Proceedings of the 56th Hawaii International Conference on System Sciences | 2023

# Cybersecurity Governance – An Adapted Practical Framework for Small Enterprises

Dr. Petra Maria Asprion
University of Applied Sciences
Northwestern Switzerland
petra.asprion@fhnw.ch

Patrick Gossner
SIX Group
patrick.gossner@six-group.com

Bettina Schneider
University of Applied Sciences
Northwestern Switzerland
bettina.schneider@fhnw.ch

## Abstract

*Digitalization is advancing and the associated risks are a strategic task for enterprises of all sizes. One risk area to which small businesses often do not pay enough attention are cyber risks. Often, the governance of cyber risks is not embedded at the owner or management level. However, it is important to evaluate, direct and monitor cyber risk mitigation activities by a company's leaders or its owner. A ´cybersecurity governance framework´ for small enterprises was developed and validated by applying Design Science Research. The framework focuses on criteria that are essential for small businesses, such as simplicity of understanding and ease of use (both for non-experts). Six principles identified relevant build the common thread of the framework, which guides the main activities to be implemented: 'responsibility', 'strategy', 'cybersecurity threats and risks', 'development and change', 'conformance' and 'people, skills and competencies'.*

***Keywords*** *Cybersecurity, Risks, Governance, Guidelines, Frameworks, Small Business, SME*

## 1. Introduction

Digitalization affects all industries and enterprises, including small and micro enterprises (S&ME) on which we place a focus in this research. The target audience for are scientists, cybersecurity experts, and small and micro enterprise executives/owners.

We use the OECD's interpretation which states that micro enterprises have fewer than ten employees and small enterprises fewer than 50 employees [1]. According to Rothrock et al. [2] or Corallo et al. [3], cybersecurity risks are an essential part of business risks in today's world which must be considered, regardless of the size of an enterprise.

Governance is the approach by which the leaders ensures that stakeholder needs, conditions and options are evaluated; the aim is to ensure that balanced, agreed-upon enterprise objectives are achieved. Governance involves setting a direction through prioritization, decision making and monitoring performance, and compliance with agreed-upon direction and objectives [4].

### 1.1. Relevance

It was already shown in Symantec's report [5] that 43 percent of phishing attacks in 2015 targeted S&ME – compared to 2014, an increase of 9 percent. According to Sloan [6], this is because budget for cybersecurity is often inadequate, or cybersecurity measures are not even listed as budget items. Based on Tejada [7], the influence of technology on S&ME has boomed in the last years. The increased use of the internet of things (IoT) and the desire to be more competitive have led to companies of all sizes taking advantage of the benefits of the internet [7]. The exposure to the internet makes enterprises and S&ME more vulnerable to cyber-attacks [8]. Simanowski [9] states that the corona pandemic has given a further boost to digitization and consequently also to cybersecurity risks. The increased use of IT confronts decision makers more frequently with IT-related decisions [10]. This makes governance as an organizational perspective essential [11]. Governance is the enabler for definition/implementation of structures, policies processes and procedures. This enables both business and IT stakeholders to take responsibility and the objectives of business and IT into account [10].

According to Ključnikov et al. [12], S&ME often do not have the necessary resources to tackle cybersecurity and appropriately address related risks. There is often a lack of not only financial but also human resources with the right expertise to implement controls [13], which should usually be carried out according to the most common frameworks (Section 2.1). In addition, Sadok et al. [14] show that S&ME exposed to cybersecurity risks are not given the necessary attention by management or owners. The fact that cybersecurity measures are sometimes neglected, underlines that the governance perspective with regards to cybersecurity is not sufficiently embedded at the owner or management level. Millaire et al. [15] state that S&ME are basically exposed to the same risks as large companies; however, large companies invest a large amount of money in cybersecurity every year. The fact that S&ME lack these resources is one of the main reasons why hacker organizations have shifted their focus on S&ME in recent years [15]. In addition, often S&ME have a "It Won't Happen to Me" attitude to cybersecurity [16] - such an attitude makes them neglect the issue.

URI: https://hdl.handle.net/10125/103354
978-0-9981331-6-4

### 1.2. Research Gap

There are various frameworks available to address cyber risks also in the context of S&ME. Comprehensive frameworks such as ISO/IEC 27001:2013, the Information Security Management System [17] or the NIST Cybersecurity Framework (NIST CSF) [18] support – according to their description – all sizes of companies in dealing with cybersecurity risks. However, as we derived, these frameworks do not adequately cover the governance perspective overall and the S&ME's needs (Section 2.4) [19]. In addition, less comprehensive frameworks (e.g., FTC Guidelines [20], NIST Small Business Information Security: The Fundamentals [21]), which are outlined as more suitable for S&ME, do not cover the governance perspective. For example, the term governance is not mentioned at all in the FTC Guidelines [20]; in the framework 'NIST Small Business Information Security: The Fundamentals' [21], the term is mentioned but neither explained nor addressed. In addition, the studies available do not outline the process of implementing cybersecurity governance within organizations [22].

### 1.3. Research Method

Due to the derived lack of cybersecurity-supporting frameworks covering the governance perspective, the following research questions (RQ) were developed and methodically aligned with the process-oriented approach of Hevner & Chatterjee [23]:

1. Which cybersecurity frameworks exist, and which areas are covered (awareness phase – to find out if an existing framework can be used)?
2. What cybersecurity governance-related aspects need to be considered (suggestion phase – to suggest a solution for S&ME)?

The results of the investigation of (cyber)security-related frameworks indicated that it would be wise to develop a suitable and easy-to-use artefact for S&ME (development phase –develop an artefact); the Design Science Research (DSR) approach [23] together with the development process of Vaishnavi and Kuechler [24] was applied. For RQ1 and RQ2 a systematic literature review (LR) was performed based on Hart [25]. In the LR, the first step was to define the research language (English); then keywords and keyword combinations (cybersecurity governance etc.) and relevant databases (ACM Digital Library, Google Books, IEEE, ScienceDirect, Springer, etc.) were selected and analyzed. The LR resulted in an overview of relevant cybersecurity frameworks (see Section 2.1). In addition, cybersecurity governance aspects that need to be incorporated in a governance-oriented framework for S&ME were derived based on a reconciliation of frameworks that cover certain governance perspectives (e.g., ISF Standard of Good Practice for Information Security [26], NIST CSF [18], ISO/IEC 38500 – Corporate governance of information technology [27]). To create a sufficient cybersecurity governance framework for S&ME, a systematic analysis of (cyber)security-related frameworks was performed (Section 2.4). Furthermore, to develop the new artefact, the FTC Guidelines [20] were selected as 'baseline' framework and extended or adjusted to adequately include the governance perspective. The developed governance-focused framework was then evaluated in expert interviews. Appropriate adjustments were made based on the evaluation results.

## 2. Framework Clustering

There are various frameworks that support companies in dealing with cybersecurity. The purpose of this section is to compare as relevant identified frameworks with the leading framework NIST CSF and derive relevant governance principles and activities.

### 2.1. Selection

The criterion for selecting suitable frameworks was their applicability to S&ME. To be able to assess the applicability for S&ME, information from the framework providers in which they claim the applicability of their framework as well as secondary recommendations (consulting companies ("grey papers"), scientific articles with contributions regarding S&ME applicability (very rare)) and results respectively experiences from experts derived from the interviews as well as further discussion (e.g., evaluation interviews) were analyzed. Due to the relation of this reseach to the EU H2020 project ´GEIGER´ (project.cyber-geiger.eu, [28]) and as the (first) evaluation of the framework was planned in the context of the pilot-phase in Switzerland), two Swiss-specific frameworks developed explicitly for S&ME were included in the analysis. As a result, the following frameworks were selected for a first clustering (listed in alphabetical order, the numbers are used for the clustering in Figure 1):

1. Center for Internet Security (CIS) Controls (Implementation Group 1 (1a), 2 (1b), 3 (1c)) [29]),
2. COBIT Prof. Guide for Information Security [30],
3. COBIT Transforming Cybersecurity [31],
4. COBIT Cybersecurity for Small and Medium-sized Enterprises [32],
5. FTC Guidelines [20],
6. ICT Switzerland [33],
7. ISF Standard of Good Practice for Information Security (fundamental requirements (7a), fundamental & specialized requirements (7b)) [26],
8. ISO/IEC 27001:2013 – Information Security Management Systems – Requirements [17] and ISO/IEC 27002:2013 – Code of Practice for Information Security Controls [34],

9. ISO/IEC 27032:2012 – Guidelines for Cybersecurity [35],
10. NIST Cybersecurity Framework [18],
11. NIST Small Business Information Security: The Fundamentals [21],
12. SIFMA Small Firms Cybersecurity Guidance [36],
13. Swiss Cyber Defense DNA [37].

## 2.2. Clustering

The frameworks selected (Section 2.1) are different in terms of coverage, depth of coverage, and understandability; therefore, certain criteria are required for the comparison. Figure 1 shows the result of the clustering in a four-field matrix, according to the criteria 'Understandability' (y-axis) and 'Extent' (x-axis). As S&ME usually do not have cyber specialists within the company [15], the understandability and a manageable extent (comprehensiveness) of the framework is important. The two criteria are subdivided in 'Easy to understand' (requirements and explanations are understandable for non-experts) up to 'Difficult to understand' (expert knowledge is required to understand and evaluate the requirements and explanations) as well as 'Clear & concise' (important aspects are covered manageable) and 'Comprehensive' (comprehensive controls/explanations that cover the areas holistically).

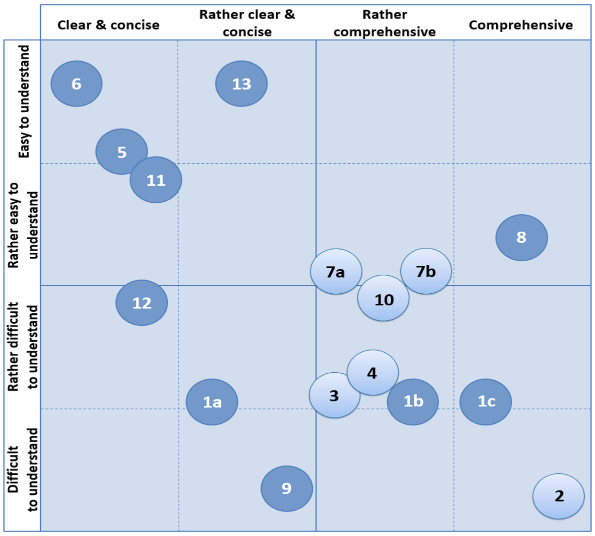


**Figure 1:** Cybersecurity Frameworks Clustering

## 2.3. Content

We compared the content of cybersecurity-related areas in the selected frameworks identifying cybersecurity-related categories and elicited a common verifiable denominator. We also wanted to outline which areas are neglected. For the comparison of the frameworks, one was selected to serve as a basis, a leading template for the comparison. The following three criteria were used for the selection of this leading framework:

1. comprehensive (Figure 1; x- axis),
2. includes a governance perspective,
3. built with a traceable structure with different functional areas which are generalizable.

Using the categorization scheme (Figure 1) and applying the first two criteria, the frameworks 2, 3, 4, 7, and 18. were selected. Considering criterion three, the NIST CSF is the most suitable to serve as the leading framework, as it is divided into five functions, 23 categories, and related subcategories, which are well suited for comparison. Further, Castañón Moats & Joyce [38] postulate that the applied functions (identify, protect, detect, respond, and recover) of the NIST CSF provide a holistic approach for enterprises to manage cybersecurity risks. For our comparison, the functions and the related categories served as a basis.

**2.3.1. Holistic Approach.** The comparison of the selected frameworks has shown that five cover to a certain extent the categories of the NIST CSF functions. We concluded that the frameworks 2, 4, 7a, 7b, and 8 cover relevant areas of cybersecurity to manage cybersecurity risks. By comparing these frameworks, including the NIST CSF with Figure 1, these frameworks can be classified as comprehensive.

**2.3.2. Common denominators.** The analysis revealed that most frameworks fully or partially cover the categories of the NIST CSF (Table 1, left column); the right column, the 'Common denominators' describes areas or sub-categories covered in most of the compared frameworks (Appendix 1 shows an excerpt of the comparison; all details can be downloaded on: (will be added after peer review). Table 1 also shows that most frameworks recommend measures that can be assigned to all five NIST CSF related functions.

**2.3.3. Neglected NIST categories.** The framework comparison has shown that the less comprehensive frameworks (Figure 1, first and second column) do not focus on the NIST CSF categories outlined in Table 2. It can be assumed that the neglected categories can be considered less important compared to the categories which are part of the common denominator.

| NIST CSF Function (F) & Category (C) | Common denominators |
|---|---|
| **F**: Identify,<br>**C**: Asset Management | Identification of business-critical information and systems |
| **F**: Protect,<br>**C**: Identity Management, Authentication and Access Control | Control and limitation of access to business information<br>Implementation of password rules |
| **F**: Protect,<br>**C**: Awareness and Training | Training on information security rules (e.g., use of email/internet) |
| **F**: Protect,<br>**C**: Data Security | Protection of wireless network<br>Implementation of web/email filter<br>Implementation of firewalls |
| **F**: Protect,<br>**C**: Information Protection Processes and Procedures | Patch management |
| **F**: Detect,<br>**C**: Anomalies and Events | Malware protection |
| **F**: Respond,<br>**C**: Response Planning | Establishing an emergency and response plan |
| **F**: Recover,<br>**C**: Recovery Planning | Backup management |

**Table 1:** Common denominators

## 2.4. Governance Components

One of the goals of this research was to define the most relevant governance principles and related activities – (easy) understandable and practicable for S&ME. Determining governance aspects for S&ME, contents describing governance aspects were analyzed.

Figure 1 shows that only five frameworks provide guidance on a certain governance level: (1) COBIT Cybersecurity Guidance for Small and Medium-sized Enterprises [32], (2) COBIT Professional Guide for Information Security [30], (3) COBIT Transforming Cybersecurity [31], (4) ISF Standard of Good Practice for Information Security [26], and the (5) NIST CSF [18]. When analyzing the corresponding content, it became apparent that governance aspects are handled differently in each framework. We worked out the following conclusions for our target group of S&ME:

- COBIT Professional Guide for Information Security [30], COBIT Transforming Cybersecurity [31] and ISF Standard of Good Practice for Information Security [26] are very extensive and high level and therefore less practical and tangible.
- COBIT Cybersecurity Guidance for Small and Medium-sized Enterprises [32] is described as low level, but still includes too extensive activities.
- NIST CSF [18] describes four governance activities (subcategories of the category Governance) but at the same time, refers to other comprehensive frameworks, including CIS [29], COBIT 5 [39], and ISO 27001 [17] for their implementation.

| NIST CSF Function (F) & Category (C) | Category Description |
|---|---|
| **F**: Identify,<br>**C**: Business Environment | The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. |
| **F**: Identify,<br>**C**: Risk Assessment | The organization understands the cybersecurity risk of organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. |
| **F**: Identify,<br>**C**: Risk Management Strategy | The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. |
| **F**: Protect,<br>**C**: Maintenance | Maintenance and repairs of industrial control and information system components are performed consistently with policies and procedures. |
| **F**: Protect,<br>**C**: Protective Technology | Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. |
| **F**: Detect,<br>**C**: Security Continuous Monitoring | The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. |
| **F**: Detect,<br>**C**: Detection Process | Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. |
| **F**: Respond,<br>**C**: Communication | Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies). |
| **F**: Respond,<br>**C**: Analysis | Analysis is conducted to ensure effective response and support recovery activities. |
| **F**: Respond,<br>**C**: Mitigation | Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. |
| **F**: Respond,<br>**C**: Improvements | Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. |
| **F**: Recover,<br>**C**: Improvements | Recovery planning and processes are improved by incorporating lessons learned into future activities. |
| **F**: Recover,<br>**C**: Communication | Restoration activities are coordinated with internal & external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs). |

**Table 2:** Neglected NIST categories

Another conclusion was that based on the governance-related contents of the five selected frameworks, it was not feasible to derive governance principles and related activities that were tangible and implementable for S&ME. Not only was the level of difficulty too high, but the information was also "hidden" in various places and there was no coherent presentation.

Therefore, to systematize relevant governance principles and activities for S&ME, we selected, after further analysis of certain frameworks or standards the model of ‘Corporate governance of information technology’ from ISO/IEC 38500 [27] as a baseline. ISO/IEC 38500 recommends six principles for a good corporate governance of IT: (1) Responsibility, (2) Strategy, (3) Acquisition, (4) Performance, (5) Conformance, and (6) Human Behavior. These six principles we adapted to define valuable governance principles from a cybersecurity perspective for S&ME. By choosing ISO/IEC 385000, we wanted to base our framework - as a structural substance - on a recognized model, or standard. For the definition of relevant activities, the governance aspects from the five frameworks (Section 2.4), as well as from the standard ISO/IEC 38500 (2008), were considered. We used the ´Evaluate-Direct-Monitor´ cycle outlined in ISO/IEC 38500 [27] when framing the relevant governance activities.

| Principle | Description Principle | Description of Activities | | |
|---|---|---|---|---|
| | | **Evaluate** | **Direct** | **Monitor** |
| **Responsibility** | Defined cybersecurity roles and responsibilities. The person with the responsibility for actions also has the authority to perform those actions. | Suitable persons who can fulfil the responsibilities based on the defined cybersecurity roles. | By means of organizational measures the possibility that the persons can fulfil their responsibilities. | Whether the persons responsible for the defined cybersecurity roles are adequately fulfilling their responsibilities. |
| **Strategy** | The enterprise's business strategy considers the current and as far as possible the future state of cybersecurity. The strategic plans for cybersecurity satisfy the current and ongoing needs of the enterprise's business strategy. | Business’ strategic development to ensure that cybersecurity will provide support for the current and future business needs. | Cybersecurity activity overall, by communicating the enterprise’s risk appetite, the cybersecurity policies, and guidelines, as well as allocating sufficient resources. | Implemented cybersecurity measures to ensure that the intended benefits are achieved. |
| **Cybersecurity Threats & Risks** | Cybersecurity risks, threats and vulnerabilities are analyzed and assessed on a regular basis. | Cybersecurity threats, risks, and vulnerabilities on a regular basis. | Cybersecurity measures are balanced between benefits, costs, and risks, in both the short and long term. | Implemented cybersecurity measures to ensure that the intended benefits are achieved. |
| **Development & Change** | Business- or IT-related process changes as well as application and infrastructure development are analyzed. Relevant cybersecurity requirements are considered in developments and changes. | IT and business process changes; application and infrastructure development with regards to cybersecurity. | Cybersecurity measures that need to be incorporated. | Implemented cybersecurity measures to ensure that the intended benefits are achieved. |
| **Conformance** | Internal and external environmental factors and trends in the business environment that may influence cybersecurity are identified and analyzed. Policies and practices are defined, implemented, and enforced. | Whether the internal and external environmental factors and trends that have an impact on cybersecurity are identified. | Policies are established and enforced to enable the enterprise to meet its obligations. | Conformance of the defined policies and guidelines. |
| **People, Skills & Competencies** | A culture that is conducive to cybersecurity is introduced and maintained. Appropriate consideration is given to employees, their skills, and competencies. | Relevant cybersecurity topics, skills and tools that are of importance to the company. | Adequate and sufficient guidance, tools, and assistance to strengthen individual competencies, skills, and awareness. | Whether the employees have the necessary skills and competencies they need for their daily work. |

**Table 3:** Cybersecurity governance principles and related activities recommended for S&ME

Table 3 outlines principles and activities based on the analysis performed: ´**Responsibility**´, ´**Strategy**´ und ´**Conformance**´ were adopted from ISO/IEC 38500 [27]. However, the description of these principles was revised to ensure that cybersecurity aspects are covered. The recommended principle ´**Performance**´ from ISO/IEC 38500 [27] was replaced by ´**Cybersecurity Threats & Risks**´. The analyzed literature showed that it is important to identify and understand the cybersecurity threats and risks a company can face and to address them appropriately [18; 26; 30; 31].

Furthermore, the principle ´**Acquisition**´ from ISO/IEC 38500 [27] was substituted by ´**Development & Change**´, since the further development or changes of applications, infrastructure, IT, and business processes must be assessed from a cybersecurity perspective, as new risks could arise [26; 30].

According to ISACA [32], S&ME need to have the necessary skills and competencies to effectively handle cybersecurity matters. Since cybersecurity requires employees with the corresponding know-how, the governing body (in most cases the owner) should be aware that external support is a possibility if the skills and competencies are not available or not retrievable within the company. For this reason, the principle ´**Human Behaviour**´ recommended in ISO/IEC 38500 [27] was replaced by ´**People, Skills & Competencies**´. Table 3 shows the cycle adopted from ISO/IEC 38500 [27] consisting of three derived governance activities that can be interpreted as most relevant.

## 3. Cybersecurity Governance Framework for S&ME (CGF4S&ME)

We abbreviated our 'Cybersecurity Governance Framework for Small and Micro Enterprises´ with '**CGF4S&ME**'. The overall objective was to develop a framework – clear and concise as well as easy to understand – for S&ME´s owners or decision makers to be able to address the existing research gap. The framework should emphasize the governance perspective and provide cybersecurity measures on an operational level to address the cybersecurity risks of this specific target group. The CGF4S&ME provides the basis for an effective, efficient, and acceptable implementation of cybersecurity measures.

### 3.1. Approach

As shown in Section 2.1 and Figure 1, there are several frameworks available that provide guidance. Whereas in Section 2.3 a leading framework was selected as a basis for comparing the selected frameworks, in this section a baseline framework suitable for S&ME was determined, which was then extended to include the governance perspective for this target group. It was crucial that the baseline framework is not overly comprehensive and does not require expert knowledge on cybersecurity for its application. Table 4 shows the evaluation criteria used for selecting the baseline framework along with a justification of the criteria (further information on the selection of the baseline framework can be found in Appendix 2).

| # | Evaluation Criteria | Justification |
|---|---|---|
| 1 | Clear and concise | The baseline framework should be clear and concise. A framework that is overly comprehensive would make it difficult for non-experts to determine relevant controls or requirements due to lack of expertise (Figure 1). |
| 2 | Easy to understand | The baseline framework should be understandable for lay-people. It is further important that the framework shows in an understandable way why certain controls or requirements may be relevant. The interviews conducted showed that different assets are relevant depending on the business model. For this reason, different cybersecurity measures are necessary. Guidance why certain measures are important is therefore helpful in determining appropriate cybersecurity measures (Figure 1). |
| 3 | Covers the common denominator | The baseline framework should cover the common denominator of most frameworks. Thus, at least all five domains of the NIST CSF are covered (see description of common denominator of most frameworks in Section 2.3) |
| 4 | Suitable to protect IT and internet facing assets | Based on the interviews conducted with the S&ME, relevant IT and internet facing assets were identified. The selected framework should contain requirements to protect these assets.<br>Note: this criterion was included to consider data privacy and protection, which is a relevant risk for S&ME. |
| 5 | Addresses the top 15 ENISA Threats | To address the most relevant threats, the 15 threats evaluated and justified by ENISA [40] are selected as classification criteria. This decision is in accordance with the results of the GEIGER project [41].<br>Note: these criteria were included considering current threat patterns (identified as relevant from ENISA and used in the GEIGER project to educate S&ME employees about threat awareness). |

**Table 4:** Cybersecurity governance principles and related activities

The results from Section 2.4 were incorporated in the CGF4S&ME. Information on the structure and format of the CGF4S&ME is provided in Table 5:

### 3.2. The CGF4S&ME Framework

Based on the criteria outlined in Table 4, from the analyzed cybersecurity-related frameworks the FTC Guidelines [20] were the most suitable framework; additionally, the FTC Guidelines provide further relevant information on their website [20] regarding how cybercriminals operate along with explanations of the importance of individual cybersecurity measures and controls. In addition, explanatory videos and quizzes are assessed as suitable for the target group of S&ME, respectively their owners. This stronger guidance in cybersecurity is particularly crucial for S&ME, as they often do not have expert knowledge available in the company. Another positive aspect is that the FTC Guidelines [20] also introduce the five NIST functions (Identify, Protect, Detect, Respond, Recover) which would thus simplify the application of the NIST CSF.

In the recommended measures as part of the guidelines, particular reference is made to the NIST function 'Protect'. It is also worth mentioning that the FTC Guidelines are an international recognized framework while other frameworks examined, such as "ICT Switzerland" or "Swiss Cyber Defense DNA", are locally limited due to language or even certain (local) terminology or legislative references.

| Area | Criterion Description |
|---|---|
| **Structure** | The CGF4S&ME should be no longer than four pages. This would also be in line with the criterion #1 of Table 4. It should be short and compact but at the same time describe the relevant aspects for governing cybersecurity in S&ME. The structure should be as follows:<br>**Page 1:** introduction of cybersecurity governance and the CGF4S&ME in general, target group, etc.).<br>**Pages 2 & 3:** governance principles and related activities.<br>**Page 4:** Introduction of the selected baseline framework. |
| **Format** | The CGF4S&ME shall be printable as DIN A5 brochure (four pages). |

**Table 5:** Structure and format of the CGF4S&ME

For this reason, we decided to refer to this source on the fourth and last page of our small but substantial CGF4S&ME and to recommend this guideline for further references and learning materials with the slogan: 'protect your enterprise proactively'.

Based on the defined structure and format (Table 5), we developed a first draft of the CGF4S&ME and evaluated it with different experts. Figure 2 shows the final framework divided into four pages and with the look and feel of a small brochure (the framework can be downloaded as a PDF document on: https://drive.switch.ch/index.php /s/d94gMopGTxDyQiq).

### 3.3. Evaluation

The developed CGF4S&ME was in a first phase evaluated by means of interviews with subject matter experts that have recognized expertise in governance, risk and/or cybersecurity. Based on their feedback the CGF4S&ME was further optimized.

The results of the first evaluation showed, the CGF4S&ME is appropriate for S&ME to govern cybersecurity.

Expert 1 – with several years of experience in the field of information risk & governance – mentioned that in particular micro enterprises might be overwhelmed by this framework and may need additional/external support. However, expert 1 further stated that all principles and activities are relevant and valid for S&ME.

Expert 2 – with over 10 years of consulting experience in the field of IT Risk & Cybersecurity – expressed the view that with the principles and derived activities described, S&ME should be able to understand what to consider in terms of cybersecurity (interview transcripts accessible on: https://drive.switch.ch/index.php/s/Xv9vC7R9uFCEBbz).

In addition, some informal reviews with supervisors of the field and local stakeholders were carried out, but not well documented. As a next phase for further evaluation, the application of the CGF4S&ME in one enterprise is planned (see section 4).

## 4. Discussion and Conclusion

As outlined in Section 1.1, coping with the opportunities and risks of digitalization is a challenge for companies and in particular for S&ME. Statistics show that an increasing number of S&ME are falling victim to cyber-attacks and since the Corona pandemic, they are even more vulnerable. The fact that S&ME are deficient in managing cybersecurity risks underlines that the governance perspective with regards to cybersecurity is insufficiently embedded at the owner or management level.

There are some frameworks that provide S&ME guidance in cybersecurity. However, these frameworks are rather comprehensive and therefore not very practicable for the target group S&ME, who have little expert knowledge, or these frameworks do not cover explicit (and easy to understand and find) the governance perspective (Section 2.2.).

The coherent selection of cybersecurity frameworks and their detailed and well-structured comparison and categorisation, especially regarding governance perspectives (Section 2) are an important contribution to the theoretical foundation of operational measures recommended in the context of cybersecurity. The focus on S&ME is particularly important for this target group, as there are hardly any contributions that support their needs and especially the governance perspective.

The developed CGF4S&ME framework (Section 3.2) consists of six relevant governance principles for S&ME. Appropriate related activities, defined according to the ´Evaluate-Direct-Monitor´ cycle adopted from ISO/IEC 38500 [27], support S&ME in the effective, efficient, and acceptable implementation of cybersecurity measures from the governance perspective.

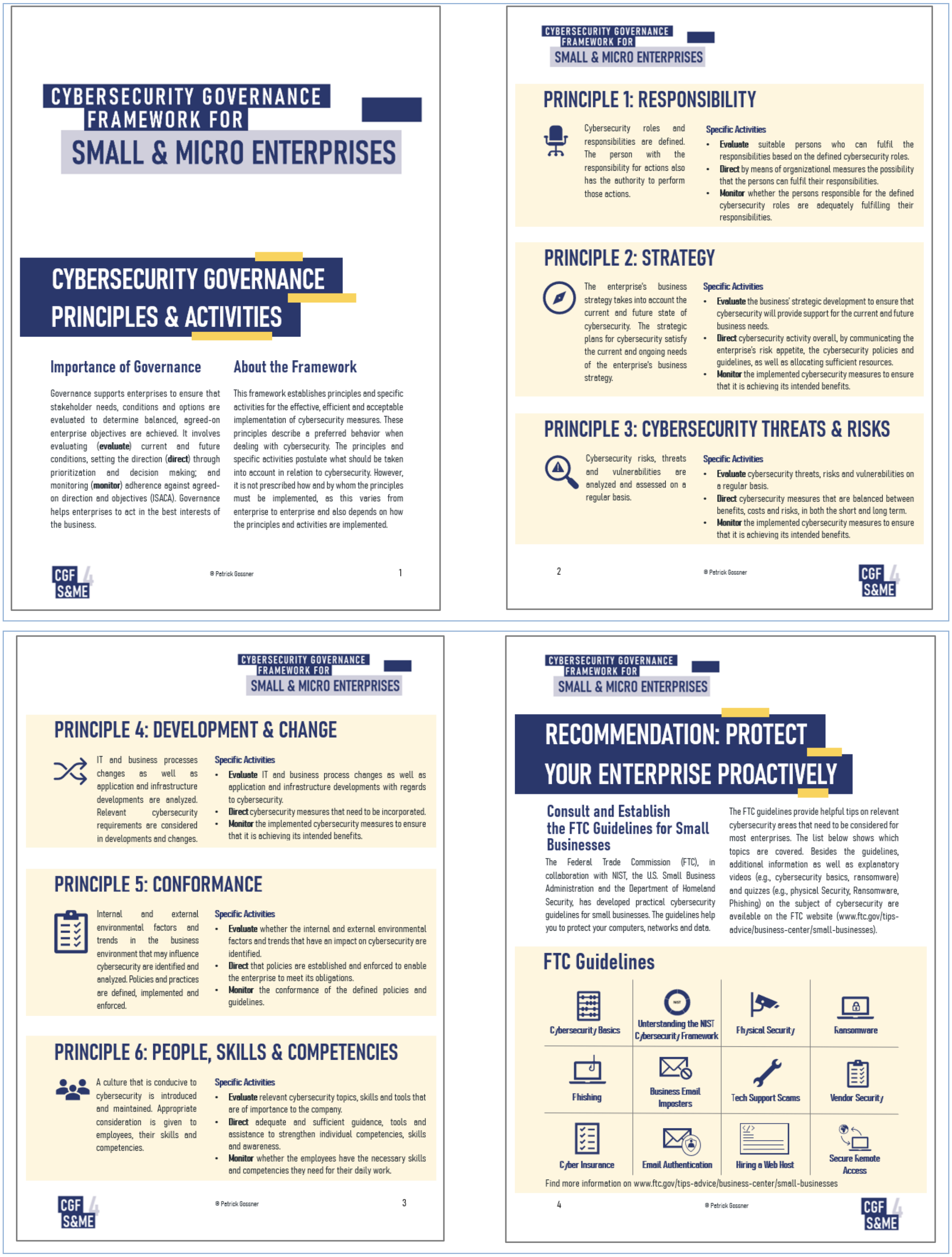
Our analysis revealed that the FTC Guidelines (Sections 3.1 & 3.2) is the most suitable framework for S&ME that provides guidance at the operational level for the implementation of cybersecurity measures and valuable learning materials unfortunately not well equipped for governance perspective.

In this contribution, we extensively discussed the application of existing frameworks for S&ME. We made comparisons between frameworks and delineated for instance the understandability per framework. A review by experts of the comparisons (Section 2) is considered as a limitation in this contribution.

As further research activities, we plan to evaluate the CGF4S&ME with users from the target group along with the monitoring and evaluation of the CGF4S&ME implementation –as part of the GEIGER project and the S&ME's target group there. [28].

## Acknowledgements

This work was made possible with funding from the European Union’s Horizon 2020 research and innovation program, under grant agreement No. 883588 (GEIGER). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.



CYBERSECURITY GOVERNANCE FRAMEWORK FOR

SMALL & MICRO ENTERPRISES

## CYBERSECURITY GOVERNANCE PRINCIPLES & ACTIVITIES

### Importance of Governance

Governance supports enterprises to ensure that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives are achieved. It involves evaluating (**evaluate**) current and future conditions, setting the direction (**direct**) through prioritization and decision making; and monitoring (**monitor**) adherence against agreed-on direction and objectives (ISACA). Governance helps enterprises to act in the best interests of the business.

### About the Framework

This framework establishes principles and specific activities for the effective, efficient and acceptable implementation of cybersecurity measures. These principles describe a preferred behavior when dealing with cybersecurity. The principles and specific activities postulate what should be taken into account in relation to cybersecurity. However, it is not prescribed how and by whom the principles must be implemented, as this varies from enterprise to enterprise and also depends on how the principles and activities are implemented.

CGF4 S&ME © Patrick Gossner 1

CYBERSECURITY GOVERNANCE FRAMEWORK FOR SMALL & MICRO ENTERPRISES

## PRINCIPLE 1: RESPONSIBILITY

Cybersecurity roles and responsibilities are defined. The person with the responsibility for actions also has the authority to perform those actions.

**Specific Activities**

- **Evaluate** suitable persons who can fulfil the responsibilities based on the defined cybersecurity roles.
- **Direct** by means of organizational measures the possibility that the persons can fulfil their responsibilities.
- **Monitor** whether the persons responsible for the defined cybersecurity roles are adequately fulfilling their responsibilities.

## PRINCIPLE 2: STRATEGY

The enterprise's business strategy takes into account the current and future state of cybersecurity. The strategic plans for cybersecurity satisfy the current and ongoing needs of the enterprise's business strategy.

**Specific Activities**

- **Evaluate** the business' strategic development to ensure that cybersecurity will provide support for the current and future business needs.
- **Direct** cybersecurity activity overall, by communicating the enterprise's risk appetite, the cybersecurity policies and guidelines, as well as allocating sufficient resources.
- **Monitor** the implemented cybersecurity measures to ensure that it is achieving its intended benefits.

## PRINCIPLE 3: CYBERSECURITY THREATS & RISKS

Cybersecurity risks, threats and vulnerabilities are analyzed and assessed on a regular basis.

**Specific Activities**

- **Evaluate** cybersecurity threats, risks and vulnerabilities on a regular basis.
- **Direct** cybersecurity measures that are balanced between benefits, costs and risks, in both the short and long term.
- **Monitor** the implemented cybersecurity measures to ensure that it is achieving its intended benefits.

2 © Patrick Gossner CGF4 S&ME

CYBERSECURITY GOVERNANCE FRAMEWORK FOR SMALL & MICRO ENTERPRISES

## PRINCIPLE 4: DEVELOPMENT & CHANGE

IT and business processes changes as well as application and infrastructure developments are analyzed. Relevant cybersecurity requirements are considered in developments and changes.

**Specific Activities**

- **Evaluate** IT and business process changes as well as application and infrastructure developments with regards to cybersecurity.
- **Direct** cybersecurity measures that need to be incorporated.
- **Monitor** the implemented cybersecurity measures to ensure that it is achieving its intended benefits.

## PRINCIPLE 5: CONFORMANCE

Internal and external environmental factors and trends in the business environment that may influence cybersecurity are identified and analyzed. Policies and practices are defined, implemented and enforced.

**Specific Activities**

- **Evaluate** whether the internal and external environmental factors and trends that have an impact on cybersecurity are identified.
- **Direct** that policies are established and enforced to enable the enterprise to meet its obligations.
- **Monitor** the conformance of the defined policies and guidelines.

## PRINCIPLE 6: PEOPLE, SKILLS & COMPETENCIES

A culture that is conducive to cybersecurity is introduced and maintained. Appropriate consideration is given to employees, their skills and competencies.

**Specific Activities**

- **Evaluate** relevant cybersecurity topics, skills and tools that are of importance to the company.
- **Direct** adequate and sufficient guidance, tools and assistance to strengthen individual competencies, skills and awareness.
- **Monitor** whether the employees have the necessary skills and competencies they need for their daily work.

CGF4 S&ME © Patrick Gossner 3

CYBERSECURITY GOVERNANCE FRAMEWORK FOR SMALL & MICRO ENTERPRISES

## RECOMMENDATION: PROTECT YOUR ENTERPRISE PROACTIVELY

### Consult and Establish the FTC Guidelines for Small Businesses

The Federal Trade Commission (FTC), in collaboration with NIST, the U.S. Small Business Administration and the Department of Homeland Security, has developed practical cybersecurity guidelines for small businesses. The guidelines help you to protect your computers, networks and data.

The FTC guidelines provide helpful tips on relevant cybersecurity areas that need to be considered for most enterprises. The list below shows which topics are covered. Besides the guidelines, additional information as well as explanatory videos (e.g., cybersecurity basics, ransomware) and quizzes (e.g., physical Security, Ransomware, Phishing) on the subject of cybersecurity are available on the FTC website (www.ftc.gov/tips-advice/business-center/small-businesses).

### FTC Guidelines

| | | | |
|---|---|---|---|
| Cybersecurity Basics | Understanding the NIST Cybersecurity Framework | Physical Security | Ransomware |
| Phishing | Business Email Imposters | Tech Support Scams | Vendor Security |
| Cyber Insurance | Email Authentication | Hiring a Web Host | Secure Remote Access |

Find more information on www.ftc.gov/tips-advice/business-center/small-businesses

4 © Patrick Gossner CGF4 S&ME

**Figure 2:** Cybersecurity Governance Framework for Small and Micro Enterprises (CGF4S&ME)

# References

[1] OECD, “Enterprises by business size,” 2019. Available: https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm.

[2] R. A. Rothrock, J. Kaplan, and F. Van Der Oord, “The board’s role in managing cybersecurity risks,” MIT Sloan Manag. Rev., vol. 59, no. 2, pp. 12–15, 2018.

[3] A. Corallo, M. Lazoi, and M. Lezzi, “Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts,” Comput. Ind., vol. 114, p. 103165, Jan. 2020, doi: 10.1016/j.compind.2019.103165.

[4] ISACA, Glossary. Available: https://www.isaca.org/resources/glossary.

[5] Symantec, “Internet security threat report,” Netw. Secur., vol. 21, no. 2, pp. 1–3, 2016.

[6] J. Sloan, “Phishing Mitigation for Small and Medium Businesses,” no. 1, pp. 1–6, 2020.

[7] L. Tejada, “Cyberattacks on Small Business: An Escalating Problem,” Utica College, 2020.

[8] S. Bell, Cybersecurity is not just a'big business' issue, 536-539, Governance Institute of Australia, Sydney, 2017.

[9] R. Simanowski, “Die Corona-Krise pflügt unsere Gesellschaft um – und wenn es einen Gewinner gibt, dann ist es die digitale Welt,” NZZ, Zurich, 20-Apr-2020.

[10] S. De Haes, T. Huygh, A. Joshi, and W. Van Grembergen, Enterprise Governance of Information Technology. Cham: Springer International Publishing, 2020.

[11] H. K. Skrodelis, J. Strebko and A. Romanovs, “The Information System Security Governance Tasks in Small and Medium Enterprises,” 2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), pp. 1-4, Latvia, 2020.

[12] A. Ključnikov, L. Mura, and D. Sklenár, “Information security management in SMEs: factors of success,” Entrep. Sustain. Issues, vol. 6, no. 4, pp. 2081–2094, Jun. 2019, doi: 10.9770/jesi.2019.6.4(37).

[13] M. C. Holland and J. Burchell, “Low Resource Availability and the Small- to Medium-sized Retail Enterprise’s Ability to Implement an Information Security Strategy”, BMRA, vol. 1, no. 2, pp. 48–76, Jul. 2022.

[14] M. Sadok, S. Alter, and P. Bednar, “It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs,” Inf. Comput. Secur., vol. 28, no. 3, pp. 467–483, 2020, doi: 10.1108/ICS-01-2019-0010.

[15] P. Millaire, A. Sathe, and P. Thielen, “What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets,” Symantec, vol. 10, pp. 1–8, 2017.

[16] M. Wilson, S. McDonald, D. Button and K. McGarry, It Won’t Happen to Me: Surveying SME Attitudes to Cyber-security, Journal of Computer Information Systems, 2022 ,doi: 10.1080/08874417.2022.2067791.

[17] ISO/IEC, “ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements,” ISO/IEC, Geneva, 2013.

[18] NIST, “Cybersecurity Framework,” 2018. Available: https://www.nist.gov/cyberframework.

[19] A. Shahim and S. Schinagl, “What do we know about information security governance? From the basement to the boardroom: towards digital security governance”, Amsterdam, 2019.

[20] Federal Trade Commission, “Cybersecurity for Small Businesses.” Available: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity.

[21] C. Paulsen and P. Toth, “Small Business Information Security: The Fundamentals,” Gaithersburg, MD, Oct. 2016.

[22] E. Vlahu-Gjorgievska, K. Than Win, and S. Safar A Al Ghamdi, Information security governance challenges and critical success factors: Systematic review, Wollongong, 2020.

[23] A. Hevner and S. Chatterjee, Design Research in Information Systems, vol. 22. Boston, MA: Springer US, 2010.

[24] V. Vaishnavi and W. Kucheler, Design Science Research Methods and Patterns - Innovating Information and Communication Technology. New York: Auerbach Publications, Taylor & Francis Group, Boca Raton, 2007.

[25] C. Hart, Doing a Literature Review, 2nd ed. London: SAGE Publications Ltd, 2018.

[26] A. Jordan, G. Haken, and J. Creasey, “The Standard of Good Practice for Information Security 2018,” London, 2018.

[27] ISO/IEC, “ISO/IEC 38500:2008 - Corporate governance of information technology,” ISO/IEC, Geneva, 2008.

[28] GEIGER, “Solution for small businesses to protect themselves against cyber threats.” Available: https://project.cyber-geiger.eu/.

[29] Center for Internet Security, “CIS Controls.” Available: https://learn.cisecurity.org/cis-controls-download.

[30] ISACA, “COBIT 5 for Information Security.” ISACA, Rolling Meadows, 2012.

[31] ISACA, Transforming Cybersecurity. Rolling Meadows: ISACA, 2013.

[32] ISACA, Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises. Rolling Meadows: ISACA, 2015.

[33] ICT Switzerland, “Cybersecurity quick check for SME.” Available: https://ictswitzerland.ch/themen/cyber-security/check/.

[34] ISO/IEC, “ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security controls,” ISO/IEC, Geneva, 2013.

[35] ISO/IEC, “ISO/IEC 27032 Information technology - Security techniques - Guidelines for cybersecurity,” ISO/IEC, Geneva, 2012.

[36] SIFMA, “Small firms cybersecurity guidance,” New York, USA, 2017.

[37] Swiss Cyber Defence DNA, “Swiss Cyber Defence DNA.” Available: https://scd-dna.ch/#.

[38] M. Castañón Moats and S. Joyce, “A board’ s guide to the NIST Cybersecurity Framework for better risk oversight,” vol. 1, no. February, pp. 1–8, 2019.

[39] ISACA, “COBIT - Effective IT Governance at your Fingertips.” Available: https://www.isaca.org/resources/cobit.

[40] ENISA, “ENISA Threat Landscape - 2020,” 2020. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends?tab=details.

[41] B. Remmele, B. and J. Peichl, “Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro-and Small Enterprises”, The 16th International Conference on Availability, Reliability and Security, pp. 1-7, 2021.

# Appendices

## Appendix 1: Framework comparison

The following table shows an example of how the comparison was performed for the frameworks using the first three categories of the NIST Function 'Governance'. The frameworks that are considered rather easy to understand and rather clear & concise (quadrant 1) according to Figure 1 were compared with each other in the table below (all details about the comparison can be downloaded on: https://drive.switch.ch/index.php/s/YfaFg8SDS1lh0Go.

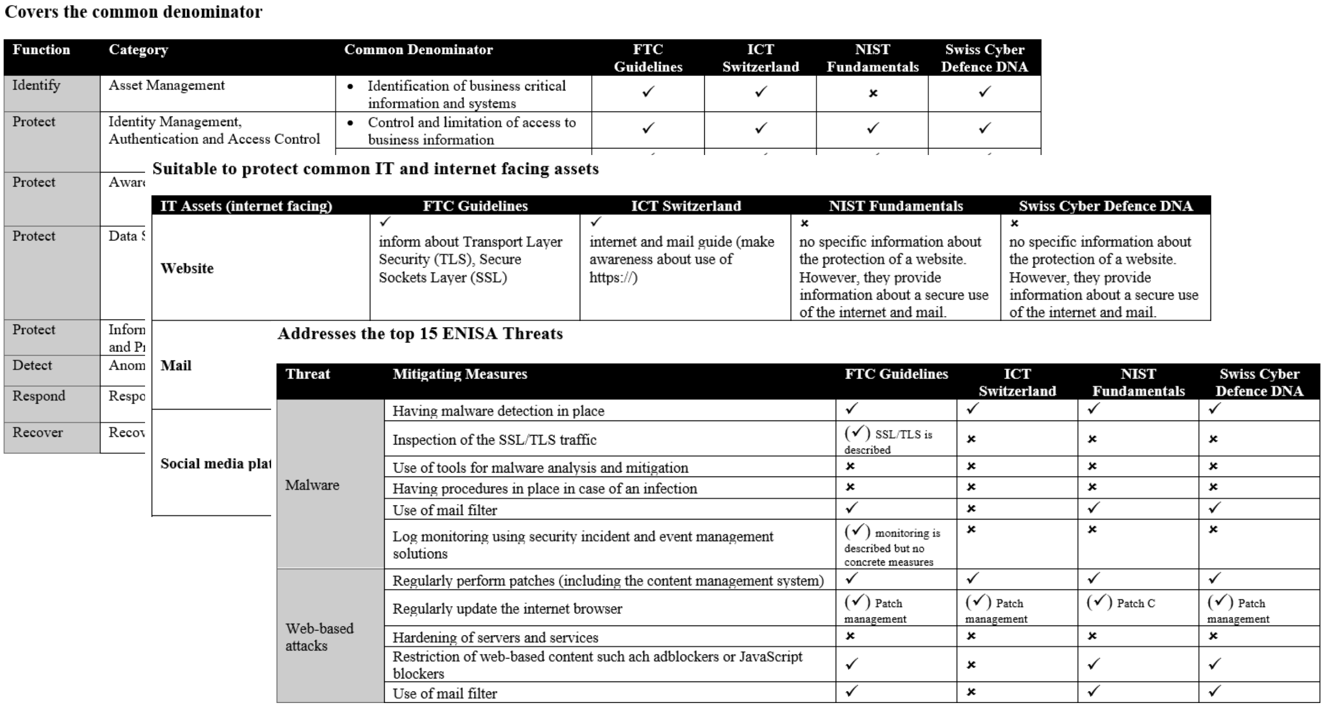
| NIST Category | FTC Guidelines | ICT Switzerland | Small Business Information Security: The Fundamentals | Swiss Cyber Defense DNA |
|---|---|---|---|---|
| **Asset Management (ID.AM):** data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | (x): business critical information & systems are identified | (x): business critical information & systems are identified | (x): background checks | (x): Keep hardware and software up to date |
| **Business Environment (ID.BE):** organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | | | | |
| **Governance (ID.GV):** policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | (x): policies and procedures for information security, define responsibilities | (x): define responsibilities | (x): policies and procedures for information security | (x): define responsibilities |

The use of colors has the following meaning:

| | |
|---|---|
| (x) | The area is partially covered by the framework |
| | The area is not explicitly covered by the framework |

## Appendix 2: Baseline framework selection

The frameworks FTC Guidelines, ICT Switzerland, NIST Fundamentals and SWISS Cyber Defence DNA met the first two criteria of Table 4. The following figure shows an excerpt of how criteria 3 'Covers the common denominator', 4 'Suitable to protect common IT and internet facing assets' and 5 'Addresses the top 15 ENISA Threats' were applied (all information can be downloaded on: https://drive.switch.ch/index.php/s/YfaFg8SDS1lh0Go).



**Covers the common denominator**

| Function | Category | Common Denominator | FTC Guidelines | ICT Switzerland | NIST Fundamentals | Swiss Cyber Defence DNA |
|---|---|---|---|---|---|---|
| Identify | Asset Management | • Identification of business critical information and systems | ✓ | ✓ | ✗ | ✓ |
| Protect | Identity Management, Authentication and Access Control | • Control and limitation of access to business information | ✓ | ✓ | ✓ | ✓ |
| Protect | Aware | | | | | |
| Protect | Data S | | | | | |
| Protect | Inforn and Pı | | | | | |
| Detect | Anom | | | | | |
| Respond | Respo | | | | | |
| Recover | Recov | | | | | |

**Suitable to protect common IT and internet facing assets**

| IT Assets (internet facing) | FTC Guidelines | ICT Switzerland | NIST Fundamentals | Swiss Cyber Defence DNA |
|---|---|---|---|---|
| **Website** | ✓<br>inform about Transport Layer Security (TLS), Secure Sockets Layer (SSL) | ✓<br>internet and mail guide (make awareness about use of https://) | ✗<br>no specific information about the protection of a website. However, they provide information about a secure use of the internet and mail. | ✗<br>no specific information about the protection of a website. However, they provide information about a secure use of the internet and mail. |
| **Mail** | | | | |
| **Social media plat** | | | | |

**Addresses the top 15 ENISA Threats**

| Threat | Mitigating Measures | FTC Guidelines | ICT Switzerland | NIST Fundamentals | Swiss Cyber Defence DNA |
|---|---|---|---|---|---|
| Malware | Having malware detection in place | ✓ | ✓ | ✓ | ✓ |
| | Inspection of the SSL/TLS traffic | (✓) SSL/TLS is described | ✗ | ✗ | ✗ |
| | Use of tools for malware analysis and mitigation | ✗ | ✗ | ✗ | ✗ |
| | Having procedures in place in case of an infection | ✗ | ✗ | ✗ | ✗ |
| | Use of mail filter | ✓ | ✗ | ✓ | ✓ |
| | Log monitoring using security incident and event management solutions | (✓) monitoring is described but no concrete measures | ✗ | ✗ | ✗ |
| Web-based attacks | Regularly perform patches (including the content management system) | ✓ | ✓ | ✓ | ✓ |
| | Regularly update the internet browser | (✓) Patch management | (✓) Patch management | (✓) Patch C | (✓) Patch management |
| | Hardening of servers and services | ✗ | ✗ | ✗ | ✗ |
| | Restriction of web-based content such ach adblockers or JavaScript blockers | ✓ | ✗ | ✓ | ✓ |
| | Use of mail filter | ✓ | ✗ | ✓ | ✓ |