Eberhard von Faber

Managing IT Service Security

Methods and Recipes for User Organizations and Providers Along the Supply Chain

Springer

Managing IT Service Security

Eberhard von Faber

Managing IT Service Security

Methods and Recipes for User Organizations and Providers Along the Supply Chain

Springer

Eberhard von Faber
Brandenburg University of Applied Science
Brandenburg, Germany

ISBN 978-3-031-55532-9 ISBN 978-3-031-55533-6 (eBook)
https://doi.org/10.1007/978-3-031-55533-6

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Ensuring the IT security or cybersecurity of IT services can be a complex undertaking. Adequately assessing the level of IT service security achieved is no less so. The larger the IT production and the more diverse and complex the IT services, the more confusing these tasks become.

People do not want to read extensive documents that mainly contain information that is not relevant for them. Yet, in practice a lot of documents are required to instruct employees on how to care for IT security in their respective work areas. But how to manage all these details so that they are correct and consistent?

This book is for IT service providers (including IT departments), user organizations (including business units) as well as for manufacturers, vendors etc. insofar as the IT is rather complex.

This book is about managing IT security, or more precisely, managing the security of IT services in terms of organization, orchestration, and optimization.

The primary task of an organization's management is to create the necessary conditions for defined goals to be achieved. Managers instruct experts to do their work. Primarily, however, they have to CREATE THE NECESSARY CONDITIONS that enable employees to WORK EFFECTIVELY (i.e., to achieve common goals) and EFFICIENTLY (i.e., with the least possible use of resources and time). In larger organizations, one creates the necessary conditions for effectiveness and efficiency by first creating organizational forms such as processes and divisions of topics and task areas. This is precisely the goal and content of this book.

The book describes a management system called ESARIS (Enterprise Security Architecture for Reliable ICT Services). This metasystem or security architecture builds on more than a decade of day-to-day experience in the IT industry with multi-national customers. The methods and recipes are field-proven.

The book is a compendium that compresses the complex subject matter into individual terms and their definition. This ensures, that we really get to the point. Explicit DEFINITIONS ARE PROVIDED FOR ABOUT 75 TERMS which can be used to look up a topic. FORTY-ONE FIGURES as well as ELEVEN TABLES further support orientation and understanding. Of course, detailed introductions and explanations are also given. Connections between the terms and topics are revealed by the sequence and hierarchy of the terms as well as by references and intermediate texts. The overall context is already apparent from the more general terms at the beginning. The understanding is further deepened the more details subsequent descriptions provide.

ARE YOU WONDERING what is so complicated about 'IT service security' and why it takes a book to explain how to 'manage' it? Below you will find a simple example of four types of compliance. All four are important to both the user and the IT service provider. This alone adds to the complexity. But the example also shows how they can be mastered with a bit of systematics.

WHY 'IT SERVICE SECURITY' IS MORE COMPLEX than one might think... One example:

Compliance is a trend, a must or simply something very fundamental. Because goals, targets, standards, and the like are meaningless if you do not also check whether they are achieved or complied with, i.e. you have been able to establish compliance. And without goals, targets, standards and the like, everything is arbitrary and therefore useless.

Fig. 0.1 illustrates which compliance must be checked and ensured so that an IT service (top right in red) complies with the contractual promises (in yellow on the left). There are four types or formations of target-actual pairs for which compliance must be checked. This is what the user (customer) expects and the IT service provider must establish and verify (with support from its suppliers).

We discuss all four cases one after the other in the shortness offered at this point. (Further down in the book, the terms and contexts will be explained in more detail).

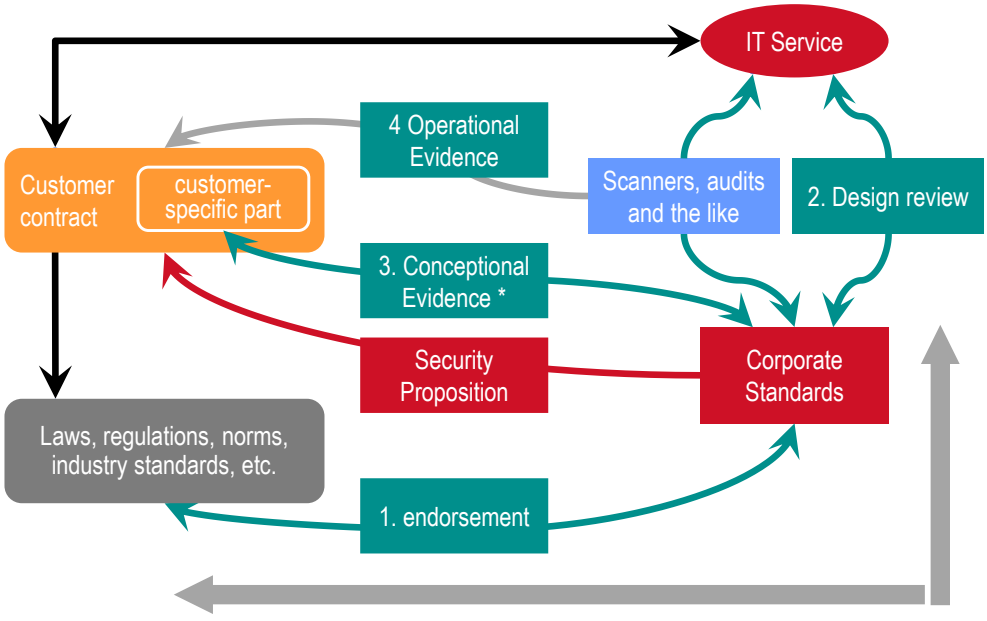

Fig. 0.1: Four ways of determining the compliance of an IT service

1. Endorsement (see Fig. 0.1): User organizations themselves must comply with laws, regulations, standards, and the like, and some of these requirements may affect IT that they do not produce themselves but obtain from an IT service provider. Following its own standards (corporate standards, see Fig. 0.1), the IT service provider ensures that the IT services are secure. The provider will therefore check in advance whether its own standards are sufficient to meet the customer's requirements that arise for it from certain laws, regulations, standards, and the like.

The user organizations (customers) receive information on the IT security of the IT services (see Security Proposition in Fig. 0.1) that are based on the standards of the IT service provider.

2. Design reviews (see Fig. 0.1): The IT service provider develops and implements its IT services. Its own standards are the basis for this and determine how they are secured. As part of quality assurance, it must check whether and to what extent the applicable standards were actually implemented during development and implementation. This is the second compliance area.

3. Conceptual evidence (see Fig. 0.1): Larger user organizations in particular often have their own ideas and requirements for IT service security. This can have very different reasons. But IT is rarely completely identical and 'one size fits it all' does not always apply in IT security either. In these cases, it must be checked whether the customer-specific requirements can be met. This third form of compliance is only relevant in the case of customer-specific contracts or contract clauses.

4. Operational evidence (see Fig. 0.1): If everything is correct up to this point, the contract can be signed and the IT service provider can deliver the IT service. However, IT is constantly changing, the threat situation may also change, and the IT security measures must be continuously checked to ensure that they are sufficiently effective. Therefore, both the IT service provider itself and the user organization need and expect appropriate checks and reports on their results, usually in the form of security reports. These compliance checks are usually highly automated.

The four cases have only been sketched cursorily here. They are intended to show that there are various sources (for specifications) and several types of verification (of compliance). This alone is one of the reasons for more complexity in securing business IT services and their use.

However, the example is also intended to illustrate how this book uses systematics and terminology to create order, illuminate relationships, and provide concrete support for implementing IT service security successfully and with an eye for the essentials.

All 41 figures and possibly further supplementary material are available as a PowerPoint file. Contact the author by email or via LinkedIn.

The author has decided to use the concept of his books from 2021 and 2023:

- The core of information on a topic is given by means of term definitions. These are sorted hierarchically. Subsequent ones expand and refine already explained terms and contexts.
- By means of giving a definition not only a term but a 'matter' is explained, sometimes also fully explaining other terms that are important in this context.
- The individual explanations of terms are lexicon-like, i.e. mostly short and precise. This suits readers who are used to processing snippets of information, which they then piece together step by step.
- Each topic is accompanied by generally understandable introductions, which above all provide the context that makes it easier to establish a practical connection and invites to explore the possibilities for own use.

Structuring by terms has great advantages:

- It facilitates the exchange of information enormously. If one uses these terms, it is ruled out from the outset that experts spend valuable time on a long discussion only to finally find out that (once again) they have completely missed each other's point because everyone started from a different situation or constellation.
- Most of the terms used in this book are not common property. Rather, they were chosen by the author to divide the complex undertaking of 'IT service security' into individual small sections, to make it manageable and easier to understand.

Boldface is used for the term when it is explained at this point. *Italics indicate* that the term is explained elsewhere. SMALL CAPS are used for emphasis. If the reader is unable to find a particular term definition, it is recommended to consult the index at the end of the book.

Since the eBook is also available by chapter, references to sources and further reading are repeated from time to time. This is also deemed necessary because sometimes even unmarked self-citations are considered problematic. This book contains earlier text and illustrative material of the author.

Thank you very much if you HAVE already BOUGHT this book. It takes a lot of work to write such a book. Feel free to recommend the book to others if you find it useful. But PLEASE DO NOT copy it.

IS SOMETHING MISSING? DO YOU DISAGREE? Send me an email at ESARIS@t-online.de!

Eberhard von Faber

Table of Contents

About the Author

Eberhard von Faber studied electrical engineering and physics and earned his doctorate in the field of semiconductor physics. He is Chief Security Advisor, IT Services, at T-Systems and a part-time professor for IT security.

In January 1992, he began his career in the industry as a security systems developer. He developed CryptCard, the world's first hardware-based security system for notebook computers including all highly integrated electronical chips.

He then worked in various fields in security engineering, security consulting and the security evaluation of products and solutions. In 1995/1996, he demonstrated that the DES cryptographic algorithm can be broken by a brute-force attack using hardware he designed for this purpose. It was then decided to replace the algorithm in all components of card-based payment systems.

Eberhard has long been active as an evaluator. Specifically, he investigated the security of chips used worldwide in payment systems. He developed some sophisticated, mostly invasive new attack techniques. He is the principal author of an international standard for integrated circuit security. He built up the business of evaluations according to ITSEC and later Common Criteria, and headed the internationally active, commercial security testing laboratory.

As head of staff of a business unit of an IT group specializing in IT security services and solutions, he was responsible for strategy and business development. He then worked as Offering Manager for IT Security and later as Executive Consultant.

At the end of 2010, Eberhard took on the task of improving and completely reorganizing the IT service security at T-Systems. He developed dozens of new methods and standards and improved transparency, effectiveness, and efficiency. This resulted in the *ESARIS* security architecture.

Eberhard is the author of several books and is responsible for more than 170 publications and conference contributions. His special interest is the efficient execution of IT security, the implementation in complex delivery networks and the relationship between customers and IT service providers.

Editorial Note

Chapters 1-6 and 9 are modified translations from the author's German book "IT-Service-Security in Begriffen und Zusammenhängen" (ISBN 978-3-658-41932-5). The translation was done by the author with the help of DeepL Translator from Cologne, Germany (https://www.deepl.com/translator).

1 The Environment

Is securing IT services really that complicated? To understand why, we look at an example from another industry. Fig. 1.1 shows two airplanes. On which one do we need to do more for safety/security? For the Airbus A380, of course (shown on the right). And why? Not because the two-seater (left) is much cheaper and offers fewer options than the world's largest commercial aircraft. The A380 must do much more! That is why the safety/security measures are incomparably more extensive. Examples of this are included in the figure. The same applies to IT and *IT services*: The higher and farther you fly, the greater the demands on IT security. But much more has changed in IT than just size and reach. This introductory chapter explains what it means to provide IT services instead of selling products, how today's IT including cloud and container works in principle, and why supply chain complexity not a side issue. It is briefly described how modern IT services are deployed and maintained, how the user organization comes into play and how IT security is related to IT service management.

Fig. 1.1: Case study comparison of two aircraft

E. von Faber, *Managing IT Service Security*, https://doi.org/10.1007/978-3-031-55533-6_1

The 'Cloud' began with the customer promise of high standardization and rapid deployment. 'Simplicity' and 'IT as if from a power socket' were buzzwords. The image of an opaque cloud hovering over everything suggested that it would not be necessary to know the details. Today, however, the reality is completely different. The technology is highly complex, and the options are more diverse than ever.

At the same time, the demands on IT and also on IT security have increased. Both factors have to do with the fact that IT is being used in ever larger areas of application. Whereas it was initially limited to a few central business applications in the 'back office', IT applications soon became mobile, networking increased greatly, and the centralization of data storage and processing experienced a renaissance, and finally these models captured ever new areas of application.

All this has not made IT security simpler, but initially much more complex. Today, attempts are being made to combine and centralize IT security functions in cloud-based security solutions in order to reduce complexity for users. However, this does not fundamentally change the fact that the complexity still exists. The industrialization of IT, however, is leading to a major shift in responsibilities within the supply chain or supply network. As a result, each party can focus on specific IT security problems and issues, depending on the current technology and the associated division of labor. However, in terms of a comprehensive, end-to-end approach, important problems and issues remain: Which set of individual IT security solutions is adequate for a given application, and which parties should provide which services? The selection of IT security solutions is not made any easier by the constant progress and change in the market and does not answer the question of who is responsible for the IT security of the overall construct.

How should the security architecture be designed? The information technology (IT) in a data center usually does not show what it is used for and what it accomplishes. And each device in turn consists of many components, mostly in the form of software and therefore hidden from view. IT users see their screen and keyboard along with the mouse. How much is done by the local computer itself and what is done remotely in the data center is often hardly apparent. IT is very abstract. When it comes to safeguarding this abstract world, knowledge of the logical structure with chains of effects and processes is necessary. In the following, we want to develop the imagination and structure the world of IT a little.

1.1 Subject: IT as a Service

It was not until the beginning of the 2000s that there was a shift towards 'IT as a service'. What is meant by this? Whereas the IT departments of even large companies initially still supplied IT components (products) to install and operate them themselves or with outside help, today an increasing proportion of IT is no longer

purchased, but paid for. The service concept is gaining ground, and this has far-reaching consequences. Unlike a product, production takes place at the same time as use. *IT services* are provided continuously; the type of production is different. IT products, and thus also the IT systems made from them, have predominantly fixed properties at the time of installation and also afterwards, which they basically also retain [1]. In the case of 'IT as a service', on the other hand, it is primarily the function that is purchased. The underlying realization (technology) can change. Since service contracts often run for several years, it is likely that changes will be necessary and will take place.

But one very consequential difference concerns the loss of transparency and influence [2]. Risks regarding IT security are associated with any type of service delivery. In order to make a business decision about whether the user organization is willing to accept them (or improvements are needed), one needs knowledge about the security level.

Therefore, there are two real issues [2]:

A) the existence of unacceptable risks (i.e., lack of IT security) and

B) lack of knowledge about existing risks or the integrated security measures (lack of trustworthiness, or insufficient assurance).

Using IT services produced and provided by third parties may well improve IT security (A), but the knowledge on the part of the *user organization* (B, the 'trustworthiness' or 'assurance') decreases system-inherently if no systematic countermeasures are taken. Now this situation is relatively 'new' at best for IT. Outsourcing to third-party service providers began much earlier in other lines of business. The commercialization of aviation is a good example. Here, too, by the way, the passenger (user) bears the greatest risk, while only the manufacturer of the aircraft and the operator (the airline) can ensure that the risks are small and remain controllable. It is the same with IT services. However, the governments of leading countries have ensured with very rigid regulations that aircrafts crash extremely rarely. Unfortunately, the same cannot be said of IT. In general, the quality of IT is much poorer. This also applies to IT security.

Can *user organizations* rely on the IT security of third-party services at all? Of course, because larger, specialized IT companies can usually ensure quality better than smaller teams with limited resources. However, this does not mean that user organizations can use third-party services unconditionally without any precaution and rely on their IT security. They need to know and assess the risks. And they need ways to influence IT security - at least through their purchasing decisions by choosing one service over another.

The term ‘security measures’ is extensively used in this book. That is why a definition is given now before proceeding with considering IT in general.

Security measure

> Precautions taken to reduce risks as well as to identify and comprehend any circumstance that may indicate risks (i.e., the possible loss of confidentiality, integrity, or availability). Security measure is synonymous with security control. Security measures can be administrative, organizational, process-related, technical, or legal in nature.
>
> Checking and monitoring whether other security measures, for example technical security measures, have been implemented and are effective should also be defined as a security measure. Only then will a complete catalog of security measures be created.

In very simplified terms, nowadays ‘IT’ looks as shown in Fig. 1.2. The very largest part of IT is located in data centers. Sometimes the data center is operated by the *user organization* itself (left), but usually by *IT service providers* (on the right). The ‘cloud’ also consists of computers located in data centers. In all possible cases, users or their end devices are connected to the data centers via networks. This enables them to use the *IT services* offered.

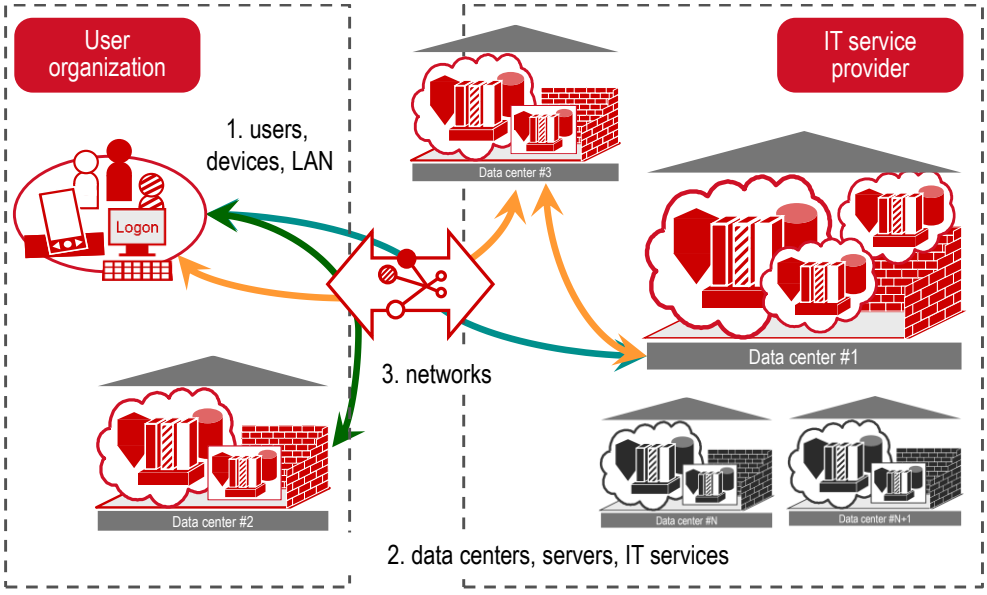

Fig. 1.2: Users, data centers and networks (basic model)

Now, finally, a few explanations of terms or definitions follow. Further explanations can be found below the term definitions.

NOTE: The following definitions are taken from the author's encyclopedia [3].

IT service (overview)

IT stands for information technology (IT). An IT service is provided over a longer period of time with the help of IT. In contrast to products (tangible goods), the benefit arises at the same time as production. A **product** is an asset (object) that has been manufactured for its intended, foreseeable use. Since the use is clearly defined a product (in contrast to a service) can in principle be specified precisely and completely.

Computing Service

Computing services comprise services for the operation of an application software (application) in a data center. In the case of infrastructure services, the *IT service provider* DOES NOT PROVIDE the application itself, but only operates it with the help of various IT and network components. Computing services essentially have three performance parameters or basic components: computing capacity (compute), storage capacity (storage) and network capacity (network).

Computing services are often simply called *IT services*. They are very diverse and differ primarily in terms of the service that the *IT service provider provides* deliver to the user or the *user organization*. The → *Service Model* classify IT services and define their most important groups or types.

Service Model

The Service Model is a characteristic of an *IT service*. There are different Service Models. Each Service Model characterizes which activities are part of the IT service and which IT components provide functionalities that are directly part of the IT service. The activities, functionalities and IT components are highly abstracted, so that roughly a dozen types or models can be distinguished.

The Service Models differ in terms of the IT components and activities for which the *IT service provider* bears responsibility. Since the IT stack is always complete and most of the activities always have to be performed, the user or the *user organization* must take care of the missing IT components and activities.

The last two explanations of terms have pointed to two realities that make IT security a complex undertaking even today:

1) Cost pressure, standardization, product success, compatibility, monopolies, and singular technologies[1] do indeed lead to standardization in IT. Nevertheless, there are many different IT services, because the requirements of the users or

[1] This refers to technologies for which there are no or only few alternatives. No fixed terminology!

user organizations are very different.[2] In many industries, IT has become a decisive competitive advantage. If all competing companies would use the same IT (the same IT services), there could be no clear differentiation through the use of IT.

2) IT consists of many function-providing parts (technical components) that are stacked on top of and sometimes next to each other. In addition, there are many supporting components for monitoring and maintenance. Very often, not all parts (components) are provided by and are the responsibility of the IT service provider. This is more often true the more specialized the business transactions or business applications to be supported are. For example, large companies bring their application software (application) or have it created by another IT specialist and/or configured specifically for them. It may also be necessary to purchase additional IT services from other IT service providers and link these to the original core service. One example is additional IT security solutions for cloud services, for example in the form of a cloud security gateway.

3) Many activities, some of them quite extensive, are required to install, integrate, operate, and maintain the necessary parts (technical components), i.e., to provide IT services with consistent quality and to deliver corresponding evidence. Various IT service providers do not offer a complete service here, so that certain activities are left to the user organization, which needs its own IT personnel for this or must commission another IT specialist. This reduction by the IT service provider can have various reasons: Business model, indication of lower prices, no own capacities, etc. However, since many of the activities are required to establish and maintain IT security, the division of labor (the *Service Model*) is an important factor for the user organization.

All this makes IT security management quite complex - even today. For the user organization, because of the diversity and specifics of IT services. For the IT service provider, this is also true in principle, but there is also the complexity of the internal and external supply chain because an IT service provider is dependent on various trades as well as many manufacturers, whose contributions must be adequately managed and integrated.

---

[2] This is not limited to IT either and also applies elsewhere, for example to safety: Cars are built from standardized components. In most cases, however, the car finally purchased differs from the many others of the same make and type. One person chooses airbags everywhere, while another buyer is fully satisfied with airbags for the driver and front passenger.