https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-252

Measuring IT security, compliance and data governance within small and medium-sized IT enterprises

***Andreas Johannsen* [1]*, Daniel Kant* [1]*, Reiner Creutzburg* [2]**

[1] ***Technische Hochschule Brandenburg, Department of Business and Management, Magdeburger Str. 50. D-14770 Brandenburg, Germany***

[2] ***Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany***

Email: johannse@th-brandenburg.de, kantd@th-brandenburg.de, creutzburg@th-brandenburg.de

Abstract

Like many other industries, small and medium IT enterprises (IT SMEs) find themselves challenged by globalization and digital transformation. This paper highlights the implications and challenges for IT SMEs in the area of IT security, compliance, and data governance. It describes the secure and compliant integration of IT products and services of IT SMEs in order to enhance their relative competitive position against global players of the IT industry. The paper presents an approach that entails competence areas for IT security, compliance, and data governance and shows a web-based tool for surveying and measuring areas in order to derive actual readiness of IT SMEs in these areas. The paper concludes with an outlook on the expected findings and planned further developments of the approach and tool.

Keywords

IT security; compliance; data sovereignty; data governance; security awareness; IT security readiness; data protection; mobile security; small and medium-sized IT enterprises

Introduction and Motivation

In a globalized and digitized world, especially medium-sized IT enterprises, face new challenges to remain competitive against international actors. The IT industry of every economy is critical both as a key industry on its own and functioning as a driver for many other industries and sectors. SMEs within the IT industry often have a special focus in one or a few niche industries of their customers. However, this focus can increasingly result in a disadvantage in global competition. Hence, their products are often stand-alone solutions with proprietary data formats. Concerning IT security, these solutions may contain security gaps that represent serious impediments for further digital transformation. This, in turn, threatens to slow down the digitalization of the overall economy for the German and other EU national market situations for IT SMEs), while US IT SMEs are generally more focused on rapid standardization and platform thinking [33]). Concrete challenges for IT SMEs on a global scale are:

- A radically new competition with strong international actors (e.g., Microsoft, Amazon, Google, and others) based on the cloud and thus global availability of ever more IT products and services (see e.g., [40]).
- New requirements in secure development and standardization of interfaces as well as simplified availability of new technologies, especially in the field of "Industry 4.0" [22].
- Rising attack vectors through interconnected devices (especially in the field of Industrial Internet of Things (IIoT) [22].
- Transformation of proprietary solutions to cloud services in the course of digitalization, generating a new wave of commoditization in software offerings including software products, services, and business models [28]. This wave is again disrupting the existing Information and Communications Technology (ICT) industry after the previous commoditization during the turn of the millennium described by [7].
- General spread of cloud computing as well as significantly shorter innovation-cycles of software through DevOps and continuous integration of releases [1], [2].
- Further standardization and consolidation of software and IT service providers, strong competition and restructuring towards professional and global "IT Factories" [44].
- Shift of business models away from license-based software towards data-driven services for buyers of IT [11].

Driven by these trends, a demand of standardized, secure, and interoperable software among national and regional customers of IT SMEs grows rapidly. The majority of today's specialized niche solutions of IT SMEs within each local industry software market typically do not meet these requirements [38], [33]. These challenges can be faced by increased cooperation and joint product- and service developments among IT SMEs, especially on a long-term horizon, going beyond the "comfort zone" of full order books. However, IT SMEs possess only weak R&D departments and scarce strategic resources (see [3]). Actual digital readiness within IT SMEs is low, especially compared to large companies [40]). Strong developments can be perceived within the German "Mittelstand 4.0 program" of the Federal Ministry for Economic Affairs and Energy that supports SMEs with regard to digital transformation [14].

IT security, compliance, and data governance within IT SMEs

One solution for solving the problems mentioned above lies in stronger cooperation and joint innovation of IT SMEs among themselves. The ”Mittelstand 4.0 Competence Center for the IT Industry“ as part of the German ”Mittelstand 4.0 program“ aims to support secure cooperation and innovation among IT SMEs (see [25]). Support in secure bundling of resources and services over the Internet puts IT SMEs in a position to interconnect the existing software solutions as well as developing entirely new digital products and services. However, this calls for governance, security, and compliance as the sum of all competencies of an IT SME to organize and generate added value with joint products and services within digital networks and cloud platforms together with partners. For this reason, our research focuses on the safe and secure as well as compliant use of digitized processes and joint business models for IT SMEs. Small and medium-sized IT enterprises have to adhere to an increasing number of regulations, policies, and standards, not only since the advent of the European General Data Protection Regulation (GDPR) in 2016-2018 (see [10]) Therefore, the successful understanding and management of IT compliance is an important success factor for IT SMEs that want to engage in cooperation and cloud business models actively. IT compliance is the accordance of corporate IT systems with predefined policies and procedures [26]. However, there is a debate on the usefulness and value of the GDPR (see e.g., [39]). In particular, IT SMEs are facing rising costs to meet compliance requirements while at the same time missing appropriate resources compared to large enterprises. Moreover, many SMEs are hoping to see a reduction in bureaucracy in their day-to-day business activities. When emerging with data-driven business models or technologies like artificial intelligence, there is a need for an enormous amount of data. At the moment, however, the majority of gathered data are held by a few global players - for instance, Google, Apple, Facebook, or Amazon. For IT SMEs, it is nearly impossible to collect data in the same quantity, which results in a dependency on a few data held companies. For measuring and enhancing secure, sovereign, and compliant business of IT SMEs, the ”Governance, Security and Compliance (GSC)“ framework and tool was developed, which represents a first tool-based service to identify and measure the competencies mentioned above as well as needs for action. For companies using the GSC tool, central challenges for the joint design, marketing, and support of software products and services together with partners can be estimated. Also, they reach an awareness of critical aspects of data privacy, compliance, and IT security. Apart from the scientific objective of digital readiness determination, the tool serves as an efficient means of determining needs for action for the intended forms of cooperation for the participating IT SMEs.

Research- and tool design

Especially small IT SMEs are not always aware of the areas, and the extends in which IT-security, compliance, and data governance competencies are necessary today. For example, joint security management competencies of all parties involved across organizations play an essential role, apart from technical competencies (see [13] [12]). The GSC tool is designed to perform a first assessment whether the IT SMEs possess the competencies needed to design, develop, sell and maintain business software as new cloud services together with partners in a compliant, secure and effective way. The requirements that IT SMEs have to comply with in order to persist and remain competitive in today’s digital and data-driven markets are to be collected with the GSC tool in a self-assessment from February to June 2020. The self-assessment is based on the eight assessment categories that are presented in the next section. The benefit of the tool-based self-assessment for the participating IT SMEs is given in an easily usable web interface that issues quantitative and automated results directly after the survey. Optionally, an individual result set can be sent some days after the survey results have been analyzed in detail. After representative survey data has been gathered, it is additionally planned to give the result values also concerning the anonymous peer group values.

Target groups for GSC data gathering

The primary target groups for the survey are all persons that contribute to or are accountable for governance, IT-security, and compliance competencies within IT SMEs. This includes the following roles: CEOs, CIOs, Chief Security Officers, Heads of IT, Heads of product development, managers and official representatives for data protection and security, labor unions, customer managers, as well as consulting managers. The target groups thus include management levels as well as subject matter experts in the respective customer, product, and technology areas.

GSC readiness framework

Within recent years, many proposals have been made to measure the digital maturity of corporations, some originating from practice, focusing for example on cloud-readiness of traditional industrial producers (see for instance [29]), and others from research (see [43]).

Since the publication of the bestseller from Westerman/Bonnet/McAfee [42], these have been increasingly developed on a global scale. The approach by [42] that has been extracted from a series of international studies assesses companies in two dimensions (briefly summarized as “digital intensity” and “transformation intensity”) and classifies them into one of four distinct maturity levels [43]. An approach derived from international consulting practice is that of [35], that measures 10 categories of digital transformation abilities of corporations. The “Digital Maturity Model” of the IWI-HSG-Institute of the University of St. Gallen is well-known in german-speaking countries. It entails nine dimensions, that, in turn, are operationalized utilizing different indicators [4]: (1: Customer Experience, 2: Product innovation, 3: Strategy, 4: Organization, 5: Process digitization, 6: Cooperation, 7: Information technology, 8: Culture & Expertise, 9: Transformation management). Several maturity models use content or methods of successors from software engineering and project management, as e.g., those of the CMMI-model (see [21]). The approaches mentioned above of digital maturity typically shed no or very little light on governance, IT security, and compliance abilities or issues. Moreover, they are often not concrete and thus not suited for SMEs in general. Nor are they suited for IT SMEs in particular, whose cloud-technologies [33] often support primary and secondary processes. All companies, not only big corporations, have to measure the actual state and the quality of their information security. They need reliable information on the maturity of their security processes and practices. The

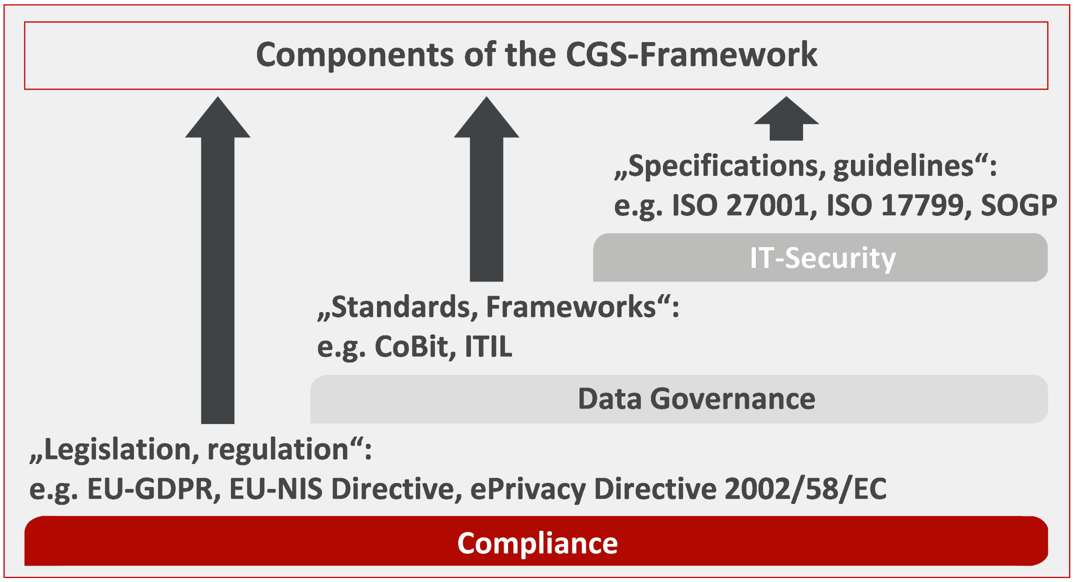
Components of the CGS-Framework
„Specifications, guidelines“:
e.g. ISO 27001, ISO 17799, SOGP
IT-Security
„Standards, Frameworks“:
e.g. CoBit, ITIL
Data Governance
„Legislation, regulation“:
e.g. EU-GDPR, EU-NIS Directive, ePrivacy Directive 2002/58/EC
Compliance

Figure 1. *Scope of the Compliance, CGS-Framework*

necessity of measuring information security arises from different reasons. There are many standards and guidelines for governing and measuring IT security and compliance. In Figure 1, we have depicted but a few of them that have global or at least European relevance. Some of them to not have the focus of SMEs, such as the Sarbanes-Oxley Act (SOX) and EuroSOX for Europe, that came into effect in 2002, but includes section 404 a/b since 2009, is only relevant for US-companies that are listed on the stock exchange. However, SMEs, as well as IT SMEs, often do not consider and apply all these standards and guidelines fully due to a lack of resources and competences. In addition, new standards and threats require permanent improvements in security procedures. Moreover, compliance with these regulations, standards, and guidelines is not an easy process that can be duplicated from organization to organization. “Measuring” how a firm complies to the binding legal regulations as well as to the optional standards and guidelines chosen by the top management typically involves detailed controlling of the realization of the goals and requirements defined (typically laid down in organizational information security policies) and derived from the regulations, standards, and guidelines given in an organization (i.e., the comparison of actual values with “To Be” values) on a periodical basis. Furthermore, gaps and deviations have to be managed within appropriate management frameworks such as the PDCA cycle (“Plan”, “Do”, “Check”, “Act”, see e.g., its application in ISO/IEC 27001).

IT security regulations, standards, and guidelines typically include the establishment of rules that must be obeyed. The rules define competences as well as restrictions for making decisions and set out consequences for breaches of the rules. Decisions are made by human beings, and humans as well need to understand and accept the meaning and purpose of the rules and to establish secure and compliant business processes. This leads us to content that all levels of management are essential elements for compliance, governance, and security management, especially within SMEs. Our literature review revealed no attempt to implement an integrated but also lean and usable compliance, governance, and security framework for SMEs worldwide. Similarly, up to date, no practice-oriented framework or tool to measure compliance, governance, and security readiness or maturity has been put forward. An established approach is the production of security metrics through the collection of best practices is based on ISACA [20]. However, this production is a complex endeavor for SMEs since the metrics have to be designed mainly by IT professionals that are competent with all relevant IT security and compliance regulations. The rather complex definition of “metrics” by the National Institute of Standards and Technology (NIST) in its Special Publication (SP) 800-55 already shows this: “*Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions, based on observed measurements*” [8]. Based on our literature review, research on IT-related maturity or digital readiness of SMEs is often restricted to specific aspects. Studies exist on the competence area of secure software development (see e.g. [24], [34], or continuously integrating security [45], [44]. Other studies focus on the design of an ISMS-related scorecard [36] or IT security maturity in a technical sense [19].

To sum up our literature review, no frameworks for SMEs do exist for measuring IT security levels that include data governance and compliance issues in a lean and applicable way that furthermore integrate global standards and regulations (such as ISO/IEC, COBIT, EU-GDPR, and SOGP) which are increasingly relevant for SMEs with international customers. As a result of the literature review summarized above, we thus derived eight relevant categories for measuring IT security, data governance, and compliance readiness of IT SMEs. We then operationalized these eight categories using actual competence and action areas (see "statements" below). The approach presented here unites technical competencies concerning the use of IT security technologies as well as organizational and strategical competencies of an IT SME to ensure and broaden long-term business success through compliance and data governance-related abilities. We define compliance, governance, and IT-security (CGS) readiness based on these eight categories, which will be presented in the following.

Categories

Security Awareness Information Security Awareness (ISA) can be regarded as a major and still growing field of information security. ISA is most frequently referred to as a cognitive state of mind, which is characterized by recognizing the importance of information security and being aware and conscious of information security objectives, risks, and threats, and having an interest in acquiring the required knowledge to use information security responsibly [17].

ISA entails more than defined by some authors, who merely connotate this concept with the awareness and knowledge of the content of all relevant security regulations and policies in a given organization. It is instead a multidimensional concept, as e.g., [18] have shown. The most significant inhibitors to defending against cyber threats in organizations are probably the lack of a security budget and low-security awareness among employees. An optimistic attitude among organizations is also quite common [19]. In information systems, the sole use of technical security mechanisms and systems does not suffice. Moreover, these systems have to be considered as social-technical [15], including human interference e.g., employees may accidentally execute malicious email attachments and thus compromise an entire corporate network. "*The lack of modern security protocols and tools, however, does not address perhaps the most significant security risk to industrial control systems: the propensity of humans to ignore common sense and inadvertently expose the network to malware through their behavior*" [27]. Besides technical attack vectors, social engineering is another source (with a high prevalence) for malicious intent.

Data Governance The term Data Governance stands for holistic management of data over its complete life cycle in a company or organization (see [23]). The main objective is to comply with relevant data quality, security, and processing standards. This enables companies to have full sovereignty over their digital data, meaningfully owning and controlling them. Data governance and sovereignty in inter-organizational settings are becoming more and more important also for IT-SMEs, including aspects of the degree of openness of global and regional digital platforms as well as access to and free trade with these platforms (see [5], and [9]).

(IT) Compliance / Data Privacy Compliance, in general, means conforming to policies, rules, standards, specifications, guidelines, or laws. IT compliance is the appliance to the IT environment or systems. Data Privacy governs how data is collected, shared, and used. Compliance requirements can be distinguished into internal rules and regulations and external legislation. Concerning internal regulations, they comprise guidelines or operating procedures. Today's business of IT-SMEs is increasingly flooded by cloud computing (e.g., SaaS, PaaS, and IaaS). As mentioned in the introduction, global but also regional IT markets currently undergo a profound disruption. Global public cloud services markets are projected to grow by 17.33% in 2019 to a total of $206.2B, up from $175.8B in 2018, according to Gartner [16]. Especially for IT SMEs, there are opportunities but also risks. Therefore, security and privacy remain challenges for IT SMEs. The new privacy-related laws and regulations (e.g., The General Data Protection Regulation in Europe) are considered aspects of this category.

Information Security Management (ISM) This category describes policies, procedures, and methods that an organization needs to implement to regulate and control information security. This aims to ensure the confidentiality, availability, and integrity of assets from threats and vulnerabilities. ISM is highly connected with information risk management. Common standards like ISO/IEC27001, COBIT, or ISM3 proof as unpractical to apply within the majority of SMEs due to complexity and the necessity of high resources [34].

Technical / physical IT Security The term technical IT Security refers to IT systems from hardware firewalls to security mechanisms. With physical IT security, access to rooms or facilities is meant, as well as measures like anti-theft protection. This category encompasses electronic and computer technologies such as backups, authentication, encryption, power supply, network security, server security, platform security, etc. on the one hand, but also physical technology and infrastructure on the other hand.

Cyber Security / Cloud Security This category includes protection against cyber-attacks using sophisticated security mechanisms. Cloud security comprises a large number of individual measures that protect against risks such as data loss, service failure, or unauthorized access when using cloud services. Compliance with legal data protection regulations is also related to cloud security. However, leading researchers state that cyber security is about to lose the battle against cyber attacks [37]. Thus, cyber security must be practiced as a principled engineering discipline, and especially IT-SMEs need to be prepared to increase their cyber security budget to stay successful in their markets.

Web Application Security / Secure Software-Engineering Web Application Security is a branch of information security dealing specifically with securing web interfaces or web sites, web applications, and web services. These applications are commonly used and may be vulnerable to e.g., Cross-site scripting, SQL injection, or code injections. Secure Software-Engineering deals with flaws in configuration or implementation of software - which can result as an attack vector - as well as the mitigation of them. Recent research proposes the "security by design" approach that encourages security awareness and considerations in all phases of the software development life cycle. Security awareness, in particular in the requirements engineering stage of the software development life cycle (SDLC), is essential in building secure software (see e.g., [30]).

Mobile Security / BYOD The last category is measuring Mobile Security in general, including end devices like laptops, tablets, or smartphones. Bring Your Own Device (BYOD) is the term describing the use of private mobile devices in companies. These devices can turn to a serious security threat, in particular, because they contain a microphone, a camera as well as a mobile internet connection. The majority of recent studies report that users, especially those without strong information technology familiarity, tend to ignore or be unaware of many critical security

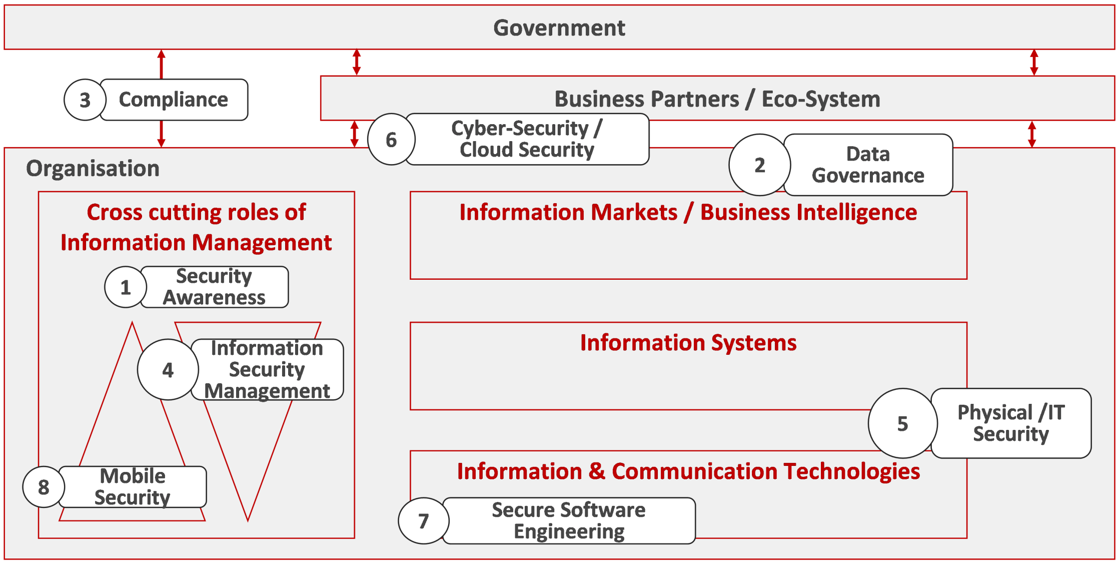
Government
3 Compliance
Business Partners / Eco-System
6 Cyber-Security / Cloud Security
2 Data Governance
Organisation
Cross cutting roles of Information Management
1 Security Awareness
4 Information Security Management
8 Mobile Security
Information Markets / Business Intelligence
Information Systems
5 Physical /IT Security
Information & Communication Technologies
7 Secure Software Engineering

Figure 2. *The eight categories of the GSC readiness framework within the corporate Eco-System*

risks and also their options [41]. In the light of their special security challenges, long-term security strategies for managing mobile devices in SMEs are increasingly necessary [6]. A rather new type of corporate management information systems category is that of “Mobile Device Management” (MDM) or “Enterprise Mobility Management” (EMM) systems, that help not only IT administrators but also CISOs, CIOs, and CTOs to assess the risks associated with mobile devices used inside and outside of corporate networks [31].

Table 1 summarizes the eight categories of our approach and shows key competence areas that we measure within each category.

Approach for tool-based readiness determination

For determining capabilities, the target groups and respondents of IT SMEs follow a defined process that is based on a standardized online survey tool as part of the “Governance, Security and Compliance Tool” (GRC tool) and proceed in six steps:

1. Initially, all eight main statements have to be rated (“quick check”).
2. A PDF report is directly generated as output.
3. For an advanced evaluation, the appropriate statement pool is chosen (32, 64, or 100).
4. Now, detailed statements have to be rated by different experts within each IT SME.
5. Optionally, further employees of the IT SME can be invited to take part in the rating process.
6. Finally, detailed analysis results will be generated.

For all eight categories, statements have been generated. For each category, one main statement exists (total of 8), as well as (32, 64, or 100) detail statements for the measurement of the respective competencies. With a growing number of statements in these sets, the calls for action given later as a result of the survey are becoming more and more detailed.

Figure 4 shows a main statement and some detailed statements on the category “Information Security Management (ISM)”. All answers given by the respondents are structured in a Likert scale, ranging from total agreement to complete disagreement with the statement. Respondents are asked to give their individual and subjective rating concerning the importance (*very important*, *important*, *neutral*, *less important*, *not important*), as well as for the capability (*very good*, *good*, *satisfactory*, *sufficient*, *inadequate*) of their company or organisation in relation to the given statement. In addition to this, the respondents can add own feedback as free text to the survey within each of the eight categories.

A pretest of the study design, as described here, was performed with chief executives of three IT SMEs, which resulted in a partial adaption of some of the statements. The survey has been carried out utilizing SSL-encrypted evaluation sheets that are sent over the Web to the individual respondents of the IT SME, some of them having been invited by other respondents (typically the CEO of the IT SME) that successfully underwent the registration process. It is planned in later versions of the survey tool to indicate mean values based on the evaluations of all other respondents and companies given to each statement so far.

This way, a relative CGS readiness compared to the overall peer group or industry can be calculated for each company or organization. The anonymous results of all individual surveys of an IT SME will be sent to the chief executive officer (CEO) in case the respondent agreed to this. In addition to this result document, it is planned that an analysis can be offered to each participating IT SME via a secure download link. The analysis generally focuses on comparison and interpretation of the Likert-based in-

Categories	Competencies (Excerpt)
Security Awareness	- Awareness of companies regarding IT Security in general - Degree of sensitization employees as well as the management - Motivating employees in awareness - Frequency, attendance and quality of training sessions - Social Engineering Awareness (e.g. CEO Fraud) - Sensitization for Secure Engineering - Informing employees about recent security threats - Evaluation of Security Awareness measures
Data Governance	- Measure of data quality - Data governance strategy - Usage of Big Data - Adherence of data integrity - Evaluation of the data collection process - Determination of data ownership - Information Lifecycle Management (ILM)
(IT) Compliance / Data Privacy	- Presence of certificates (e.g. ISO) - General Data Protection Regulation-Compliance - Evaluation of data processing policies - Quality and frequency of audits
Information Security Management	- Established Information Security Management System (ISMS) - Definition of security policies, procedures, processes, concepts, and methods - Evaluation and adjustment of security measures - Existence of an Incident Management - Cyclic revision of policies - Applying the PDCA cycle - Overall risk assessment / risk management
Technical / physical IT Security	- Usage of encryption - Usage of authentication - Sandboxing and Container Management - Update/Patch Management - Technical security mechanism (e.g. firewall, anti-virus-application) - Access authorization concept - Quality of data backup concepts - Physical reliability mechanisms - Implementation of redundancy mechanisms
Cyber-Security / Cloud-Security	- Detection and prevention mechanisms for cyber attacks - Cyclic penetration testing and vulnerability scans - Protection mechanisms against brute-force and dictionary attacks - Deep Packet Inspection - Data Leak Prevention - Logging and Monitoring of network traffic - Computer Emergency Response Team (CERT) - Cloud Policy
Web App Security / Secure Software-Engineering	- Protection against top 10 threats [32] - Fuzzing - Usage of security frameworks - Temporary login blocks - SSL/TLS usage - Password complexity
Mobile Security / BYOD	- File system encryption - Remote deletion - Encryption mechanisms for remote access to resources (e.g. VPN) - Black- and Whitelisting of Apps - BOYD directive - BYOD user agreement - Mobile Device Management Systems (MDM) - Mobile Application Management Systems (MAM)

Table 1: Competence areas within the 8 categories of the GSC framework

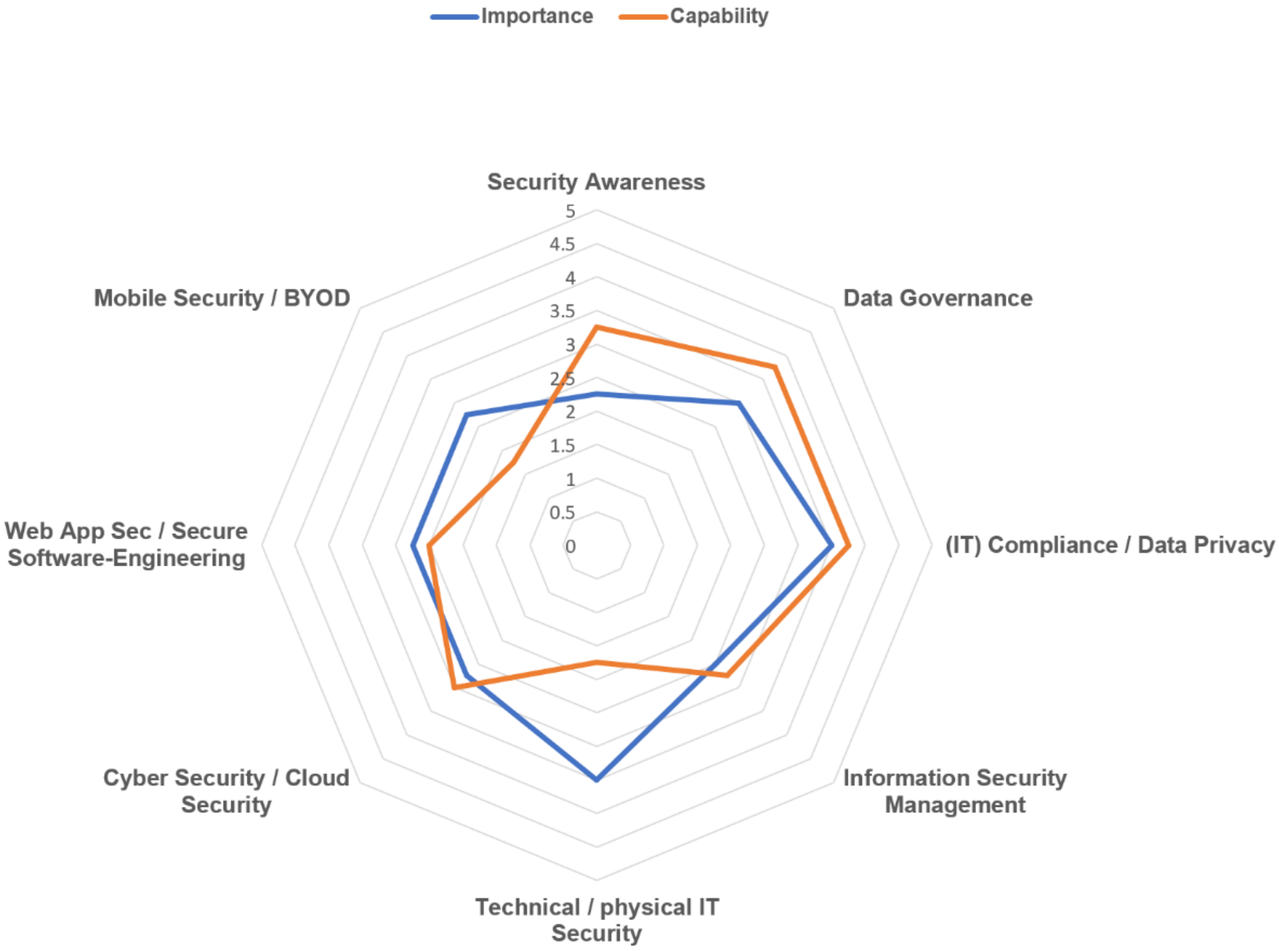

Figure 3. *Comparison of capability and importance of the detail statements (spider diagram)*

dividual evaluations of importance and capability connected with each competence statement given for the individual set of statements. From this, the As-Is situation and calls for action for the IT SME can be derived.

Evaluation

After answering the main statements, an automated PDF short evaluation takes place, that can be downloaded immediately after the respondent took part in the "quick check" survey. This contains two pages. The first page presents the aggregated results of the assessment of the importance and ability of the eight categories. On the second page, the entered data is automatically evaluated on the basis of a first classification to provide rough strengths and weaknesses, general conclusions, and needs for action. Within the detailed evaluation, on the other hand, bar charts and spider diagrams are generated automatically from the evaluations of one or more IT SME employees, which are integrated into a final report for optional download. In bar diagrams, the answers to the specific competence areas are displayed. Importance and capability are clearly compared so that deviations and gaps can be seen at a glance. If importance and capability differ substantially from each other, then there is a need for action for the company or organization. The spider web diagram (Figure 3) allows identifying discrepancies between the indicated importance and ability quickly as well as to identify corresponding areas of action.

Summary and Conclusion

Based on the anonymous evaluation of the assessments made to date by the managing directors of three IT SMEs within a pretest in November 2019, it can be summarized that the GSC Readiness Tool (GSC-Tool) contributes to sensitizing and qualifying the target group's need for action. The collected data will be used anonymously, as planned, to evaluate the target group's level of governance, security, and compliance readiness. The evaluation of the results for the responses is always carried out by interpreting and comparing the indicated importance/significance of a competence area and the indicated capability in the competence area. This entails a restriction of the identification of the actual situation and the need for action, which cannot cover the entire picture of the IT SME and its sub-sector within the IT industry, especially in the case of the automated evaluation of the main statements. In this respect, the approach of measuring the degree of maturity of the governance, security, and compliance readiness of IT SMEs does not replace further analyses and evaluations in individual cases.

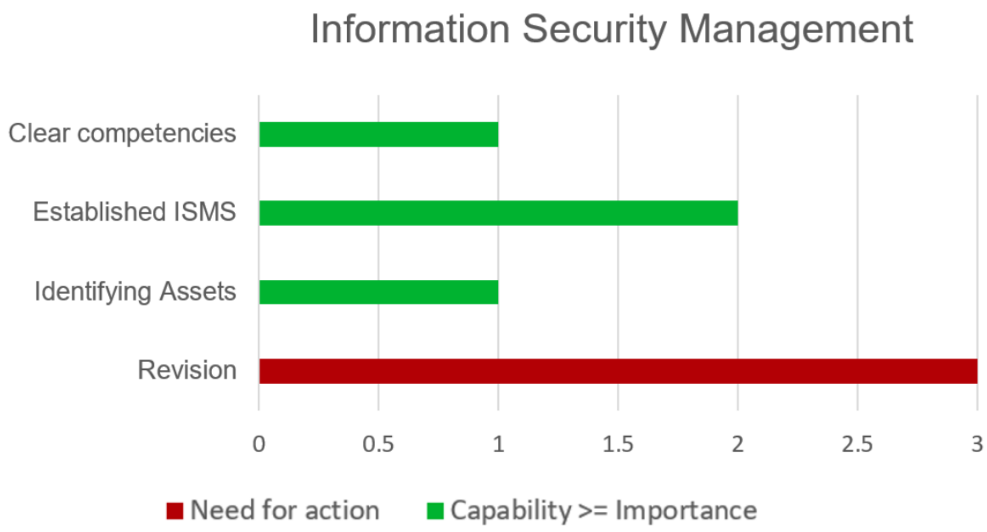

Figure 4. *Example evaluation for the specific category Information Security Management*

Nevertheless, the structured presentation of the detailed evaluations according to the eight categories, in particular, provides a first picture of the strengths, weaknesses, and needs for the action of the IT SMEs concerned. This has been confirmed by the CEOs of the three companies participating in the pretest. In this respect, the practice-oriented and pragmatic approach of determining the readiness level through self-assessment of actors from the target group presented here can be confirmed at this early stage. On the one hand, the separation between short, automated quantitative evaluation of the main statements (target group ”managing directors/executive board members”) and the detailed evaluation of the detailed statements appear to be a successful approach for the high participation of the target groups. We expect other exciting insights from differences in the answers and ratings of the different target groups within IT SMEs (managing directors, IT managers, product development managers, corporate information security officers (CISOs), data protection officers, union members, product and customer managers, service consulting managers), which are to be evaluated and interpreted individually.

Future Work

We plan to start to go-live of the GSC tool in spring 2020, and a first empirical survey based on a two-month data-gathering phase. Meanwhile, the approach for modeling and measuring governance, security, and compliance readiness of IT SMEs utilizing our GSC-framework, and the GSC-readiness tool itself are to undergo a series of extensions and validations in the next project phases in 2020. After representative survey data has been gathered, primarily from IT-SMEs within the EU, it is additionally planned to automatically display the result values also to the anonymous peer group values in the automated evaluation reports. It is planned in later versions of the survey tool to indicate mean values based on the evaluations of all other respondents and companies given to each statement so far. This way, relative governance, security, and compliance readiness compared to the overall population (more precisely to the peer group of the specific sub-industry) can be calculated for each company or organization. Initially, the detailed evaluations of individual persons at the level of an IT SME participating in the evaluation will only partially be evaluated automatically. However, automatic evaluations would make it possible to investigate a significantly higher number of empirical cases and thus a higher proportion of IT SMEs, while at the same time reducing the effort involved in the evaluations. It is also planned to enrich the capability areas of IT SMEs in future versions according to further research and the feedback of the respondents. The dissemination and application of Artificial Intelligence solutions for IT security could be one of the trends that could be identified within the group of the participating IT SMEs. It is also planned to draw up hypotheses based on higher numbers of respondents and to test them against the anonymous database in order to generate further conclusions for research questions relevant for IT SMEs.

References

[1] Al-Ali, A. G.; Phaal, R.: Design Sprints for Roadmapping an Agile Digital Transformation, in: 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC).

[2] Abolhassan, F. (Ed.): The Road to a Modern IT Factory Industrialization – Automation – Optimization, Springer, Berlin Heidelberg, 2014.

[3] Aumasson et al.: The economic and social impact of software and software based services in Europe Final Report 2010.

[4] Back, A.; Berghaus, S.; Kalternrieder, B.: Digital Maturity & Transformation Report, Institut für Wirtschaftsinformatik, Universität St. Gallen, March 2017.

[5] Stefi, A.; Berger, M., and Hess, T. (2014): What Influences Platform Provider’s Degree of Openness? – Measuring and Analyzing the Degree of Platform Openness, in: C. Lassenius and K. Smolander (Eds.): ICSOB 2014, LNBIP 182, pp. 258–272, 2014. p. 258.

[6] Brodin, M.: Mobile Device Strategy: From a Management Point of View, J. Mob. Technol. Knowl. Soc., vol. 2017, pp.

1–9, 2017.

[7] Carr, N. G.: IT Doesn’t Matter, Harvard Business Review, May 2003.

[8] Chew, E.; Swanson, M.; Stine, K.; Bartol, N.; Brown, A.; Robinson, W.: Performance Measurement Guide for Information Security, NIST Special Publication 800-55 Revision 1, July 2008.

[9] Duch-Brown, N.; Martens, B.; Mueller-Lange, F.: The economics of ownership, access and trade in digital data, JRC Digital Economy Working Paper 2017-01, European Commission.

[10] European Commission: Regulation (EU) 2016/679 (...) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://data.europa.eu/eli/reg/2016/679/ retrieved: November 2019.

[11] European Commission: ANNUAL REPORT ON EUROPEAN SMEs 2018/2019: Research & Development and Innovation by SMEs, 2019.

[12] von Faber, E.; Behnsen, W.: Joint Security Management, Springer Vieweg, ISBN 978-3-658-20833-2, 2018.

[13] von Faber, E.; Behnsen, W.: Secure ICT Service Provisioning for Cloud, Mobile and Beyond, ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers, Springer Vieweg, 2017.

[14] Federal Ministry for Economic Affairs and Energy, VALUING SMEs, THE GERMAN SME STRATEGY, www.bmwi.de, October 2019.

[15] Gardner, B.; Thomas, V.: Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats, Syngress, 2014, ISBN-13: 978-0124199675.

[16] Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019, `https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019` (retrieved: December 2019).

[17] Häussinger, F.; Kranz, J.: Antecedents of Employees’ Information Security Awareness -Review, Synthesis, and Directions for Future Research, Proceedings of the Twenty-Fifth European Conference on Information Systems (ECIS), Guimarães, Portugal, 2017, ISBN 978-989-20-7655-3.

[18] Hanus, B.; Wondsor, J.; Wu, Y.: Definition and Multidimensionality of Security Awareness: Close Encounters of the Second Order, in: The DATA BASE for Advances in Information Systems, Volume 49, Special Issue, April 2018, pp. 103-132.

[19] Heikkila, M.; Rattya, A.; Pieska, I.; Jamsa, J.: Security Challenges in Small- and Medium-Sized Manufacturing Enterprises, in: SIMS 2016 International Symposium on Small-scale Intelligent Manufacturing Systems, 21-24 June 2016, Narvik, Norway, IEEE.

[20] ISACA: Monitoring Internal Control Systems and IT, ISACA, Rolling Meadows 2010.

[21] Johannsen, A.: Introduction for Software Project Managers in Classic and Agile Contexts. Dpunkt, Heidelberg, 2017.

[22] Kant, D.; Creutzburg, R.; Johannsen, A.: Investigation of risks for critical infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan, in: IS&T International Symposium on Electronic Imaging 2020 Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2020, Society for Imaging Science and Technology.

[23] Karel, R.: Data Governance: What Works and What Doesn’t, edited by Forrester Research. Cambridge, MA, 2007.

[24] Khan, S.A.; Khan, S. U.: A Preliminary Structure of Software Security Assurance Model, in: 2018 ACM/IEEE 13th International Conference on Global Software Engineering, pp.132-135.

[25] Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft, https://itwirtschaft.de, retrieved: May 2019

[26] Kim, S.: IT compliance of industrial information systems: Technology management and industrial engineering perspective. J. Syst. Softw. 2007, 80, 1590–1593

[27] Kirkpatrick, K.: Protecting Industrial Control Systems Finding, and plugging, the security holes in SCADA, in: CACM, October 2019, VOL. 62, NO. 10, p.14-16.

[28] Kushida, K. E.; Murray, J.; Zysman, J.: Cloud Computing: From Scarcity to Abundance, in: Journal of Industry Competition and Trade (2015) 15:5–19, Springer.

[29] Loebbecke, C.; Thomas, B.; Ullrich, T.: Assessing Cloud Readiness: Introducing the Magic Matrices Method Used by Continental AG, in: M. Nüttgens et al. (Eds.): Governance and Sustainability in IS, IFIP AICT 366, pp. 270–281, 2011.

[30] Mufti, Y. et al.: Readiness Model for SRE, in: IEEEAccess, Vol. 6, 2018, pp. 28611-28631.

[31] Ortbach K.; Brockmann, T.; Stieglitz, S.: DRIVERS FOR THE ADOPTION OF MOBILE DEVICE MANAGEMENT IN ORGANIZATIONS, in: Twenty Second European Conference on Information Systems, Tel Aviv 2014.

[32] OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks; Open Web Application Security Project; `https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf`, retrieved: December 2019.

[33] Picot, A.; et al.: The Internationalization of German Software-based Companies: Sustainable Growth Strategies for Small and Medium-sized Companies, Springer Cham Heidelberg New York London, 2015.

[34] Ponsard, C.; Deprez, J.-C.: Helping SMEs to Better Develop Software: Experience Report and Challenges Ahead, Belgium, ACM/IEEE 40th International Conference on Software Engineering: Software Engineering in Practice, 2018.

[35] 2015 Global Digital IQ® Survey, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/advisory-services/digital-iq-survey-2015/campaign-site/digital-iq-survey-2015.pdf, 2015, retrieved: February 2019.

[36] Sanchez et al.: Management of Scorecards and Metrics to Manage Security in SMEs; in: MoSE+DQS’09, November 2009, Hong Kong, China, ACM; p. 9-16.

[37] Saydjari, S.: Engineering Trustworthy Systems: A Principled Approach to Cybersecurity, in: CACM, June 2019, VOL. 62, NO. 6 p. 63-69.

[38] Markus, S.: Business Models in the Software Industry – The

Impact on Firm and M&A Performance, Springer Gabler, 2014, ISBN 978-3-658-04351-3.

[39] Sirur, S. et al.; Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR); MPS ’18, October 15, 2018, Toronto, ON, Canada, ACM, 2018.

[40] United Nations: Digital Economy Report 2019, UNCTAD/DER/2019, `un.org/publications`, New York, 2019.

[41] Watson B.; Zheng, J.: On the User Awareness of Mobile Security Recommendations, in: ACM SE ’17, April 13-15, 2017, Kennesaw, GA, USA.

[42] Westerman, G.; Bonnet, D.; McAfee,A.: Leading Digital – Turning Technology into Business Transformation, HBR Press, Boston, Mass., 2014.

[43] Westerman, G.; McAfee, A.: The Digital Advantage: How Digital Leaders Outperform Their Peers in Every Industry. Research Brief by the MIT Center for Digital Business, 2012.

[44] Wiedemann, A.; Forsgren, N.; Wiesche, M.; Gewald, H.; Krcmar, H.: Research for Practice: The DevOps Phenomenon, in: CACM, August 2019, VOL. 62, NO. 8, pp. 44.

[45] Williams, L.: Continuously Integrating Security, in: 2018 ACM/IEEE 1st International Workshop on Security Awareness from Design to Deployment, 2018.