BUCHAREST UNIVERSITY OF ECONOMIC STUDIES
Business Administration Doctoral School

PhD THESIS

Presented and defenced publicly by author:

GEORG SVEN LAMPE

Title of the PhD-Thesis:

RESEARCH ON INFORMATION SECURITY IN BUSINESS PROCESSES RELATED TO GLOBAL RISKS

Scientific supervisor: Prof. Univ. Dr. Marieta Olaru

Defence Committee of the PhD-Thesis:

Prof. Univ. Dr. Cristinel Vasiliu (president) - The Bucharest University of Economic Studies
Prof. Univ. Dr. Liliana Nicodim (referent) - The Ovidius University, Constanța
Prof. Univ. Dr. Elena Cerasela Spătariu (referent) - The Ovidius University, Constanța
Crof. Univ. Dr. Mihaela Maftei (referent) - The Bucharest University of Economic Studies
Prof. Univ. Dr. Marieta Olaru (scientific supervisor) - The Bucharest University of Economic Studies

Bucharest, 2024

a) Content

TABLE OF CONTENTS

b) Keywords

Management System Standards, ISO norms, Integrated Management System, Performance, Evaluation, Risk Management, Information Security, Cyber Security, Business Continuity, Sustainability, Agility, Business Processes, Agile Methodology, Enterprise Risk Management, Organizational Effectiveness and Efficiency, Performance Management, Leadership, Knowledge Management, Model Development, holistic solutions.

c) Summary

This dissertation examines the problems of evaluating integrated and non-integrated management systems in the context of corporate business processes for information and cyber security, business continuity, sustainability and risk management. Based on a literature review, the author evaluated the current trends and known findings in this research field and conducted his own empirical studies over the last five years. The focus of these studies was on several areas that are closely related to the research topic. One aspect is the performance of the organization, including measuring criteria of established business processes and measured methods for multidimensional approaches, which also include the strengthening of the dimensions of information and cyber security, business continuity and sustainability required by the EU. Other aspects are their link with risk management and the success factors of management systems. The risk management concepts offer practical solutions for company-wide management systems and their measurement.

Another focus is the importance and linking of strategic and technological criteria for strengthening management systems and their top management. In this dissertation, the author places particular emphasis on problems in this research area that he has identified during many audits of established management systems that he has conducted and the evaluation of the solutions used.

With developing a model for evaluating integrated and non-integrated management systems, considering the given context criteria, the focus was on the applicability of the results for strategic, organizational and technological use and their dependencies. The model includes the use of an adapted failure mode and effects analysis with an extended and agile methodology linked to a strategic mapping process and the Plan-Do-Check-Act cycle of management systems. Furthermore, it represents an approach for scientists, consultants and practitioners to further deepen, review and test the existing understanding and experience of related topics in an aim-oriented manner.

The aim of this work was to develop an adapted information model of risks and opportunities that combines the business processes, information objects, supporting assets, threats) for cluster analysis, which demonstrates the integrated approach of organizations to risk assessment with multiple criteria in the areas of energy supply and generation companies and information and telecommunications companies. This model can be applied both to different management systems and to achieve an increase in the efficiency of the risk management process (RMP).

The author based his work on various research methods, the first methodology involving a literature review in the relevant areas. From the identification of the current state of knowledge and existing research gaps, the author derived problems, existing approaches and solutions. The author of this work has also carried out personal scientific studies to identify important aspects for this work, which are also based on the knowledge and insights gained in years of practical experience. In this context, the first step was to analyse the current approaches to global risks in information security in the context of business continuity management, the continuous improvement of information security and the definition of an information security management system in the context of business continuity management. The author is intensively involved in the implementation, development and evaluation of integrated and non-integrated management systems with various companies in critical and non-critical sectors. He is very interested in gaining knowledge because it is primarily about continuously improving existing knowledge for practice and for the scientific community. With this research, the author intends to solve an important aspect of his daily work, namely the assessment of risks and their impact and the maturity level of integrated and non-integrated management systems used by organizations and their business processes worldwide.

A special focus was placed on and analysed the current approaches to global risks in information security in the context of business continuity management, the continuous improvement of information security and the definition of an information security management system in the context of business continuity management. This means defining, evaluating and achieving corporate goals that do not only meet the traditional goals. However, the financial value, which in the past was considered the most important aspect of organizations, must not be lost sight of, because this must also be achieved and reported to management. New insights are also being gained in this area in connection with sustainability.

A sustainable business process in the context of information security, cybersecurity and business continuity is not only a process based on an input of financial value, but also generates outputs in various other aspects. Some of these security aspects are part of establishing

measures in the sustainability concept, e.g. better results in terms of the ecological and social perspective.

Depending on the business area in the various sectors (energy, health, etc.), other elements may also be required for a performance assessment. For example, not only the creation of general and specific knowledge is required, but also the sharing of knowledge and knowledge transfer for the organizational culture. This is also part of the company's image to face up to society and its responsibilities internally and externally and to assume corporate social responsibility.

It is recognized that the assessment of risks and associated opportunities as a decision is partly carried out under uncertainty. In addition, the following text brings together the recent discussion on the extension of the existing risk management process (RMP) within BCM due to the epidemic/pandemic risk threat to the information security of critical infrastructure, managed utilities and telecommunications services and examines its impact on crisis management (CM) measures.

In addition, there are different perspectives on the importance of business processes and the information objects to be protected and the risks to be addressed that affect the supported asset. The performance, which depends on the stakeholders and various aspects (organizational, technical, technological, personnel, etc.), must also be taken into account when evaluating the performance of any management system. A performance evaluation of management systems is necessary because every system requires a continuous improvement process. This makes it possible to gain maturity over time. To achieve this initial goal, the methodology shown below was used in this work.

In the first part of this work, a literature review was conducted to examine the current scientific data in the field of performance assessment of management systems and business processes and risk management.

Chapter one deals with the literature review in this field to analyse current approaches related to global information security risks in the context of business continuity management, continuous improvement of information security and the definition of an information security management system in the context of business continuity management.

It begins by discussing the history, definition and current scientific status of information security in the context of global risks and business continuity and risk management.

The author identified various characteristics of organizations and roles, e.g. the need to operate in a changing environment or Scope of Applicability (SoA) with the need to adapt to these changing circumstances. This also includes the distributed digital activities ranging from

local, regional management and knowledge to global interaction and the global integration of security business and culture processes.

Risk management for the classic protection goals is described, which is an iterative process for listing, evaluating and treating risks. By identifying the causes of failure and quantifying the probability of occurrence, it is possible to determine risk priority numbers using a failure mode and effects analysis (FMEA) (ISO/IEC 31000) and the risk matrix.

By identifying the causes of failure and quantifying the probability of occurrence, it is possible to determine risk priority numbers using a failure mode and effects analysis (FMEA) (ISO/IEC 31000) and the risk matrix. In addition, the application of the BIA/RIA process is also taken up in order to identify safety-relevant information from authorities and associations, warnings and safety incidents that influence the results of risk treatment. BCM is a holistic management process that enables companies to deliver critical services and/or products at an acceptable, predefined level after an incident in order to minimize the damage. Related BC strategies are included in the analysis to determine an acceptable minimum level and a sustainable level of operation.

In the second study, performance evaluation is explained in more detail, as it plays an important role for organizations. The basic definition here means that the performance of an organization is measured by the ability to complete all the tasks required to achieve its organizational and financial goals. Both internal and external influencing factors must be taken into account when evaluating performance. Process orientation is a mandatory aspect of BPM. The ability to change as quickly as necessary is a basic requirement of today's companies and therefore an important aspect within an evaluation process of a management system for performance measurement, which is explained in more detail.

In the third analysis, agile methods are taken up, as they have gained popularity in recent years, with a focus on flexibility and adaptability in project management, such as SCRUM. This is also taken up in the analysis, because in today's dynamic business environment, agility and appropriate responsiveness are of great importance.

In Chapter 2, aspects of risk management were examined as an essential part of an organization to be prepared for visible and invisible events within digitalization. In the current digital business landscape, characterized by a very VUCA environment, companies are facing unprecedented challenges that require a new approach to organizational structure and leadership.

In addition to classic risk management, which is based on the fundamentals of risk management and risk management methodology (e.g., incorporating the approaches of risk identification, risk measurement, risk monitoring, risk mitigation, etc.), a discussion of

traditional risk management according to COSO ERM, ISO 31000 and ISO/IEC27001 is conducted to provide a basis for a better understanding of the framework.

This study highlights the importance of considering risk factors, computing power and multi-criteria decision-making processes to improve overall performance and results in the context of risk management. Through further analysis, the importance of measuring the effectiveness and efficiency of risk management practices is highlighted, especially in relation to Key Performance Indicators (KPIs). By using frameworks, methods and tools such as RMI, internal control mechanisms, companies can improve their risk management strategies and achieve better results in different sectors. This also means that assessing the maturity of risk management is an important method to improve risk management and adapt it to the strategic and operational objectives of the company.

In the literature review of chapter 3, the relationship between business processes and the influence of information security and business continuity requirements (e.g. based on the Plan-Do-Check-Act cycle) is highlighted by the author, because this is an essential aspect of organizational management. Therefore, the most relevant management systems are listed and the high-level structure is examined in more detail in order to identify the organizational trends, analyse them in more detail and show the difference to a Harmonized Structure. This involves a thorough examination of the MS in its entirety and in all its aspects at the respective company locations.

In order for management systems to develop their full effect and lead to the desired results, the interaction of various success factors is crucial, which are specified in the following study. In addition to structural and procedural aspects, the factors of leadership and commitment to employees and the organizational culture play an important role. The aspects with the factors such as transparency, trust and a culture of continuous improvement are important keywords here and form the basis for a functioning management system. Depending on the protection requirements implemented, these can be divided into independent, classified measures, groups or maturity levels according to Capability Maturity Model Integration (CMMI). The author therefore suggests analysing the CMMI principle and the application for recording and measuring CMS system maturity.

The third analysis specifies that efficient and reliable business processes (BP) are essential in relation to the information to be protected (Information Objects – IO) and their information and communication technology (ICT)-supported systems/services (Supporting Assets – SA). Only in this way can the company's complex operational challenges be overcome. This also includes certification according to the internationally recognized standard for

information security management systems according to ISO/IEC 27001 in all industries with critical and non-critical infrastructure.

The part II of this paper is the personal contribution of the author of this paper to the field of study. It contains empirical studies that extend the results of other studies mentioned in part I to derive an evaluation model.

In Chapter 4, the author analysed the relationship between business processes and the intellectual knowledge level in the context of the processes to be secured and the associated maturity level of the company's performance to be secured, in order to demonstrate the importance of integrating security requirements for the impact of performance. The aim of the research was to identify possible relationships between defined goals, their nature and the reported organizational performance.

The first study focused on the performance measurement of several external audits in four organizations that provide IT managed services to their customers. The authors checked the level of compliance with the service management system described in the ISO/IEC 20000-1 requirements standard. The focus is on the integration of security requirements based on a risk analysis into the IT services provided. Shifting the focus to meeting the key performance indicators from the service level agreements can help IT service providers, among other things, to avoid security incidents, but it can jeopardize contractual obligations with customers.

When adjusting the security level and measures for the IT services provided, specific aspects should be taken into account, such as critical assets and services that need to be secured. The authors of this study conclude that there is a clear connection between information security and service management. It is also emphasized that the two concepts can be successfully integrated. If implemented well, information security has a positive effect on service management. In addition, it was recognized that the introduction of an integrated information security management system can help the IT service provider to address the specific security measures in much more detail. This confirms the approach to an integrated management system.

In the further analysis, the topics of researching the dependencies of information security management in relation to business continuity and characterizing the impact on the business in the context of the global crisis were taken up. It is specified that the ISMS can achieve many protection goals that ensure information integrity within an organization. In addition, business continuity, together with the associated additions to controls and control objectives, can be well mapped in a general management framework. Additions must be taken into account that address specific topics such as policy, organization, personnel, inventory, IT operations and IT communication as well as business continuity management from an ISMS perspective. If an ISO 27001-compliant system already exists, it can build on its results and the

expansion towards BCM creates added value for the organization. This means that essential management procedures are tried and tested.

It is confirmed that the security threats from cyber-attacks in intelligent automation and digitalization structures are increasing and the likelihood of serious disruptions such as epidemics / pandemics is increasing. Therefore, continuous development of information security management and information security risks during digital transformation is necessary. Only in this way can the occurrence of global serious influences be identified more efficiently and associated disruptions in business process and business continuity management be minimized.

The third research analysed the strategic potential for managing an independent maturity model in connection with the digitalization of processes while complying with the protection goals for information security and data protection. In this context, a conceptual approach for the multi-stage digitalization stages was developed to show that the creation of modelled processes is an important step in the automation of standard processes. This extension shows the direction of an agile information and cybersecurity organization and creates added value for the organizations.

This creates the opportunity to try out and test the essential business processes. By comparing with the SCRUM-specific elements, focused and secure operations for information and cyber security requirements are established. The risk management process is no longer based on a one-time risk assessment and static threat catalogues, but the organizational and technical processes adapt to the security requirements and continuously evolve. Consequently, risk assessment assessments are derived in a more agile manner and implemented in a sufficiently detailed and agile manner. Therefore, company-wide efforts must be made to protect critical data, IT networks, applications (software) and associated systems as part of the integrated management system.

The proposed model was evaluated using a case study approach within the consultancy. It can be concluded that the proposed model can be practically used for an assessment of the risk management of companies.

The conclusion of the last part of the fourth chapter showed that modern management approaches such as agile principles of the value-added industry are beneficial for the efficiency and effectiveness of organizations. This underlines the importance of rapid adaptation in a rapidly changing market and the importance of these operational principles and tactics as influencing factors for performance.

Chapter 5 deals with research in the field of information security management systems and the influence on the performance of business processes through associated frameworks in

order to enable classified measures and to identify the critical success factors in the context of sustainability and managed services.

For the area of ICT-supported processes, the ISO/IEC 27005-based requirements are used to assess the need for protection for the supporting assets. A need for protection is an inheritable asset of the information objects to be protected that are used for transactions and related business processes. Information objects are assigned to places of use and service providers. Threat catalogues are created based on the damage potential of the processed information. The protection requirement is calculated according to the maximum principle. For this purpose, an organizational, process-oriented and legal framework was analysed that defines the management of information security and data protection in the context of digitalization and at the same time meets the various protection goals.

In the second part of the research, it was shown that by considering the protection goals, it is possible to implement an agile method and develop an adapted risk matrix based on the Failure Mode Effect Analysis (FMEA). As a result, the organizational requirements of the ISMS could be examined within the framework of an organizational and process-oriented framework.

In addition, it was confirmed that the ISMS plays a central role for critical and non-critical infrastructures. As part of the analysis, it was found that the ISMS can be expanded by integrating information security management processes. As a result, measures could be classified, combined and improved, which ultimately affects the level of maturity.

By adapting the process and specifying a specific cyber risk register, it was shown that proactive management of cyber security risks is possible. This leads to improved implementation of management activities, which increases the efficiency of the risk management process (RMP).

In this context, a process interaction model was developed that can be used as an industry-independent maturity model for assessing business processes for the actors. The model contains several dimensions that operationalize the processes within the process level through the assessed risk criteria for quality, data security and data protection and provide the corresponding process transparency for all those involved.

The third part of the research deals with the dependencies of the existing management requirements and information objects to be protected in the organizations, which are specified by the protection objectives. The associated information security processes must be clearly defined so that they can be divided or categorized into strategic and operational information security in the areas of responsibility of those responsible in the security organization.

The process-oriented categories are individual disciplines that are set up and categorized in a goal-oriented manner in order to manage them effectively, efficiently and sustainably. This requires the adaptation of management activities, which leads to secure and sustainable measures through the categorization of information and group-specific consolidation and prioritization. Increasing the efficiency of the risk management process (RMP) is not only possible but is foreseeable through group-related consolidation and the prioritization of measures.

Chapter 6 deals with the development of measurement models and assessment of integrated and non-integrated management systems in different sectors. This was done as a result of studies carried out within the framework of the doctoral program. This was achieved by supplementing the results of the studies mentioned in the previous chapters with additional personal research results and then working out possible solutions to the problems discovered.

The author is personally involved in a number of management system audits of integrated and non-integrated management systems in different sectors and therefore has valuable data that can be used to deepen this topic. The results of the quantitative analysis showed that in certain areas there are more non-conformities and recommendations with the requirements for management systems than in others.

The first research part highlights the problems in the implementation and application of information security management systems based on the author's professional experience in consulting and auditing management systems. It begins with the presentation of studies that include important dependencies and reasons and focus on key criteria in critical and non-critical infrastructures for this research. This is based on an empirical analysis resulting from the results of external audits carried out by the N3I auditor (neutral, independent, impartial, integrity) and the resulting audit findings.

The audits carried out demonstrate the targeted conformity checks of organizational, technical, personnel and physical measures. The certification process carried out by the auditor or team of auditors is documented in accordance with the normative requirements. If there are deviations from the standard conformity, this is specified and verifiably recorded as a finding. The aim of these recommendations is to optimize the efficiency, effectiveness and conformity of the management system with the relevant standards and best practices.

In addition, the current EU requirements for the new EU directives on measures for a high common level of cybersecurity are addressed and explained in more detail. The strategic potential for sustainable compliance management of legal and regulatory requirements for a fulfilling requirement and risk culture of critical and non-critical services is also discussed.

In the third part, the author develops an evaluation and classification system based on failure mode and effects analysis to evaluate the performance of management systems in the context of information security and business continuity management and verifies it for practical use.

In summary, the research work contained in this dissertation highlights the following fundamental points:

- Complexity of performance evaluation: The performance evaluation of management systems is a challenge for both practice and research. This is mainly due to an inconsistent understanding of the concept of performance and a lack of standardized methods.
- Multidimensional understanding of performance: The performance of organizations is often reduced to financial indicators. The dissertation advocates a more comprehensive understanding of performance that includes other dimensions such as operational excellence, process efficiency and effectiveness.
- Diverse evaluation methods: Various models and methods for multidimensional performance evaluation exist. A promising approach is the combination of the FMEA methodology with agile processes such as SCRUM. SCRUM was originally developed for software development but can be adapted for holistic performance evaluation by integrating sustainability and risk management perspectives.
- Success factors for integration and operation: The successful implementation and certification of management systems depends largely on four factors: management commitment, appropriate leadership styles, suitable evaluation methods and a continuous improvement process.

The dissertation thus provides valuable insights for practice and research in order to capture and optimize the performance of management systems in a more holistic manner. The model developed by the author proposes to evaluate performance based on indicators of various dimensions.

In addition to the identified indicators arising from the topics of information and cyber security, business continuity and sustainability, the efficiency and effectiveness of operational and strategic processes is a compelling perspective that must be evaluated. In this context, the aspects that are relevant to a specific management system topic and to the company's industry-specific goals must also be taken into account.

The models also included the measurement of maturity levels, including the generic performance of integrated and non-integrated management systems.

The final step was the verification of the proposed model using a quantitative analysis based on internal audits and related interviews. In this way, the author evaluated and compared approaches and methods, such as the proposed evaluation model.

The results showed that the proposed BIST model is a valid method for evaluating the performance of management systems in companies, in particular due to the following points:

1. The model connects the evaluation of the tested integrated management systems in different sectors with the strategic objective, as it can be used to test the promising agile approach, combining the FMEA methodology with agile processes such as SCRUM, and using the agile methodology to report the results of the evaluations in an aggregated manner to top management.
2. The model is linked to the development of operational business processes based on the defined strategy of the organization.
3. The model can be used to measure values from all relevant dimensions, including the methods and KPIs used, sustainability and the assessment of the risk management of companies. The BIST model proposes well-known and established methods.

With this knowledge, it can be concluded that the proposed model identifies and solves concrete problems discovered by other authors and scientists during the daily work and scientific research of the author of the doctoral thesis. By applying different research approaches, a holistic measurement framework for evaluating performance evaluations of the integrated management systems examined was derived and empirically tested in the research project. In this work, the strategic relevance of integrated management systems and their evaluation was identified, since management systems combine a variety of topics from the operational to the strategic level.

d) Curriculum Vitae

PERSONAL INFORMATION

LAMPE, Georg Sven

Kerkower Dorfstraße 47, 16278 Angermünde, Germany

+49 173 866 49 15

lampe@compliance-docs-group.com

Sex Male | Date of birth 30.07.1976 | Nationality German

I am highly motivated engineer on the one hand with several years of experience in the energy and telecommunications sectors and on the other hand with excellent organizational abilities and strategic as well as business thinking skills.

I am accustomed in the complex project through my experience to focus directing and orderly resolution the company strategies, efficiently organize, implement and develop targeted. Through my professional and personal leadership skills I am used to make independent decisions as well as to act team-oriented and to behaviour entrepreneurial.

I am conscience team worker who enjoys taking initiative and can work very effectively on my own.

I am very interested in studying new performance improvement for management systems compared with an implementing integrated management system (quality, environment, security, social responsibility) for a better understanding of new organizational and strategic business communication systems.

I am a very fast learner who welcome new challenges and open to new experience.

PROFESSIONAL EXPERIENCE

Oct 2021 – current

Chief Executive Officer (CEO), Manager, Team Lead Project Management

Compliance Docs Group Verwaltungs GmbH, Angermünde

- ISO 27001 Certification Auditor / Partner of TÜV Süd Management Services
- Status: Auditor with Audit performance since 10.2015: approx. 350 d
- Focus: Information Security
- Planning and implementation of transnational certification projects with multiple standards and coordination of international teams
- Consolidation of the results of the audit teams, comparison with the business case, strategy & risks as well as presentation to SMEs and corporations
- Author and co-author: various international conferences in the field of information security, cybersecurity and data protection, BMC, etc.
- Business Unit Supply and Telecommunications Networks (E/TK/LST) for ITIL / ISO 20000, ISO 27001 Information Security, ISO 27019 Critical Infrastructures, (B3S), ISO 22301 Business Continuity, ISO 50001 Energy, ISO 9001 Quality, General Data Protection Regulation, Economic Risk MMS
- National IT Service Mgmt. Projects and SOC
- Digitization Officer
- Implementation of information security processes (ISO 27001 ff.)
- Preparation of risk analysis, emergency planning & disaster recovery concept
- Implementation and optimization of operational IT processes to increase efficiency
- Measures to improve processes and increase maturity
- ITIL Process Modeling for Data Center and Application Management, etc.
- Synchronization with software, engineering and support teams at Singapore and Malta/N.Y. sites
- Coordination, management of an offshore supplier team with 30+ members
- Supplier contract management, annual budget planning

Business or sector Information Technology, Consulting

Oct 2021 – current

Chief Executive Officer (CEO)

Compliance Docs Group GmbH & Co. KG, Angermünde

- Founder mentality with an extremely high level of customer orientation
- Experience in the establishment/development of new business activities, e.g. in the IT industry environment with a strong creative will for information and cyber security, data protection, quality, etc. with an unconditional focus on success and goals as well as visionary thinking
- Experience in successfully setting up a multinational B2B/B2C distribution (analogue and digital)
- Extensive IT technical understanding (architecture, conception, implementation, etc.)
- Responsibility for the complete strategic, organizational and technical alignment and project execution using the business strategic project management methods and process coordination according to ITIL, PMboK in comparison with BSI, ISO/IEC 27001, ISO/IEC 27019, ISO 9001, ISO/IEC 27701, ISO/IEC 50001, ISO/IEC 55001, Smart Market, etc.
- Responsibility for the operational business (planning, development and implementation) in compliance with legislation as well as internal regulations and guidelines
- Establishment of sales channels; Customer service; Public relations and representation obligations as well as regular reporting to the shareholders
- Establishing the capital market readiness of companies
- Coordination of connected trades up to the drafting of contracts for the entire external company management
- Responsibility for all business and technical topics as well as assumption of the entire budget responsibility
- Development/implementation and responsibility of measures for legal framework conditions and requirements in the energy industry, e.g. Technical basics of electricity and gas supply, basics for grid operation, network control and dispatching, IT-critical infrastructures for grid operation, scope of the ISMS according to IT security catalog § 11 para. 1a EnWG
- Development/implementation and responsibility of measures for legal framework conditions and relevant regulations for the energy industry (esp. unbundling) as well as electricity generation and gas production (hydrogen project – hybrid power plant), technical expertise in generation, basics of plant operation and plant control, technical expertise on the various energy plant categories and their special features, critical IT infrastructures for plant operation – scope of the ISMS according to IT security catalogue § 11 para. 1b EnWG
- Manager for a team of software engineers developing solutions for factory control systems around IBM SiView MES and Equipment Interfaces
- Responsible for target setting dialogues, annual performance reviews, resource planning, job interviews, organization of team building events
- Synchronization with software, engineering and support teams at Singapore and Malta/N.Y. sites
- Coordination, management of an offshore supplier team with 30+ members

Supplier contract management, annual budget planning

Business or sector Consulting and Auditing

Jan 2020 – Nov 2022

Lead Manager for Management Systems, Managing Partner

Stadtwerke Schwedt, Schwedt/Oder

- Head of Digitalization and Management Systems in the Supply and Telecommunications Networks Division (E/TK/LST) in the organizational unit
- Responsibility for the complete strategic, organizational, technical and budgetary handling of digitization projects and IT services using the project management methods ITIL, PMboK, Scrum
- Responsibility for the design, implementation and operation of security operation of power control for electricity, gas and district heating in compliance with legislation as well as internal regulations and guidelines (ISO/IEC 27001 Information Security, ISO/IEC 27019 Critical Infrastructures (B3S), ISO/IEC 22301 Business Continuity, ISO/IEC 50001 Energy, ISO 9001 Quality, General Data Protection Regulation) until their business process design and establishment of the service operation level (SLA, OLA) from incident handling (operational disruptions, security incidents, emergencies/crises)
- Development, implementation and responsibility for measures on the legal framework and requirements of grid-bound energy supply in the energy industry, e.g. Technical expertise in electricity and gas supply, grid operation, grid control and dispatching, IT-critical infrastructures for grid operation, scope of the ISMS according to the IT security catalogue §§ 11 para. 1a
- Responsibility for the preparation of recommendations for action and coordination of related trades up to the drafting of contracts for IT security and requirements management as well as IT Business strategic process coordination with the top management and the department heads
- Guidance (personnel, professional) up to 5 employees

Business or sector Energy Consumption and Production, Renewable Energy, Technology, Consulting

March 2017 – current

Chief Executive Officer (CEO)

Bürgerwind Schönfeld GmbH & Co. KG, Kerkow

- business area for renewable energies and responsibility for the entire organizational management including development of appropriate business processes under using the project management methodologies ITIL, PMBOK as well as quality-, security and data privacy management
- coordination trades up to the drafting of contracts
- Manager (quality, security) and leader (IT groups & projects) in business system as well as service development (tele-/data communication)/energy data management
- Responsibility for the entire organizational and technical project management including development of appropriate business processes and data interfaces using the project management methodologies ITIL, PMBOK, Scrum
- Planning, development and implementation of renewable energy system with specification via business and interface adjustment, request and order management, coordination trades up to the drafting of contracts
- Instructions (technically, personnel) up to 5 employees and trainee
- Certification lead auditor as partner of TÜV Süd Management Service GmbH, DEKRA
- Consulting services for information security audits (ISO27001, BSIG §8a, IT-SiKat), TISAX VDA-ISA, ISMS
- Project Management (Software, Automation, ITSM), Scrum Master

Business or sector Renewable Energy, Technology, Consulting

May 2009 – current

Lead Manager for Management Systems, Managing Partner

ENERTRAG AG, Dauerthal/Berlin

- Manager (quality, security) and leader (IT groups & projects) in business system as well as service development (tele-/data communication)/energy data management
- Responsibility for the entire organizational and technical project management including development of appropriate business processes and data interfaces using the project management methodologies ITIL, PMBOK, Scrum
- Planning, development and implementation of renewable energy system with specification via business and interface adjustment, request and order management, coordination trades up to the drafting of contracts
- Strategy/Processes BSI, IT Security, Data Protection, Cybersecurity, Quality, ITIL and B3S
- international IT service mgt. projects as well as based on SOC
- Control of operational IT service management processes and operations (international SLA, OLA for major customers)
- Management of the crisis team for IT and NON-IT of all sales lines for the power control of renewable energies (up to 8 GW)
- Project management in international IT projects (France, etc,)
- Development/implementation of risk management system (ISO 31000, ISO 27005)
- Trainer of internal auditors
- Instructions (technically, personnel) up to 5 employees and trainee
- Certification lead auditor as partner of TÜV Süd Management Service GmbH, DEKRA
- Consulting services for information security audits (ISO27001, BSIG §8a, IT-SiKat), TISAX VDA-ISA, ISMS
- Project Management (Software, Automation, ITSM), Scrum Master
- Process consulting, trainings, interim management

Business or sector Renewable Energy, Information Technology, Consulting

EDUCATION

2019 – 2024

PhD Studies at

The Bucharest University of Economic Studies, Bucharest

Research on Information Security in Business Processes related to Global Risks

Keywords:

Management System Standards, ISO norms, Integrated Management System, Performance, Evaluation, Risk Management, Information Security, Cyber Security, Business Continuity,

Sustainability, Agility, Business Processes, Agile Methodology, Enterprise Risk Management, Organizational Effectiveness and Efficiency, Performance Management, Leadership, Knowledge Management, Model Development, holistic solutions

2011 – 2014 **Studies at Hochschule für Telekommunikation Leipzig der Deutsche Telekom**

University of Telecommunications Leipzig, Germany,

Master of Engineering the field of Information and Communication Technology

occupational studies: IT-security, internetworking, IT-Law and business administration, project management (PMBOK, Scrum)

2003 – 2007 **Studies at Hochschule für Telekommunikation Leipzig der Deutsche Telekom**

University of Telecommunications Leipzig, Germany

Diploma - telecommunication engineering in the field of Electronic Science and Telecommunication Engineering

Priorities: IT Business Account Management including Marketing, project management

2000 – 2003 **Gymnasium (grammar school)**

Schwedt, Germany

Part-time completion of the university entrance qualification

2001 – 2003 **Apprenticeship as an IT systems electronics technician in Angermünde**

Schwedt, Germany

Part-time completion of the university entrance qualification

1983 – 1993 **Polytechnische Oberschule (elementary/secondary level school)**

Greiffenberg, Germany

with entitlement to attend the upper secondary school

TRAINING

2018 PMP, Project Management Professional (PMI)
2017 Certified Information Security Auditor acc. ISO 27001 (TÜV Süd), DEKRA
2016 PRINCE2 Foundation (Axelos)
2016 Professional Scrum Master (Scrum.org)
2006 ITIL V2 Foundation (HFTL)

PERSONAL SKILLS

Mother tongue(s): German

Other language(s)	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C1	C1	C1	C1	C1

Social skills and competences

- professional with more than 20 years of experience as manager, project lead and expert in different roles and industries
- Project realization from the point of business and risk process management
- (Planning, support, development, project planning, evaluation, regulatory framework - guidelines,

standards, regulations)
- Deploying applications systems, - function or - solutions
- Participation in all sales and technical decision-making processes and phases
- Execution of employee appraisals including determination of tasks and goals as well as assessment of the achievements, strengths, weaknesses of the employee
- Motivation of the employees by visualizing needs and showing ways in combination with the dosed setting of incentives (e.g responsibility allocation, process delegation)
- Supporting, accompanying and providing organizational and technical skills and competences using innovative training management

Organizational skills

- Leading international, distributed teams including offshore, nearshore models
- Acting as project management professional in classical or agile projects with technical or coordinating focus
- Working many years in environments with focus on development, design, and operation of high available 24/7 production systems
- Development recommendable services in the digital supply chain in compliance with the protection goals (confidentiality, integrity, availability, authenticity), building trusting relationships with customers or partners
- Analysis of the business and support processes (internal, external) as well as necessary measures including risk assessment for the safety and quality management in compliance with the data protection regulation
- Analysis of customer processes and measures

Projects:
• direct marketing and market premium regulation for renewable energies (Law- EEG),
• Measuring point service and meter operation (smart grid, smart meter and operations),
• certification according to ISO 27001 (information security management system), ISO 9001 (quality management system) and data protection management system
• planning, design according to standards / guidelines of complex system-on-chip, IT, safety and plant-specific projects based on ITIL services, PMBOK and Scrum,
• Wi-Fi/LAN networks, telecommunications solutions, development of software applications (OPC DA, OPC XML DA, SCADA systems, IEC 60870-5-101 and 104, DIN 61400-25), .Net

Tutor:
Responsibility in the area of power engineering and the area of Materials and Components
• Preparing and conducting courses for undergraduate students
• Coaching, Instruction and support of students in exercises

Membership of Student council:
• Responsibility of Unit technique and Sport

Computer skills

- Certifications in JAVA software development, Scrum, ServiceNow, ITIL, Information security & project management
- Know How inside whole Software Development Lifecycle
- Administration, Proficient user experience for several IT systems
- Technologies: Renewable energy, systems engineering, telecommunications, energy data management, application systems, simple / networked IT systems, security technology
- Programming languages: C#, C/C++, SPS, HTML, Assembler, JAVA; VHDL(Xilinx, Quartus), Eagle
- System, application and simulation software: in-depth knowledge in the architecture of each operating system (DOS, Windows) as well as application software Office and Databases, extensive knowledge of image editing with Adobe Photoshop, MatLab, LabView, PSpice

-

Date: 22.08.2024 ……

Signature: