Creation of a distinct culture for the overall system “Compliance, IT security and Data protection” in municipalities in Germany

Christian SCHACHTNER,
Professor of Public Management, IU University of Applied Sciences, Bad Reichenhall, Germany
christian.schachtner@iu.org

Abstract

Public administrations in Germany today are increasingly exposed to attacks from the digital space. Threats to their IT systems or organizations in the physical world require security strategies. The Objectives of the work are the conviction of government leaders to enable themselves to control the implementation of data protection and IT security in their organizations with priority and resources. This also includes compliance as part of information security management systems in order to better anchor compliance in the overall organization, especially at the operational level. The Prior work shows that only a few protective measures are implemented in municipalities in Germany, although models for IT-Governance are available. One reason could be the scope and abstractness of the management systems, which lead to avoiding the introduction phase. To close the gap between awareness of the relevance of the topic and the actual taking action of measures, clear vision of practical implementation must be conveyed in order to protect the organization sufficiently and permanently. The Approach is based on a combination of technology, strategy and people. A bipolar approach is to be chosen in this thesis: Government leaders are to be simulated by a game-based learning approach knowledge around the topics of IT security, data protection and compliance through serious games scenarios. At the operational level of the security officers, building blocks such as "Building information security", "Compliance processes and applications" and "Risk management" are to be developed collaboratively as predefined building blocks and meaningful process models are to be visualized at a uniform level of abstraction. The first Results lead to the realization that technical and organizational measures for institutional protection can be developed independently, so that no external consultants are required. Authority management can increasingly assume their responsibility in this area as soon as a basic understanding of sufficient resources has been established and their own roles in the overall system of compliance, IT security and data protection are assigned. The Implications include enabling government leaders to initiate and manage compliance in their organizations. The operationally responsible employees must be enabled to implement compliance in practice in cooperation with experts from thematic departments. In the long term, this is intended to create a distinct compliance culture in an organization. The Value of the work lies in getting compliance directly linked to the working level in order to anchor it directly in the organization. Government leaders are tasked with building a security- and risk-based culture. The thesis focuses in particular on adapting the mindset of employees and operational managers with regard to security risks and their consequences. Prioritization in preventive measures must therefore be shown in order to take up decisions on activities against cyber attacks and other incidents.

Keywords: IT security, data protection, compliance, mindset security risks, game-based learning, process modelling awareness.

1. Introducition and current Situation in the Field

Today, the threat situation of IT system environments can be found not only in large-scale industry but also in small and medium-sized enterprises as well as public authorities in ongoing cycles. The frequent gaps in the IT infrastructure of municipalities in particular have repeatedly been part of headlines in Germany since 2022 about successful hacking and the failure of the entire system. According to a BITKOM survey, this caused a total loss of 202.7 billion euros to the economy and the public sector in Germany in 2022 [1].
The vulnerability in the digital space presumably results from a mixture of a lack of funds for technology updates, failures in IT strategy and a lack of know-how. Information security is a strategic task of the top management level. In particular, the development of a

security- and risk-based organizational culture, the sensitization of the specialist departments, the development of a measurable criteria in a security strategy and the permanent transformation of the mindset of employees as designers of their own sphere of activity to behave under the awareness of constant cyber attacks is of great importance. Especially in municipalities, considerations are hardly made about mature concepts of procedural data protection according to ISO 27xxx, let alone such a technically oriented Information Security Management System (ISMS), although the legal obligation and also the awareness of the necessity are given [2].

There is already a process model with a focus on SMEs or municipalities: CISIS12®®. IT stands for Compliance and Informationsecurity in twelve steps and is an ISMS as a result of a ten year development period based on the experiences accumulated from different surveys of SMEs and authorities initiated by the IT Security and Safety Cluster. The framework is designed to roll out information security processes both horizontally and vertically within a fixed security structure modell focused on Riskmanagement [3].

Several reasons related to technical complexity or lack of procedural control may be reasons why so few administrative managers live up to their role in this area and also do not allocate sufficient resources to the security area.

Against this background, this paper is intended to create a new, playful approach for the target group of decision-makers in municipalities on the topics of IT security and technical infrastructure security and to provide a toolset for visualizing and structuring the necessary steps to implement an information security system.

2. Research interest and methodology

The overall goal of the study is to better understand the mechanisms and barriers to active implementation of security measures. Systemic structures in the organization are intended to permanently invest in actually better cybersecurity. In addition to the importance and implementation paths for decision-makers, employees should be enabled to playfully put current business processes into practice in terms of IT compliance.

2.1. Research interest

With a focus on public administration, specific aspects of the organization and management of municipalities in the sense of a compliance culture in the field of IT security and data protection will be examined in more detail. This study therefore deals with questions about gaining knowledge (What still needs to be understood?) and with regard to recommendations for implementation (What constitutes successful transformation in IT security? What else needs to happen?). The following areas of interest and questions are considered:

- Analysis of the current handling of information security in the context of change and transformation in public administration
- Development of a better understanding of concerns and uncertainties at the decision-making level in this field
- Finding structural starting points and a methodological xmis for access to the topics of IT security, data protection and compliance for municipalities?
- How can business and government leaders be enabled to initiate and control compliance in their organizations?

- How should the empowerment concept of employees be designed in the future so that an ISMS can be lived in everyday life after it has been introduced?

2.2. Methodology

The methodological approach followed a mixed-method approach, which was based on the approach of a Delphi study according to Häder&Häder [4]. The research design includes exploratory and prognostic components. The first empirical step of the data collection was expert inverviews, on the basis of which dimensions for the first approaches of game-based learning in the field of IT security were identified. In two rounds, a high degree of agreement between the statements and approvals of the experts was achieved. The results of the first round of surveys were presented for evaluation in the form of resulting scenarios of the mediation of ISMS building blocks during a second round.

Interviews with experts

For a sound empirical basis,various group and individual interviews with 18 experts were conducted between September and December 2022. The sample consisted of various representatives of federal levels and areas of administration, as well as associations with a scientific perspective and also consulting firms that collaborate on projects with public administration. As a rule, the municipalities were These semi-structured interviews were conducted using a conversation guide after it was designed with a test group as a pretest. All conversations were conducted and recorded via video calls. The average duration was 90 minutes. Key questions on various focal points provided the framework and stimulated discussion and exchange for the participants.

The thematic focus of the guide can be divided into four areas:

1. Status quo on challenges,
2. Status quo on dealing with compliance,
3. Dealing with experiences from previous training,
4. Classification of the importance of risk management and degree of organizational transformation.

Key questions were, for example:

- In view of the resistance and inadequacies of the employees, what do you think are the biggest challenges in the introduction of standardized information security systems?
- Which ideas, concepts, methods and approaches do you consider to be particularly relevant for dealing with the challenges discussed in practice?
- What degree of maturity of the systematic prevention measures and methods and approaches do you consider to be particularly relevant for better dealing with the challenges discussed in practice in the future?
- What are the most important administrative approaches that could increase data sensitivity for public administration workers?

The further substantiation of these approaches was pursued by means of a series of workshops in the format presented below for the acquisition of further insights with 30 decision-makers for digitization measures in municipalities. The meetings held between January and April thus represent the second part of the qualitative data collection:

Course of a workshop (2-2.5 hours)
10 min: Welcome/Short Inquiry of Expectations/Experiences
15 min: Input (e.g. on CISIS12® procedure) with knowledge level query with scenario maps + classification

25 min: Role play (at the table with everyone)
30 min: Compliance processes in groups
Pause
40 min: Risk Games: Risk Scenarios/Risk Cases; protection target abacus; TOM
Reflection/Discussion/Feedback

For the research topic in the field of technology research, a qualitative clustering was used in order to prepare the complexity of real-causal relationships in framework conditions for generalizability [5].

3. Theoretical Framework: Management Approaches to Learning of Security Infrastructure Measures

With regard to the theoretical foundation, a distinction must be made between two levels. On the one hand, there is the cybersecurity system to be conveyed in terms of content, the concept of an information security system developed as CISIS12® is geared towards reduced complexity for SMEs and municipalities.

The model comprises twelve steps with different building blocks.

- The topic of "Compliance and related processes" is becoming an essential new element, in that a vision and guideline of understanding the importance of the topic is planned.
- The structure specifications with technical standards, catalog of measures or audit scheme for criteria of excellence in security.
- References to relevant standards and catalogues often measures from BSI-IT-Grundschutz and ISO/IEC 27001.
- Integration possibilities of industry-specific standards and catalogues, such as TISAX, B3S-KRITIS.
- Supplemented documents by: Manual, training concept
- Software with project management, DSGVO module, document control

On the other hand, organizational, model or software development in the context of IT security should be methodically combined conceptually in the teaching of competencies. Since concrete demands of practice are to be included in the design phase, the Action Design Research (ADR) approach according to Sein et al. [6] is followed. In it, after an analysis phase of the real requirements, a design phase is started, based on the accuracy of the successful implementation according to the requirements.

Accordingly, a distinction must be made between the following phases within the process model:

1. Problem analysis: the exploratory interest in knowledge lies in further narrowing down the causes of problems and methodically questioning the clarity through game-based learning methods.
2. The design of game-based learning and a haptic process support system as a modular system correspond to the CISIS12® system: "Building Information Security", "Compliance Processes and Applications" and "Risk Management" as well as preparatory governance for decision-makers.
3. Evaluation and further development: practical determination of which methods of game-based learning are accepted for the target group of business/authority management or which adjustments are necessary to differentiate between different process elements. Furthermore, long-term workshops are to be held with operational staff in order to evaluate implementation details. As a result, manageable and user-friendly forms of visualization are to be further developed or adapted.

4. Results and Value

In this section, the main findings from the above mentioned qualitative surveys into a status-increasing of acceptance, concrete strategies of the cultural change and parallels of the acquisition of competence process optimization and a culture of security awareness.

4.1. Results

From the interview material from the Delphi process, three overarching categories could be derived. Based on the categories, three dimensions of implementation in the change process were developed:

1. Current state of understanding compliance in relation to information security
   The following aspects can be summarized as a definition of "compliance". Compliance as a
   ...Introduction oft a procedural view of compliance fulfilment
   ...Level based ranking, which takes into account all internal and external specifications
   ...Responsibility of the management level
   ...Basis for decision making in corresponding processes
   ...Implementation standard of the applications, the IT infrastructure and the buildings
   ...Implementation requirement for a superordinate PDCA cycles (Plan-Do-Check-Act)

This category describes the current state of affairs within the German public administration. From the different perspectives and experiences of the experts, a broad picture can be drawn of how the German administration behaves when dealing with changes in central systems. The spectrum of this status quo is diverse and ranges from active ignorance ("Existing fears are often deliberately swept under the carpet.") to active handling, but in a select circle ("In confidential meetings with executives from the administration, consequential risks are definitely addressed.").

2. Opportunities for systemic risk management in cybersecurity in municipalities
   An understanding of the target group inrelation to risk management is a combination of several criteria. Risk Management as Chance for
   ... an Introduction of a systematic management approach
   ... Implementing a structured ISMS processes in risk assessment and evaluation
   ... Core processes of identifying the "critical applications"
   ... Developing and implementa charta of comprehensible decision-making criteria
   ... Central Information pool for strategic documents of results for decision-making (management reports, internal audits, etc.)

In particular, the interviews result in approximation and attitude goals, which are evident from the adjectives used such as "better" or "higher". With regard to the goals, different areas can be differentiated, which differ in terms of their impact. Although a fundamental solution orientation for systemic approaches is still vague, it has a fundamentally positive connotation within the target group.

3. Path for a systematic transformation model to increase the implementation of an ISMS
   The creation of a culture of innovation with operational implementation of known goals and long-term desired changes can fit through the exemplary representation of dependency relationships in the context of the practical steps to establish an organization-wide system of risk impact assessment.

For this purpose, a triangular ratio of the following elements must be implemented:

A) Awareness/Sensitivity

B) Intention to act/behave

C) Ability to act (resources/structure and governance)

The prerequisite for successful change and transformation is the communication of opportunities and expectations, barriers and potential assessments. At the same time, the degree of open and transparent handling of risks for all parties involved is a decisive lever for making cultural aspects of leadership measurable in the sense of organizational transformation.

From these categories, the in-depth workshops were able to develop further important information for the design of learning settings for decision-makers. In order to allow municipalities to take concrete steps for the introduction of an ISMS in accordance with ISO standards of the 27xxx series, a reduction of the documentation obligations and the level of abstraction is essential. Certification of internal personnel as implementing experts does not solve the problem of nationwide penetration. Top management also needs to understand the link between IT security and other compliance requirements in order to determine appropriate resources and priorities. This is particularly evident from the discussions about module 2: "Raising awareness among employees", in which a series of training courses for experts is already planned as a fixed step. However, empirical results show that these measures often do not lead to an actual change in behavior in terms of compliance without signs of leadership [7].

That Teaching concept for ISMS CISIS12® comprises hence the recommendation followingr Complementary Building blocks at a base level "0":

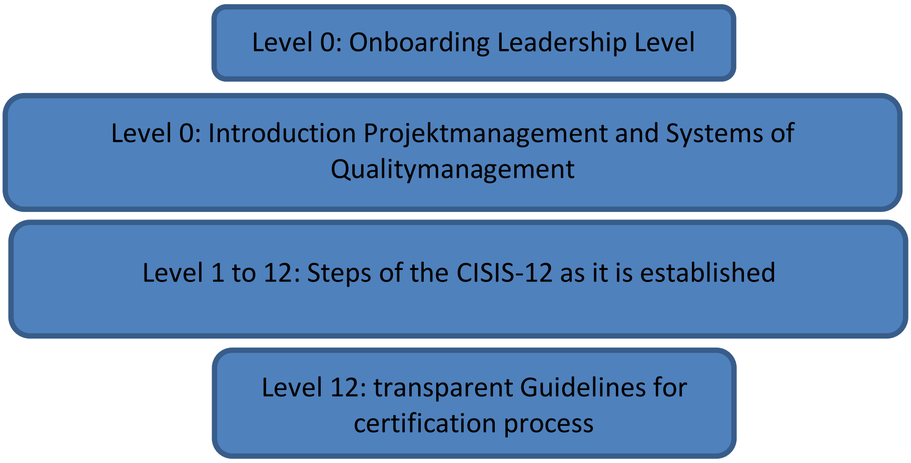
Level 0: Onboarding Leadership Level
Level 0: Introduction Projektmanagement and Systems of Qualitymanagement
Level 1 to 12: Steps of the CISIS-12 as it is established
Level 12: transparent Guidelines for certification process

Fig. 1. Additional Moduls for Teaching CISIS12®
Source: Own Diagramm based on the SHI-Concept "SECUMO" (unpublished)

Thus, a conceptual distinction is made between leadership and management in compliance, which means that specific methods would have to be developed for the respective target group in further investigations. In many small companies, but also in public administrations, this distinction between the two leadership roles has so far been little practiced.

4.2. Value

Based on the results, it can be stated in an abstract way that a two-part approach to the creation of implementation requirements for the topics of IT security, data protection and compliance can be supported in a targeted manner with game-based learning approaches. When imparting knowledge about aspects of vision, instead of passively absorbing information, the seminar participants should actively engage with learning content in order to create an opportunity for behavioral change in the first place [8].

Simulating serious gaming scenarios such as a hacker attack with the participants creates an organizational identification with concrete steps of information and action. The creation of a protected space also increases the joy of experimentation and the willingness to accept being allowed to make mistakes oneself [9].

The modularization of CISIS12® building blocks also shows the overall responsibility of all parties involved. Thus, the level of creating the necessary framework conditions such as raising awareness, forming the will to act and the competence to act must be addressed in the circle of the highest level of management. The process description and visualization of implementation components is aimed at the employees in operational implementation responsibility of the ISMS as technical experts.

Thus, a cross-cutting topic such as IT security/compliance also creates a direct connection between the working levels, which should also be anchored organizationally and made visible.

5. Conclusion

The above remarks show that municipalities are well aware that technical and organizational measures to protect them from cyber attacks are an urgent concern, as there is a high risk potential without an integrated information security system in the organization. However, the empirical surveys show weaknesses in the determination of concrete steps and meanings of compliance or risk management. Complex processes can therefore only be combined with a created culture of values of security aspects in digital work, which already addresses one aspect of the idea of digital transformation.

In the teaching of competences, it has been shown that it is not enough to leave the modelling of data and information models to a few experts. Even hiring external consultants does not create the necessary culture of compliance. Rather, modularized seminar units in game-based learning help to make the activities of the work areas comprehensible for the participants and to work out the process flows collaboratively with predefined modules of the ISMS CISIS12® and to visualize meaningful visual model adaptations at a uniform level of abstraction. This enables a new quality of participation across disciplinary and organizational boundaries. In addition to the established ISMS, additional modalities must therefore be integrated into the overall process in the didactic mediation.

References

[1] BITKOM Resarch (2022), *Wirtschaftsschutz 2022,* https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022.

[2] BSI [Bundesamt für Sicherheit in der Informationstechnik] (2023), *Die Lage der IT-Sicherheit in Deutschland 2022,* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6

[3] IT-Security Cluster e.V. (2023), *The next step CISIS12® -Information Security Management System,* https://CISIS12®.de/wp-content/uploads/2021/06/CISIS12®-Infoveranstaltung.pdf.

[4] Häder, M., Häder, S. (2022). Delphi-Befragung. In: Baur, N., Blasius, J. (eds) Handbuch Methoden der empirischen Sozialforschung. Springer VS, Wiesbaden.

[5] Mayring, P. (2015), *Qualitative content analysis: Theoretical background and procedures,* in Mayring, P. (Ed.), Approaches to qualitative research in mathematics education, pp. 365-380.

[6] Sein, M. K. (2011): *Action Design Research,* MIS Quarterly Vol. 35, No. 1, pp. 37-56.

[7] Weber, K., & Schütz, A. (2018), *ISIS12-Hack: Mitarbeiter sensibilisieren statt informieren.* Multikonferenz Wirtschsinformatik, 4, pp. 1737-1748.

[8] Prott, F., Küchler, U., Schuktomow, R., Scholl, M. (2022), Serious Games als Lernmethode zur Steigerung der Informationssicherheit, AKWI-Tagungsband zur 35. AKWI-Jahrestagung(2022), pp 325–334.

[9] TU Braunschweig (2022), Game-based Learning, https://www.tu-braunschweig.de/lehreundmedienbildung/konzepte/game-based-learning#c695740