Translation using DeepL.com of the article originally published in: Datenschutz und Datensicherheit - DuD, 45(10), October 2021, Springer Fachmedien, ISSN 1614-0702, pp 691-697

Eberhard von Faber

# On the future of IT security management in the face of changes in technology and service delivery

## A discussion paper

Security measures must be adapted to the respective new information technology (IT). But that is not enough. IT and its provision and use have changed so much that traditional forms of IT security management are no longer adequate and must be supplemented. To this end, trends in IT are examined and challenges for IT security management are identified. This is done very briefly, initially in retrospect. The subsequent, more detailed analysis of current developments leads to five challenges and four concrete proposals for more quality and future security, one of which is described in more detail.

## 1 Introduction

In principle, security management works as follows: 1. understand needs, 2. analyze threats, 3. find and assess vulnerabilities, 4. design or improve security measures, 5. implement security measures, 6. verify effectiveness (including detection of attacks, etc.), 7. respond and mitigate the impact of incidents, 8. implement remediation and initiate improvements.

In addition, there are various security principles that provide guidance for the development, implementation, and maintenance of security measures. These include segregation of duties, defense in depth, least privilege, secure by design, secure by default, and many others (see [1], Chap.2.2.3). Finally, the development of IT and its architectures lead to a change in the way IT security is implemented. Following the possibilities, local solutions are followed by centralized, mostly "cloud-based" solutions. And following the necessities, the protection is shifted to the possible location of the damage: Classic perimeter protection, for example, is being supplemented or replaced by "zero trust" models, in which identity and rights are verified every time an application or IT service is accessed or used. - There is a great deal of literature on this subject.

**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

But we are still lagging behind. Some think that the situation has not improved fundamentally. So what are we doing wrong, or what should we be doing additionally? Perhaps questions like the following will help: What has changed in the field of information technology in recent years? How have supply and demand developed? What difficulties have arisen as a result? What prevents the participating parties from implementing the right things in the right way? What would need to be achieved in general?

This paper reflects, in the required brevity, on the development of enterprise IT and its protection in the past (Chapter 2). A look at the generic tasks of IT security management and the difficulties of their implementation, against the background of the special features of today's IT, first provides indications of topics that have perhaps received too little attention to date (Chapter 3). In order to arrive at more concrete proposals, we then attempt to identify fundamental changes in enterprise IT that have implications for IT security management. To this end, we make concrete proposals on how IT security management can be further developed (Chapter 4). The fourth suggestion is entirely new and is therefore dealt with in some depth in Chapter 5. At the end, there is a brief summary of the four proposals (Chapter 6).

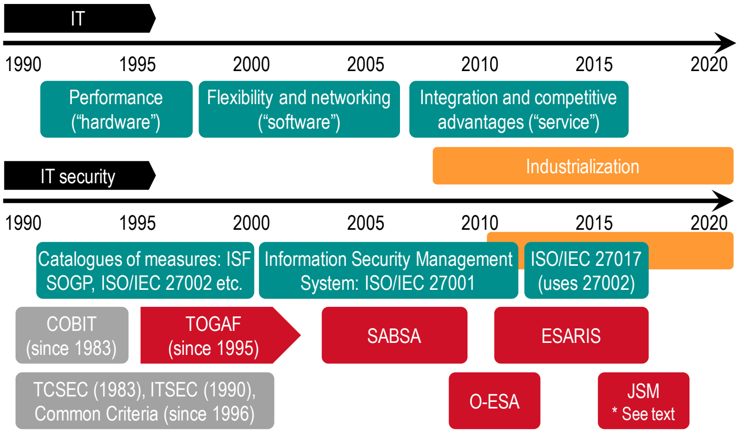
## 2 Phase 1-3: What has happened so far…

To understand the evolution of IT security and the latest challenges, it is best to look at the development and new trends in information technology (IT). Because you don't do

IT security without IT. IT security is always oriented towards the requirements of IT and its use. IT security must master challenges that arise from the way IT is constructed and used.

Figure 1 shows two parallel developments. At the top, you can see a timeline marking important phases in the development of IT. Below, the same is shown for IT security. We start around 1990, so we only go back about 30 years.

**Figure 1: Timeline of the development of IT and IT security (Source: [1])**


IT
1990
1995
2000
2005
2010
2015
2020
Performance ("hardware")
Flexibility and networking ("software")
Integration and competitive advantages ("service")
Industrialization
IT security
1990
1995
2000
2005
2010
2015
2020
Catalogues of measures: ISF SOGP, ISO/IEC 27002 etc.
Information Security Management System: ISO/IEC 27001
ISO/IEC 27017 (uses 27002)
COBIT (since 1983)
TOGAF (since 1995)
SABSA
ESARIS
TCSEC (1983), ITSEC (1990), Common Criteria (since 1996)
O-ESA
JSM
* See text

Phase 1: From today's perspective, much was still in its infancy in 1990. While the performance and universal availability of computers seem almost self-evident to us today, individual systems prevailed in those years, some of which were interconnected, but which primarily worked independently. In the 1980s, PCs supplemented central computers more than they replaced them. Even in the 1990s, the focus is on making sense of both types of systems. But performance is often the limiting factor.

The IT security standards used in this period define security functions in a generic way and describe how they are used effectively and implemented correctly and how this can be verified. The TCSEC (Trusted Computer System Evaluation Criteria), the US criteria for the evaluation and certification of IT security, especially of products, are an example of this. In Europe, TCSEC was replaced by the European security criteria ITSEC and later by the internationally used Common Criteria [2]. The restriction to products and separable systems remains. For the more comprehensive enterprise IT and its comprehensive management, catalogues of security measures of a different nature emerge, such as the compilation of best practices later published as ISO/IEC 27002 [3]. They are updated and supplemented several times, new ones are added; they are still usefully in use today.

Phase 2: By the end of the 1990s, the Internet is ubiquitous. Computers are affordable and available, and for some years they have also been in mobile use. Therefore, the focus is now less on the computer itself and more on software to support business processes and the integration of as many participants as possible or of the software on their computers, respectively. Software and networking make companies leaner and more efficient.

What does this mean for IT security? IT systems are becoming larger and more complex. Their secure design is now less important than maintaining the IT security of the overall system. The catalogues of security functions are supplemented by management systems, which should ensure the implementation and updating of the technical security functions. Among others, the later ISO/IEC 27001 [4] is created, which defines requirements for an Information Security Management System (ISMS) and is also still a standard for larger institutions today. The security architecture SABSA® (see [5] and [6]) provides templates for the development of classification schemes and systematics for the increasingly comprehensive catalogues of measures. SABSA thus pursues a similar goal for IT security as TOGAF does for IT.

Phase 3: Following the "concentration on the core business", many companies "outsourced" their IT and its operation to specialized IT service providers already in the 1990s. At the beginning of the 2000s, this trend accelerates in the direction of "IT as a service" (Service, see Figure 1). In the mid-noughties, IT makes the shift from individually used computer systems (dedicated) to shared systems (shared). This increases the utilization of computer systems and reduces costs. This period also saw the introduction of ITIL©[1] as a collection of methods for managing IT. The aim is to improve the benefits of IT, for example by minimizing downtimes and implementing any changes and improvements quickly and according to the order. All of the developments mentioned lead to an industrialization of IT provision, the hallmarks of which are standardization, modularization, process orientation and a distinct division of labor.

In line with these developments, the ESARIS security architecture is being developed. It relies on standardization to reduce the costs of IT security and on modularization to maintain the necessary flexibility. According to the principle "Secured by Definition" ([7] and [8]), the definition, implementation, maintenance and further development of measures for (technical) IT security are integrated into the IT provisioning processes as defined in ITIL or ISO/IEC 20000 [9]. The relationship between the user organization (customer) and the manufacturer (IT service provider) comes into focus. The division of labor and the management of the increasing complexity and diversity of topics are supported by architecture and diverse methods.

Meanwhile, the development of catalogues of measures continues to follow the changing technologies. The Cloud Controls Matrix (CCM) of the Cloud Security Alliance (CSA) is a good example of this (see [10]).

[1] IT Infrastructure Library®, a collection of predefined processes, activities and roles along the lifecycle of IT services, with particular attention to the operational phase. Since 2013, ITIL and IT Infrastructure Library are a brand of Axelos.

## 3 Current observations

It is in the nature of complex issues that they can be viewed from different angles and that very different focal points arise in each case. Before we look ahead, this chapter will analyze the challenges that have already arisen, but which IT security is ill-equipped to address. Table 1 shows some examples of topics that have received too little attention so far (left). The right side of the table outlines current changes that make the topic (left) a challenge.

**Table 1: Challenges for IT security management**

| Challenge | Cause/Change |
|---|---|
| **Security governance**<br>(Question of control, leadership and management) | **Diversification of service models**<br>(the functions of an IT service and the activities for its maintenance and management are increasingly being divided up in different ways) |
| | Examples of problem areas or solutions<br>Classic: Infrastructure-as-a-Service (IaaS); Monitoring<br>Newer: Management services for third party clouds |
| **Security orchestration**<br>(Question of coordination and alignment) | **Diversification of delivery models**<br>(an IT service is increasingly constructed and/or offered in different ways; applications are distributed) |
| | Examples of problem areas or solutions<br>Classic: public cloud; virtual private cloud<br>Newer: hybrid clouds; hyperconverged systems |
| **Security confinement**<br>(limit the influence of potentially insecure system components) | **Diversification in the supply market, internationalization**<br>(in particular, cloud computing services are sometimes considered untrustworthy; evidence is lacking, or legislation is contradictory; the concept of secure network is reaching its limits) |
| | Examples of problem areas or solutions<br>Classic: firewalls<br>Newer: Cloud Encryption Gateway; Cloud Access Security Broker (CASB); Secure Access Service Edge (SASE); Zero Trust Network Access (ZTNA) |
| **Security control and quality management**<br>(Question of controling the value chain) | **Accelerated development cycles (time to market, TTM), competitive pressure**<br>(re-use of components whose security properties have not been tested) |
| | Examples of problem areas or solutions<br>Classic: integration of "open source" software without service contract (maintenance)<br>Newer: Large-scale use of insecure IoT devices |
| **Security from the outset**<br>(Ability to ensure IT security from the outset without correction cycles) | **Entry of IT into areas such as discrete and process-oriented manufacturing; autonomous driving, etc.**<br>(the rapid correction cycles of IT are at odds with the requirements of the new application areas) |
| | Examples of problem areas or solutions<br>Classic: Merging of security and safety<br>Newer: very high requirements for IT security and availability and stability |

The development of catalogues of information security measures is explicitly not one of the new challenges. Nor is it yet about the practical and fundamental problems of their implementation. Rather, we are taking a closer look at the way IT security or information security management works. Of course, or rather by definition, its primary task is to implement measures to increase IT security in order to minimize risks associated with the use of IT. To do this, however, information security management must provide other services. The list in Table 1 deals with these:

- Information security management must be able to control and influence (security governance). Why is this becoming more difficult? Because of the diversification of service models. Each divides responsibility differently for the delivery of the functions of an IT service and for the activities involved in maintaining and managing it. According to this division, each service model results in a matrix of parties and their deliverables. The challenge is to understand the interdependencies between them and take them into account along the entire chain to create a secure, integrated whole.
- Information security management must be able to coordinate and harmonize (security orchestration). Finally, the overall structure must be secure. Why is this becoming more difficult? Because of the diversification of deployment models. An IT service with the same functions and activities for maintenance and administration can be technically constructed differently, be located in other places under different influence or be made available to other user groups. There are also hybrid systems that combine several such variants. As a result, applications are distributed, are located in different clouds and in different places, for example, and different subsystems are characterized by different levels of security.
- Diversification in the supply market and internationalization: Globalization in particular is making it increasingly difficult for IT service providers to make the range of their services compatible with a wide variety of requirements that are often country- or industry-specific. This means that user organizations have to make compromises - also with regard to IT security. If this is not easily possible, they can try to use compensatory measures that limit the influence of potentially insecure parts or parts that do not meet the requirements (security confinement). Corresponding "gateway solutions" now form a separate market segment. The concept of the Trusted Computing Platform (TCP) creates a security anchor in threatened systems. At the network level, Zero Trust Network Access (ZTNA) moves the line of defense directly to the applications and defines a Software-Defined Perimeter (SDP).
- Suppliers are facing increasing competition; they are accelerating development cycles. The use of third-party

components, for example, is an effective tool for this. However, these components often do not have the required security features, or this has not been checked. But if the value chain is not checked (security control and quality management), IT security is put at risk. The problem is particularly obvious in IoT systems, where it is often not clear which components with which properties are part of the system and could potentially jeopardize its security. Risks are also sometimes difficult to determine because it is not known at which points in the corporate process the data will ultimately be used.

- IT is increasingly finding its way into areas such as discrete and process-oriented manufacturing, autonomous driving and other new application areas. However, the rapid correction cycles of IT and IT security are often at odds with the requirements of the new application areas. Availability requirements are high; failures and outages lead to production downtimes and high costs. The requirements for functional reliability (safety) are often enormous, for example in the chemical industry and in autonomous driving. However, information security management is currently often not in a position to ensure IT security from a standing start and to meet the requirements without further changes (security from the outset).

This list shows potential for the further development of information security management. While the focus is often still on IT security measures alone, the aim must increasingly be to find systematic approaches to the issues of *enforcement (security governance)* and *coordination (security orchestration).*

The question of *confinement (security confinement)* has been discussed for a long time. One thinks of trusted computing and of perimeter protection, which has recently also been viewed critically. Zero Trust is one of the new approaches.

Two *quality management* topics remain: control of the value chain *(security control and quality management)* and the ability to meet security requirements right from the start without further changes *(security from the outset)*. Both are still in their infancy.

# 4 Phase 4: Looking ahead

Karl Valentin sneered: “Nothing is so difficult to predict as things that lie in the future.”[2] One should stick to that and not read too much into the coffee grounds. But a few things have already started, they seem to be on the horizon, and IT security can be expected to face them. The following list is therefore a bit more concrete in terms of possible solutions for better IT security.

## 4.1 Increasing dependence

**Situation:** It becomes apparent at the latest during the processing of a security incident: The separation between the user organization (consumer of the IT service) and the IT service provider (producer) reaches its limits. This is because the affected party and the originator often have to work closely together in the search for the root cause, the minimization of the impact and the elimination of the error. This applies in the same way to any change to IT along the entire lifecycle, with regard to monitoring the normal state and in many other situations.

**Necessary consequences:** What does this mean for IT security? An Information Security Management System (ISMS), for example according to ISO/IEC 27001, is initially organization-specific. Particularly in the case of large institutions, it is usually implemented in a way that is specific to the company or organization. The ISMS must be adapted to the circumstances of the respective company, the respective organization. This in itself is the cause of friction losses, for example if the user organization and the IT service provider use different terminologies. More critical, however, is the fact that most ISMS are still too focused on their own company or organization. They implement too few interfaces to third parties. Procurement is now more or less well analyzed and controlled, but in operations there is often a lack of coordination and interaction. What is needed is the following: Along the entire lifecycle, it must be defined in which context, which tasks with which type of distribution of responsibility are to be performed by which party and how both sides interact in each case. The *Joint Security Management (JSM)* outlines a solution for such cross-organizational security management [11]. Of course, this does not mean that the parties lose their independence.

## 4.2 Declining vertical integration

**Situation:** About 10 years ago, the word “consumerization” was already making the rounds. The trend behind this was that large user organizations were losing their dominant role on markets. It is not they alone who set the pace and determine the characteristics of IT; rather, IT companies increasingly aligned themselves with consumers, and mass products gained the upper hand. “Bring your own device (BYOD)” can be understood as a continuation of this development. Especially with the spread of public cloud services also in the enterprise market, this development started affecting also more complex IT services in a slightly different form. Self-service by the user was propagated and declared the cloud standard. This allowed IT service providers to offer their IT services more cheaply, provide them with less staff and invest the profits in expanding the business.[3] At the same time, parts of IT are becoming so complex that suppliers not only provide the technology, but also provide a larger and larger part as a managed service.

**Necessary consequences:** In addition to many advantages, this decreasing vertical integration on the part of IT service providers also has its price. On the one hand, the importance of the supply chain is increasing. Whereas in the past it was primarily product features that played a role in procurement, now it is also service promises that last for years. On the other hand, many activities remain with the IT

[2] Unattributed quote, which in my memory I attribute to Karl Valentin. What is documented, however, is: „The future is also no longer what it once was.“

[3] It should be noted that the purely technological factors scale more and can therefore be reduced (economies of scale) than the operational or process-related costs in IT service management (staff required).

departments of the user organizations or go back there. However, user organizations can also make use of a second IT service provider to take over many of these tasks. Compared to a "fully managed IT service" or "traditional IT outsourcing", IT security management in such a two- or three-party constellation is more complicated.

Also, user organizations continue to lose influence, while IT security and compliance requirements tend to increase and become more complex. Gartner predicted in 2015 for the next five years that about 95% of security failures would be caused by these "remaining" activities such as configuration and monitoring and consequently not by the provider of the core cloud computing service. Nevertheless, the provider determines what is possible in the first place and must properly inform and instruct the "users". This is done primarily via training courses with certification and within the framework of partner programs. But what happens if vulnerabilities are exploited and security incidents affect business operations? Then one must be able to fall back on service descriptions and contracts in order to be able to clarify responsibilities.

*Zero Outage Industry Standard (ZOIS)* has ventured into improvement and formalization and defined a framework for such agreements regarding IT security with the "Supplier Management Model" and the "Product Requirement Document (PRD)" [12]. In this context, not only the instructions must be comprehensible. The security measures should be as standardized as possible so that they can be used as the basis for contracts. The contracts should then be created in parallel with the configuration of the IT service in self-service and reflect the division of labor in terms of assigning responsibilities. Everything must be so comprehensible that operational IT security and risk management can be based on it. However, understandable service descriptions, contracting and the assignment of responsibilities have not yet been among the "supreme disciplines" of IT security. There is a lot of catching up to do.

## 4.3 Individualization versus standardization

**Situation:** "One size fits it all" remains limited to infrastructure and "simple" applications in the enterprise market. This is easy to understand. Large enterprises compete in the market and therefore need to generate competitive advantage. This is done by optimizing business processes including development, production, service, etc. If these are now partially automated with the help of software, the standardization of the software reaches its limits. If competitors were to use the same software to the same extent (and without customization), the possibilities for generating competitive advantages would be limited. Therefore, "Software-as-a-Service" is not the dominant service model.

**Necessary consequences:** IT security (just like the IT organization) must initially view the infrastructure and the applications separately and treat them differently. This is the case to some extent, but by no means universally. For example, identity management (administrative part) and access management (run-time) are often not considered as two disciplines. Security requirements arise from the nature of data processing at the application level, but they cannot simply propagate into the infrastructure because the latter is already in place and may not be able to be changed at all. If IT security is built up layer by layer, horizontally from the bottom up, there is no methodology to check and ensure compliance with application requirements in their application context.

In general, also IT security consists of a multitude of individual measures of a technical, procedural and organizational nature. Without a generic, security-affine architecture with a selection procedure, it will be difficult to determine whether or not these result in a secure, integrated whole. Models such as the *ESARIS Security Taxonomy* and the associated selection procedure can help here (see [8] and [13]). Basically, the answer is wide-ranging modularization (with standardized building blocks) in conjunction with a procedure that allows to determine which modules are to be considered and which are not. This requires a description of the dependencies, the scope of which would have to be kept as small as possible by defining the modules. Such a selection procedure is usually missing.

## 4.4 Abstraction, automation and division of labor

**Situation:** Modern IT is characterized by abstraction (for example, through virtualization), by automation (for example, the customer-specific provision of entire IT services by means of a script), and again by division of labor. Abstraction increases compatibility, automation requires it, for example, in the form of the existence of usable APIs. Concepts such as Software-Defined Networking (SDN) and its applications such as SD-WAN combine all three characteristics, i.e. abstraction, automation and division of labor.

**Necessary consequences:** Division of labor is associated with loss of information. As a result of automation, one also loses the ability to intervene. "Software-defined infrastructure" and "evergreen" concepts also introduce a dynamic mode of change that comes into conflict with the classic approach to IT operations and IT security management. Losses of information and opportunities for intervention complicate IT security management. Only abstraction can be beneficial as it narrows down opportunities for error and attack. "Confinement" and also "isolation" are old IT security concepts (both are found in the TCSEC and before). But the fundamental problem is different. How does one counter the inherent loss of information? How do you create opportunities for influence and how far can this go?

The literature and standards are usually primarily concerned with establishing and maintaining IT security. For user organizations, i.e., the majority of companies and institutions, however, this is not the primary task. Even among IT service providers, a large proportion of IT security experts are not concerned with establishing and maintaining IT security, but with managing information about IT security, i.e., with obtaining, evaluating and communicating information about IT security. The concept is called assurance and is the focus of TCSEC, ITSEC and Common Criteria. User organizations need information about IT security (for which the IT service provider is responsible) as a basis for their operational risk management and in order to satisfy their auditors, accountants, authorities, customers and other stakeholders. The concept of “trustworthiness” deserves more attention and must be planned and implemented with individual measures just like the establishment and maintenance of IT security. In addition to “security management”, “assurance management” is needed. How to imagine this “assurance management” in concrete terms is explained in the following chapter using examples.

## 5 “Assurance” or “assurance management”

It is important to understand that “assurance management”, unlike “IT security management”, does not increase IT security, although it may provide important impetus for it. Nevertheless, the tasks of an “assurance management” at a larger IT service provider are very diverse and extremely important, especially if they provide IT services commercially. Here are some examples related to the management of IT security information:

- Analysis of the justified information needs of the (potential) users regarding IT security and compliance of the IT services and comparison with the practices of possible competitors of the IT service provider,
- Participation in the development of an appropriate transparency strategy, which determines the importance the IT service provider attaches to informing its customers (users) and interacting with them in general, and how this is to be implemented in practice,
- Define and decide which information can be communicated to customers (users) under which conditions and which information is considered intellectual property worth to be protected and may not be communicated,
- Help formulate the IT security objectives and the customer promise (regarding IT security and compliance) in the early stages of IT service development,
- Ensure that the technical security measures of an IT service are adequately described in its service description in a user-friendly and sufficiently comprehensive manner,
- Ensure that the IT security measures related to the lifecycle (development, implementation, operation, maintenance, decommissioning) of the IT service are described adequately, user-oriented and sufficiently comprehensive in its service description,
- Ensure that both conceptual and operational evidence can be provided to demonstrate to customers (users) that the technical and lifecycle security measures have been implemented,
- Support and control that all suppliers of the IT service provider also contribute the necessary information, that appropriate agreements are made (this requires the analysis of internal and external supply relationships along the supply chain) and that the information is used adequately,
- Support that the documentation of the IT service provider is structured and that documents are marked in such a way that the strictly internal use on the one hand and the mixed internal and external use on the other hand can be practiced according to the rules and without additional efforts,
- Ensure that compliance statements are well prepared, can be substantiated and can be presented correctly,
- Support and control the creation of material for sales purposes (presentations, flyers, websites and the like),
- Accompany the drafting of terms and conditions and blueprints for contracts,
- Assist in responding to customer (user) enquiries, prior to the conclusion of the contract, during any negotiations and throughout the operational phase up to the completion of decommissioning,
- Develop solutions and monitor their application so that customers (users) are provided with information on IT security in accordance with contractual agreements (security reporting),
- Organize and support external audits, tests and certifications and pass on their results to the IT security management team, as well as any customer requests and the like that become known.

## 6 Conclusion

What can be done concretely? Table 2 shows a summary of the situations and consequences discussed in Chapter 4.

Firstly, Information Security Management Systems (ISMS) in large organizations, especially user organizations, are still too focused on activities within their own organizations. Approaches such as *Joint Security Management (JSM)* [11] can help to shape collaboration across organizations.

Secondly, supply chain management must be systematized and focus more on service descriptions, contracting and the assignment of responsibilities. ESARIS and *Zero Outage Industry Standard* [12] provide approaches with their concepts.

**Table 2: Steps for more quality and future security**

| Situation/Challenge | Consequences/Solutions |
|---|---|
| Dependencies between user organization and IT service providers; necessity for cross-organizational cooperation | Joint Security Management (JSM): cross-organisational security management |
| Decreasing vertical integration; more complex supply chains; many service and deployment models | Supplier Management Model: focus on service descriptions, contracting and assignment of responsibilities |
| Individualization versus standardization; standardization while maintaining flexibility | Architectures such as ESARIS with functioning modularization and hierarchy: decomposition and integration, complexity mastery |
| Abstraction, automation and division of labor; loss of information and control or their transfer | Concept of trustworthiness (assurance): in addition to “security management”, an explicit “assurance management” as a separate discipline |

Third: Security architectures are not nice illustrations for more complex texts. Set up correctly, they are the most important tool for IT security management! *Zero Outage Industry Standard* has already adapted parts of the security architecture ESARIS [8] [13]. Their application also supports individualization with simultaneous standardization.

Fourth: IT security experts still talk about IT security in the abstract and primarily about measures to increase IT security. Yet they already spend a large part of their time collecting, evaluating and communicating information about IT security. It is time that, in addition to "security management" (securing), "assurance management" (assuring) is also systematized and understood as a discipline in its own right. User organizations and all buyers in the value chain need information about IT security ("assurance material"; also referred to as proof of trustworthiness) in order to be able to assess risks and make appropriate decisions.

This article is intended to stimulate the discussion. Of course, the technical security measures must be adapted to the respective new information technology. But this is not enough. Information technology and its provision and use have changed so much that the traditional forms of IT security management are no longer sufficient and must be supplemented.

But before we cry "not more" and adopt a defensive attitude, we should also recognize that the developments can also mean relief for IT security management. The division of labor is indivisibly linked to the fact that certain activities are assigned to specialists and the other side does not have to worry about them much. Perhaps clever, architectural approaches will succeed in getting rid of old burdens in order to gain strength and resources for the new tasks. But that would be another topic.

## Literature

[1] 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.

[2] ISO/IEC 15408 - Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model; 2009; and: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; April 2017, Version 3.1 Revision 5

[3] ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management; 2013

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

[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] ISO 7498-2 - Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture; 1989.

[7] Eberhard von Faber: Methods: "Secured by definition" and the utilization of quality management principles, Seamless IT security through integration within IT-production processes; German original: Datenschutz und Datensicherheit - DuD, 43(7), July 2019, Springer Fachmedien, Wiesbaden 2019, ISSN 1614-0702, pp 410-417; English translation: zero-outage.com

8] 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.

[9] ISO/IEC 20000 - Information technology - Service management - Part 1: Service management system requirements, Part 2: Guidance on the application of service management systems.

[10] Cloud Security Alliance (CSA): CSA Cloud Controls Matrix (CCM); Version 4, https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[11] Eberhard von Faber and Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln – Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion; Springer-Vieweg, 2018, ISBN 978-3-658-20833-2.

[12] Managing security in the supplier network - Third Party Integration Model; Zero Outage Industry Standard, Release 2 about Security, August 2017, zero-outage.com/security

[13] ESARIS Security Taxonomy - Synopsis, Scope and Content; Zero Outage Industry Standard, Release 1 about Security, February 2017, zero-outage.com/security.