Translation using DeepL.com of the article originally published in: Datenschutz und Datensicherheit - DuD, 46(11), November 2022, Springer Fachmedien, ISSN 1614-0702, pp 703-706

Eberhard von Faber

Twelve principles for systematic IT service security

Framework and principles for sustainable success

Management is a word often used in IT security. It means as much as "to do something, to take care of". Everything is "managed". Vulnerabilities, software updates, security incidents, identities, etc. There are detailed norms, standards, and descriptions of best practices on this. But little is said about management in the sense of organizing, orchestrating, and optimizing. And even less about how to deal with all the issues at the same time and to successfully exist in the internal or external market.

1 Topic

Securing IT services is the basis for the reliability of IT-supported business processes. Essentially, we also know WHAT to do (for example, Incident Detection and Response). Basically, moreover, we know HOW to do it. (There are detailed instructions on many topics).

Yet we do *not* know how to organize and orchestrate the multitude of activities. There is also little literature and material on how to save costs, make do with resources available on hand, and keep an eye on the entire supply chain. These and similar problems will be the focus of the following.

If "IT" is small and still quite manageable, a few clever heads may be enough. In more and more organizations, however, IT services are quite extensive and complex. Then you need *a system* to take care of their security. And one that not only focuses on IT security or cyber security, but also meets market and business requirements and takes into account lessons learned from quality management.

This paper is primarily aimed at IT departments or IT service providers, including cloud service providers, but is also of interest to user organizations that use third party IT services.

Prof. Dr. Eberhard von Faber

TH Brandenburg; T-Systems, Chief Security Advisor, IT Services; work areas: Security architecture, developer of ESARIS, secure IT production, IT outsourcing, process and ITIL integration; cloud, IAM;
E-mail: Eberhard.vonFaber@th-brandenburg.de

2 Situation

The security of IT services as a whole is crucial. This includes the protection of stored, processed and communicated data as well as that of all IT components and IT systems used. But how do you successfully "manage" IT service security?

There are many standards, norms, best practices and handouts. Even more, every few years they are renewed or replaced by other approaches. What of this is established knowledge? What of it is basic knowledge that does not become obsolete? The individual security measures certainly depend on the information technology and its use. The measures are therefore often very dynamic because the information technology is developing so rapidly. But what about the "management" of all these individual IT security or cyber security measures?

The search for general principles is common to all sciences. In IT security, too, principles have been formulated that provide guidance for the development and implementation of security measures and for securing IT systems. Some of these are quite old and often forgotten, although they can still be of value today. Saltzer and Schroeder's 1975 work [1], among others, contains eight fundamental principles or rules for designing and developing defensive security measures. For nearly 20 years, larger organizations have been designing their information security management systems (ISMS) according to ISO/IEC 27001 [2]. As of 2015, NIST has published a simple but comprehensive framework in the form of the "Cybersecurity Framework" [3]. And these are just examples. For an overview, see [4].

So far, concepts predominate that are available in the form of monolithic documents. SABSA [5] and ESARIS [6] are notable exceptions. Ordered lists of aspects and measures, which are to be implemented more or less in this way, predominate. They tell us *what* we have to do. They also tell *how* we should work on individual issues. But they do *not* help us to organize and orchestrate the multitude of activities - especially since the activities are no longer in one hand, but are distributed across the supply chain in a division of labor.

A kind of metasystem is needed: It complements the information security management system ISMS) for IT service security and helps to meet business and operational requirements while improving IT security.

3 Challenge

Sometimes worlds collide when high-ranking managers and IT security experts meet. While the security experts talk about problems, solutions and successes, the manager thinks about costs and wonders if there is a simpler way. Typical manager questions are:

- How do we get the costs (for IT security) under control? How can we reduce them?
- Who is supposed to do all this? Who is ultimately responsible for this? Aren't our suppliers responsible for that?
- What do customers/users actually demand? How much is mandatory, and what is only freestyle and could be omitted?
- What do we need the many internal guidelines and standards for? Are they really used and where and how can they be found?
- How do we control implementation? The costs for audits are already very high.
- Why is it all so complicated? We have ITIL®[1] and our IT service management processes.
- How do we ensure that security does not slow us down? We are already not fast enough.

IT security managers must be able to provide answers to these questions. Our nice individual measures, processes and IT security topics are of little help here.

From this, one could derive five requirements:

1. Realism: establish connection to IT business, industrialization of IT and standardization,
2. Business administration: provide approaches to cost and complexity reduction,
3. Customer focus: thinking in terms of IT services and understanding and meeting the needs of user organizations,
4. Collaboration model: actively manage division of labor in the internal and external supply chain,
5. Complexity mastery: leveraging architecture, use classification/organization schemas, structures, and models for better IT security.

The vast majority of approaches to IT / cyber security do not take these aspects into account. Perhaps it is not their task either. But IT security is part of IT, and IT is also only a means to an end. Everything is ultimately about success in the company's core business or the proper completion of the business mission in other organizations. Aligning IT security or cyber security with requirements such as the five mentioned is therefore the basis for sustainable success.

4 principles

What if we had a few principles that a management system for IT service security should be built on – independent of the specific individual measures for IT security and the current challenges or gaps in our solutions?

Here is a suggested set of twelve principles by which an IT service security management system should be built:

1. Corporate standards:

Each organization requires its own documents (standards for IT service security) that define procedures and measures to be implemented or applied on a mandatory or rule-based basis. All security mechanisms and functions, as well as actions for implementation, control, monitoring, etc., are documented uniformly in the form of measures, as facts rather than action-oriented or in the form of requirements.

Rationale: independency, consistency and clarity on the validity of the standards to be implemented without room for interpretation.[2]

2. Standardization:

The documents (standards for IT service security) should take over proven information from other norms, standards, handbooks and the like, but organizations should adapt the information to their own operational requirements, develop their own representations and strive for standardization.

Justification: The own representation or adaptation facilitates the implementation and should be done with the aim to advance the standardization. Standardization is an indispensable success factor because it makes efficiency, cost reduction and quality increase possible.

3. Documentation Hierarchy:

The documents (standards for IT service security) are organized hierarchically. General guidelines are gradually refined to detailed, technical instructions. Each document belongs to exactly one level (layer) in the hierarchy. There are no mixed documents.

Rationale: Systematic refinement ensures quality, completeness, and consistency; documents each serve different purposes and inform different audiences; mixing purposes and audiences complicates creation, use, and maintenance.

4. Dual use layer:

The documents (standards for IT service security) of a middle hierarchy level (orchestration layer) serve not only as specifications for internal implementation. They are also used as information for users and for agreements with them. They are also used as a basis for agreements with partner companies and suppliers.

[1] "ITIL" and "IT Infrastructure Library" are registered trademarks of Axelos Limited; all rights reserved.

[2] One might wonder why documents or standards are mentioned so often here and in the following. In larger organizations, one can only rely on things that are documented. Documentation also increases quality because things are then really thought through.

Justification: Users bear the business risk and require information on IT security. This information must not deviate from the internal regulations that are implemented. Services from suppliers must meet expectations; however, suppliers are responsible for the specific implementation themselves.

5. Attainment and Fulfillment:
Defined procedures ("Attainment") must be used to ensure and monitor with reasonable effort whether the standards are being implemented and complied with. Furthermore, procedures ("Fulfillment") are required to check whether the implemented standards meet the requirements that arise from the respective business environment of the users and, if necessary, are (to be) contractually agreed. Two procedures are therefore required for compliance (compliance).

Justification: Only by combining "Attainment" and "Fulfillment" can industrially produced and appropriately secured IT services be provided in a way that is appropriate for the market and users.

6. IT related classification schema:
The documents (standards for IT service security) of the middle level (orchestration layer) and below are organized according to a schema based on the technical and organizational reality of the information technology or the IT services provided (and not according to IT security).

Justification: The IT organization (and not IT security experts) is primarily responsible for implementing IT security measures in IT services. IT security is only one quality feature among others and cannot shape the processes. Security-related classification/organization schemas are not understood, are of little help, and cause considerable frictional losses.

7. Modular specification:
Descriptions with the character of directives in the documents at the middle level (orchestration layer) and below are written in modular form throughout. Areas are divided for example into topics, which in turn are detailed by individual measures and specific implementations. There are specifications for the structure of the documents, wording (diction) and document IDs.

Justification: End-to-end modularity is the basis for standardization and necessary to reduce costs for any changes and to maintain flexibility, which is one of the indispensable criteria for success, especially in the dynamic world of IT. In addition, modularity is the basis for assigning responsibility and thus the key to a functioning division of labor in the internal and external supply chain. A functioning division of labor also has a cost-reducing effect. Specifications for documents facilitate their use.

8. Technology and Practices:
The documents (standards for IT service security) are roughly divided into two groups: A) those that describe measures that are implemented in or with IT components and IT systems, and B) those that describe measures for ensuring that the measures in the first group are implemented and that this is verified in terms of correctness and effectiveness.

Justification: In the interest of effectiveness and efficiency, procedures, processes, and practices (Group B) must be standardized as much as possible and uniquely applied to all IT components (Group A).

9. Secured by Definition:
Processes and practices related to IT security are integrated into the processes and practices of developing, deploying, monitoring and updating IT and IT services. This applies if IT and IT security activities are related, involve the same IT components, or the processes and practices share objectives, mission, and the like.

Reason: Activities running in parallel increase complexity and lead to errors. IT security measures are implemented primarily by the IT organization (and not by IT security experts). The definition of security-specific (parallel) processes increases the coordination effort and poses the risk of responsibilities that are not clearly defined and separated from one another.

10. Maintenance system:
The documents (standards for IT service security) must be made available centrally in a library. An editorial team ensures that the standards for IT service security are consistent, of high quality and up-to-date.

Justification: The high complexity requires an organizing and always available supporting hand. For this, organization and processes with responsibilities, etc. must be defined.

11. Enforcement Framework:
In addition to IT service security standards, the organization needs an operational information management system (ISMS) that provides the necessary resources, clarifies basic procedures, creates an enforcement schema ("governance"), and sets basic guidelines for information security.

Justification: These issues need to be addressed fundamentally and independently of IT service security.

12. Endorsement framework:
External sources such as laws, regulations, norms, standards, handbooks, manufacturer information and the like are extensively used when developing and updating documents (standards for IT service security). If these external sources are requirements that potential users must fulfill and therefore demand (will demand) from the IT service provider, an analysis should be carried out and documented in advance to determine IF the organization's own documents (standards for IT service security) fulfill the requirements relevant to the IT service provider.

Justification: This forward-looking approach is a prerequisite for being able to meet user requirements ("Fulfillment"), which in an industrialized environment requires making it an internal standard at an early stage and implementing it accordingly ("Attainment").

Why is there talk of principles? We are talking about a metasystem. The principles are independent of the IT services [4] to be protected. They also abstract from topics and security aspects. It is solely about:

1. how a variety of activities can be organized and orchestrated,
2. how effort and costs are minimized and

3. at the same time, the implementation of IT security can be facilitated as well as
4. how this can be achieved along entire supply chains, so that user requirements in particular are also taken into account.

These are requirements from market and business management and quality management. For the objectives and further background information, see also [6] and [7].

5 Implementation

The "management" of IT service security should be carried out using a "system" and not focus on individual symptoms or problem areas of IT security. It is about a kind of meta-system that integrates the tasks in the many subject areas and allows them to be orchestrated.

Managers are used to constantly changing the organizational structure and initiating firefighting projects to solve "current" problems.[3] Also, they are often very reluctant to introduce a "new system" to bring about fundamental change. Why? They are afraid to go different ways than the other managers. Orientation to the average, however, can only produce ordinary results.

It is sometimes difficult for them to understand that the effort (and therefore the risk) of introducing new processes is relatively small, while the savings and gains from better customer focus can be very large.[4] Therefore, it is important to implement the "new system" as a series of discrete projects. Structuring in principles and modularization in general help enormously.

Well understandable justifications must also be provided in each case: What are the goals and effects? It must be made clear that problems are fundamentally solved, i.e. sustainably. The usual managerial measures "work harder", "check more often", and "temporarily increase resources" should be rejected and it should be explained that one can do without them. The system or its implementation is also largely self-financing. Management support is therefore needed more in terms of objectives, which means that management endorses activities to achieve them. Many projects can then be implemented without major decision-making and plans. Simply do it! The risk is manageable because we want to make it simple. If such principles are implemented correctly, success is programmed.

Literature

[1] Saltzer and Schroeder: The Protection of Information in Computer Systems; Fourth ACM Symposium on Operating System Principles (October 1973), Revised version in Communications of the ACM 17, 7 (July 1974); revised April 17, 1975.

[2] ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements

[3] NIST (National Institute of Standards and Technology): Framework for Improving Critical Infrastructure Cybersecurity; Version 1.1; April 16, 2018; https://www.nist.gov/cyberframework

[4] Eberhard von Faber: IT und IT-Sicherheit in Begriffen und Zusammenhängen, Thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen; Springer-Vieweg, 2021; ISBN 978-3-658-33430-7, https://doi.org/10.1007/978-3-658-33431-4

[5] John Sherwood, Andrew Clark and David Lynas: Enterprise Security Architecture, A Business-Driven Approach; CRC Press, Boca Raton, 2005, ISBN 978 1 57820 318 5, 611 pages.

[6] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond, ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers, 2017, ISBN- 978-3-658-16481-2, https://doi.org/10.1007/978-3-658-16482-9.

[7] Eberhard von Faber: On the Future of IT Security Management in the Face of Changing Technology and Service Delivery (A Discussion Paper); https://zero-outage.com/opinion/on-the-future-of-it-security-management-inthe-face-of-changes-in-technology-and-service-delivery/; translation of the article published in: Datenschutz und Datensicherheit - DuD, 45(10), October 2021;

Deutsche Version (German version):
Eberhard von Faber: Zwölf Prinzipien für systematische IT-Service-Security, Rahmen und Grundsätze für nachhaltigen Erfolg; in: Datenschutz und Datensicherheit - DuD, 46, November 2022, Seite 703-706, Springer, ISSN 1614-0702, https://doi.org/10.1007/s11623-022-1687-3 (kostenloser Zugang über „SharedIt“: https://rdcu.be/cZLlM)

[3] Little of this is usually sustainable.

[4] Presumably this is because they generally do not trust such cost-benefit considerations, including their own.