPO. All technical and organizational security measures as well as the procedural consideration of security aspects are bundled, categorized and viewed as so-called security disciplines within the reference library. If this is related to the information objects to be exchanged using information structure models from

ISMS, CSMS, DPMS, QMS in combination with sustainability, their elements can be defined by classes with roles, objects, interactions and channels.

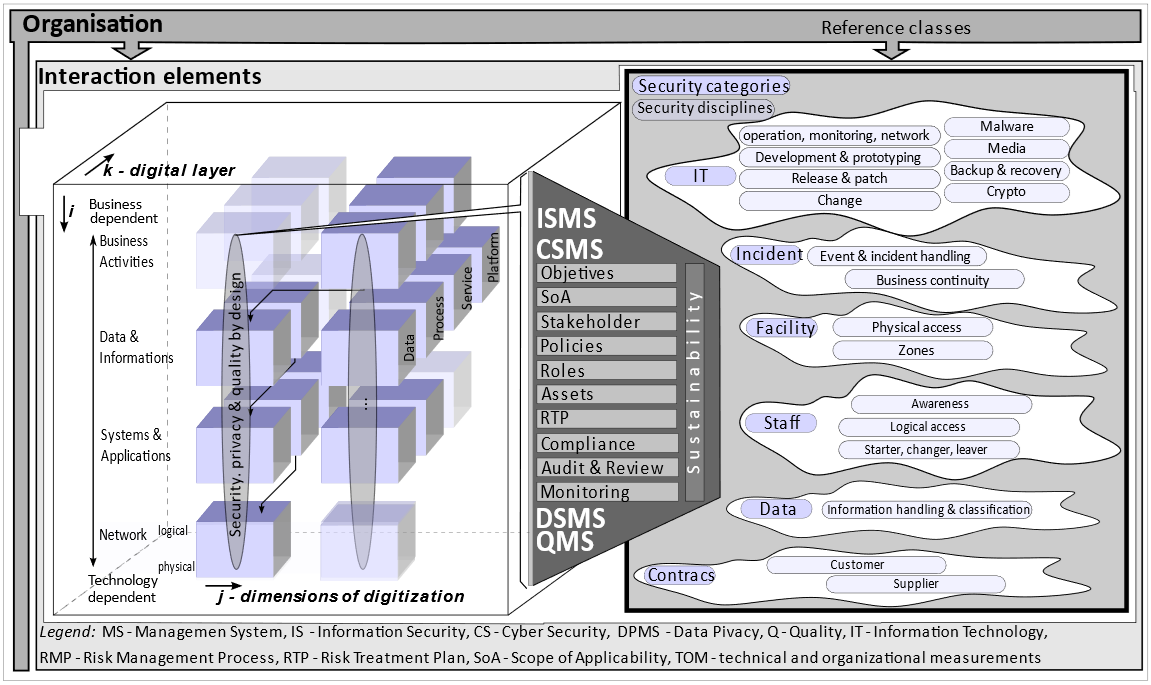

Figure 3 - Modelled interaction elements related ISMS, CSMS, DPMS, QMS in context of sustainability
Source: Authors, 2022.

By defining the dependencies of the elements and information objects, they can be categorized. The information security processes are to be clearly defined and the areas of responsibility of those responsible from the security organization are to be divided into strategic and operational information security. A total of 18 comprehensive security disciplines are defined for the ISMS, which must be established in a process-oriented, aim-oriented manner in order to control the measures of the individual disciplines effectively, efficiently and sustainable.

V. CONCLUSION

Through the combined presentation of the various management systems (IS, CS, DP, quality) with reference to the protection objectives and the most important standards as well as legal requirements, the essential dependencies could be shown. This makes it possible to derive specific requirements and to adapt for the technical and organizational measures and to measure their implementation more objectively for aim-oriented security and sustainability.

The central focus here is on the ISMS, which is intended to guarantee the various protection objectives of information, applications and IT systems and is part of the general Risk Management (RM). With the creation of the structured and classified process overview model with the significant interactions of the process under consideration for IS, CS and DP, the application of object-oriented mechanisms is made possible and can be designed flexibly. This extension creates added value for the company, since essential information exchange processes for the organizational and technical adjustment processes show and shape the direction of agile and partially automated information and cyber security as well as data protection.

The effects of risks on business processes can vary within a company branch. If protective measures for the information to be protected are based on the organizational and technical RMP approach for information security, then the structured policy system can be applied procedurally. This results in a reproducibility of the partial results for the risk assessment and treatment. Based on RMP steps can support risk assessment, management and response as well as reporting within business units. The increasing consultation of those responsible causes a conditioning of those involved by addressing the risks. This leads to an improvement in risk measurement and analysis methods by those responsible.

The establishment of a committee of responsible persons leads to a coordinated communication exchange, which addresses the cyclical activities for planning, implementation and improvement of the management systems for IS, CS and DP. The security aspects are an integral part of a large number of different IT service

processes. All measures (technical, organizational) are bundled within the reference library, categorized and considered as so-called security disciplines. These individual security disciplines can be used effectively and efficiently and managed sustainably. A consistent structure enables the provision of protective measures for critical and non-critical information resources, in which the technologies can optimally meet the security requirements and complement each other.

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. The further approach to data collection and evaluation of the effects of the risks in combination with the risk awareness for IS, CS and DP of other company branches is recommended in order to create the possibility of a branch index.

VI. REFERENCES

1. 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.
2. Bakator, M.; Đord¯evic´, D.; C´ oc´kalo, D. *Developing a model for improving business and competitiveness of domestic enterprises*. J. Eng. Manag. Comp. 2019, 2, 87–96.
3. 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.
4. Carpenter, V.L. and Feroz, E.H., 2001. *Institutional theory and accounting rule choice: an analysis of four US state governments' decisions to adopt generally accepted accounting principles.* Accounting, Organizations and Society, 26, pp.565-96.
5. Cho, C.S., Chung, W.H. and Kuo, S.Y., 2016. *Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants.* IEEE Transactions on Systems, Man, and Cybernetics: Systems, 46(3), pp.356–369.
6. 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.
7. Da Veiga, A. and Eloff, J.H.P., 2010. *A framework and assessment instrument for information security culture.* Computers & Security, 29(2), pp.196-207.
8. Fogoroș, T.E., Olaru, M., Bitan, G.E., and Dijmărescu, E., 2021. *The Risks of Agile 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.
9. 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.
10. 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.
11. Grigorescu, A. & Mocanu Niculae, A. (2020). *Teleworking perspectives for Romanian SMEs after the COVID-19 pandemic.* Management Dynamics in the Knowledge Economy, 8(4), 383-399, doi: 10.2478/mdke-2020-0025.
12. Järveläinen, J., 2012. *Information security and business continuity management in interorganizational IT relationships.* Information Management & Computer Security, 20(5), pp.332–349.
13. 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.
14. 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.
15. 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. 911-919. DOI: 10.24818/BASIQ/2022/08/098
16. 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.
17. 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.
18. 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.
19. 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.
20. Popescu, L.; Iancu, A.; Avram, M.; Avram, D.; Popescu, V. *The Role of Managerial Skills in the Sustainable Development of SMEs in Mehedinti County, Romania.* Sustainability 2020, 12, 1119.
21. 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.
22. 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.