Translation of article originally published in:
Datenschutz und Datensicherheit - DuD, 43(7), July 2019, Springer Fachmedien, Wiesbaden 2019, ISSN 1614-0702, pp 410-417

Eberhard von Faber

Methods: “Secured by definition” and the utilization of quality management principles

Seamless IT security through integration within IT-production processes

IT security does not work when it is implemented after the fact, like a band-aid applied over a wound. Security has to be implemented from the very start (“security by design”). And yet early implementation of security, in and of itself, is not enough, given the complexity of today's delivery processes and the importance of activities in IT operations. “Secured by definition”, a tried-and-tested approach, views IT security as a quality asset that is achieved not by checks and corrections but by conformance – on the part of all people throughout all parts of the value chain – with certain predefined rules. To achieve such conformance, an entire arsenal of measures has to be applied.

Overview

The methods and procedures for “secured by definition” were developed gradually, over many years. At the same time, each new method and procedure was operationally implemented immediately, as soon as it was developed. **Chapter 1** provides a short overview of the relevant background and of the results obtained with this approach.

The requirement for this approach emerged during the industrialization of the IT sector. It was first identified as such in about 2010, and the term “secured by definition” was first used in 2017. **Chapter 2** recaps the industrialization process. It also describes how problems emerged that had occurred, and were solved, in other sectors about 100 years ago. In addition, it derives five requirements which are applied to the IT sector and to IT security.

Chapter 3 discusses how the five requirements can be met. We use the term “secured by definition” in order to emphasize that we are referring to a framework that automatically generates IT security within the context of IT production. For such a framework to function properly, production processes must be suitably organized. **Chapter 4** discusses additional aspects of pertinent implementation. This discussion begins with a look at the scope and expense of the implementation. Then it turns to the relationship between resource management and quality, using an example for illustration. Finally, it emphasizes the importance of standardization and, with the help of examples, explains in detail how the necessary basis for standardization can be created. **Chapter 5** provides a summary and an outlook.

Prof. Dr. Eberhard von Faber

T-Systems, Chief Security Advisor, IT Division; working areas: security architecture, developer of ESARIS, secure IT production, secure IT outsourcing, process and ITIL integration, standardization, cloud, IAM; E-Mail: Eberhard.vonFaber@th-brandenburg.de

1 Description of the problem

It is unquestioned that IT security is a strategic task. In most cases, this task goes by the name “security management”, and most departments responsible for IT security refer to themselves as “security management” departments. In spite of such conventions, the field of IT security, as a whole, seems to suffer from a lack of useful strategies and methods.

The predominating description of strategies for implementation and management of security measures is still that found in the information security standard ISO/IEC 27001 ([1], since 2008), which outlines an Information Security Management System (ISMS). In addition, the ISO/IEC 27002 [2] standard presents a pertinent catalog of measures, with a primary focus on identifying and processing relevant issues. Methods for quality

management in a broader sense are also available (risk management[3], metrics). However, such standards are not intended to serve as practical guides for actual implementation, and ongoing updating, of the many security measures they refer to. Furthermore, the recent additions to such standards (such as [4]) only partially reflect the relevant changes that have occurred in IT business and in modern IT production.

In about 2007, T-Systems began – initially, using tools it had developed in house – to produce IT services on multi-client-capable platforms that led to what is now referred to as the "cloud". With such steps toward industrialization, IT infrastructures and IT-based customer projects became continually larger and more complex.

Following a number of major problems, various IT managers saw the need for a strategic approach to the task of assuring IT security in the companies' portfolio and new business. But what standards and procedures would bring about a real change? The following deficits in existing standards and procedures were identified:

1. An almost complete lack of integration within operational processes: A lack of process-based security measures and of a concept for operational integration.
2. A lack of a concept for efficiency and for management of limited resources: While the risk management approach does provide a method for "prioritization" and "escalation", it does not enhance the efficiency of regular day-to-day business; in fact, it is oriented to an aim other than such efficiency.
3. A lack of architecture and methods needed for managing complexity: Existing instruments are not adequate to the task of describing, and efficiently managing, IT-security complexity within the modern IT environment. In addition, no common "language", a language that all IT staff can understand, is available.
4. A lack of a customer-supplier model with suitable interfaces: The procedures used need to support modern delivery models (such as cloud-based models) and, in general, all forms of work-sharing within the supply chain (such as cloud-based service models). In addition, a basic concept must be available for the task of dovetailing service catalogs with security standards.
5. Inadequate support for user organizations: The issue of proof of trustworthiness ("assurance" [5]) is not being adequately addressed; adequate relevant methods are not being applied.

These deficits were translated into requirements pertaining to the desired framework [6], which gradually emerged via the development of new procedures and methods, and which became known as the *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* [7].

The present article focuses primarily on ways of eliminating the first of the above-described deficits. Only gradually did it become clear that the resulting solution is similar in many ways to ideas from the area of quality management. The similarities are described in the following chapter.

2 Derivation (as seen from our perspective today)

In this chapter, five requirements are derived, from a short history of quality management, that can be applied to IT systems and IT security and used as a basis for "secured by definition".

Before one can identify a good solution to a problem, and implement it adequately, one must first describe the problem precisely. Progress in describing a problem can often lag behind the development and implementation of relevant solutions. This occurred in the present case.

Often, historical comparisons are useful, and sometimes they are more relevant than one might assume. The key concepts to be addressed in this context come from the areas of IT and industrialization. The changes described in Chapter 1 that prompted the search for new solutions had to do with the IT to be secured. More precisely, those changes had to do with the transition from "manufacturing operations" to "IT production". The IT outsourcing that had traditionally been practiced, in most cases using dedicated IT stacks and customized solutions for users, had lost importance. Standardized IT services were gaining in importance. "IT production" emerged via the transition to predefined IT services, based on standardized platforms, for user organizations. This development marks the industrialization of the IT sector.

For this reason, it is useful to consider industrialization as such somewhat more closely. Changes similar to those occurring in the IT sector today occurred in other sectors many years ago. Therefore, let us leave the narrow context of the IT sector for a moment, and turn our minds' eyes back to the past.

In preindustrial eras, work methods and procedures were determined by tradition and experience. As industrialization began, it placed a central emphasis on (standardized) products.

- In this early phase, work productivity still tended to be low. It varied widely from worker to worker,
- quality varied in keeping with individual workers' skills and experience;
- In addition, workers tended to bring little motivation to their work.

Later, it became clear that

- vertically structured and product-oriented production operations and companies (with "silo" structures) used resources inefficiently.

What lessons were learned from this insight, and what solutions emerged?

Frederick Taylor (1856–1915) systematically analyzed the work methods and procedures of his day and used his results as a basis for restructuring work operations and making them more efficient. He developed a "scientific management" method that introduced a separation between work planning and work execution. In his auto-manufacturing operations, Henry Ford (1863-1947) then introduced assembly-line production, which broke down complex workflows into series of small tasks. The tasks were to be carried out precisely in accordance with defined and proven procedures that were mandated as standards. The assembly line is a fitting symbol for this

process orientation. The concept of the process-oriented organization was not formalized until the 1930s, by Nordsieck and Henning. The concept called for product-based structures (structural organization) to be complemented by structures based on the sequences in which work tasks were to be carried out (process organization; such sequences of work tasks are now known as "business processes"). Later, additional approaches to work organization emerged, including Lean Production, Kaizen, Six Sigma and Total Quality Management (TQM).

While the basic principles of TQM are summarized in different ways, one of its most important insights, introduced by William Edwards Deming (1900-1993), is clearly the following: Quality has to be produced, and not just controlled; it results from active efforts on the part of each employee. And management has to define a framework that makes quality possible.

With this review, we have identified the **five solution components / requirements** that we can apply to the area of IT security:

A1 Work methods and processes need to be defined via systematic analysis, and not solely – or primarily – via tradition and experience.

A2 The manual work of production itself needs to be separated from related planning and conceptual work. A best method should be developed, and all workers should be required to use it.

A3 High priority should be placed on supervising the manual work of production itself; supervision should be carried out by management.

A4 Process-based structures are required supplementing the vertical, product-based structures.

A5 Quality has to be produced, and not just checked. And management has to define a framework that makes quality possible.

These principles provide a basis for development of a solution for improved IT security. We use the term "secured by definition" in order to emphasize that we are referring to a framework that automatically generates IT security within the context of IT production. For such a framework to function properly, production processes must be suitably organized. The following chapter describes the structures this entails.

3 Secured by definition

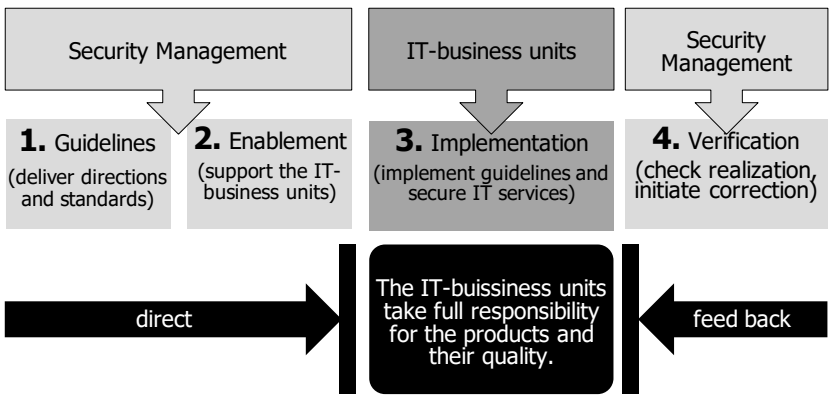
IT security has to be produced, and not just checked (cf. A5). To produce IT security, one must focus on all processes that "shape IT" (cf. A4) and must integrate IT security within all core processes of IT production. Procedures, processes and activities are systematically analyzed (cf. A1) and standardized (the conceptual, planning part of the organization), and then implemented in conformance with the resulting standards (the producing part of the organization; cf. A2). The IT-security-management organization integrates IT security within IT-production processes, defines the applicable standards and monitors compliance with the standards (cf. A3). The IT departments implement the standards and achieve the desired IT security.

3.1 Work-sharing between IT-business units and the IT-security-management organization

The first step is to assign responsibilities for defined tasks. This is outlined in the following. For this, we use a simple model that implements three of the above five requirements.

The IT-business units are responsible for the quality of the IT services they provide. IT security can be seen as one type of quality, among other types. Therefore, IT security falls within the responsibility of IT departments; it cannot be delegated. That said, we remember the success of the strategy whereby the manual work of production is separated from planning and conceptual work. Furthermore, a central IT-security-management organization is needed that can define overarching security standards and ensure they are fulfilled. Figure 1 illustrates the division of labor between a (central) IT-security-management organization (nos. 1, 2 and 4) on the one hand, and IT-business units (sales, IT production, service management) (no. 3) on the other. Structures for areas such as vulnerability management run horizontally and cut across the sections defined by the work-sharing.

Figure 1: Division of responsibilities between IT departments and IT security

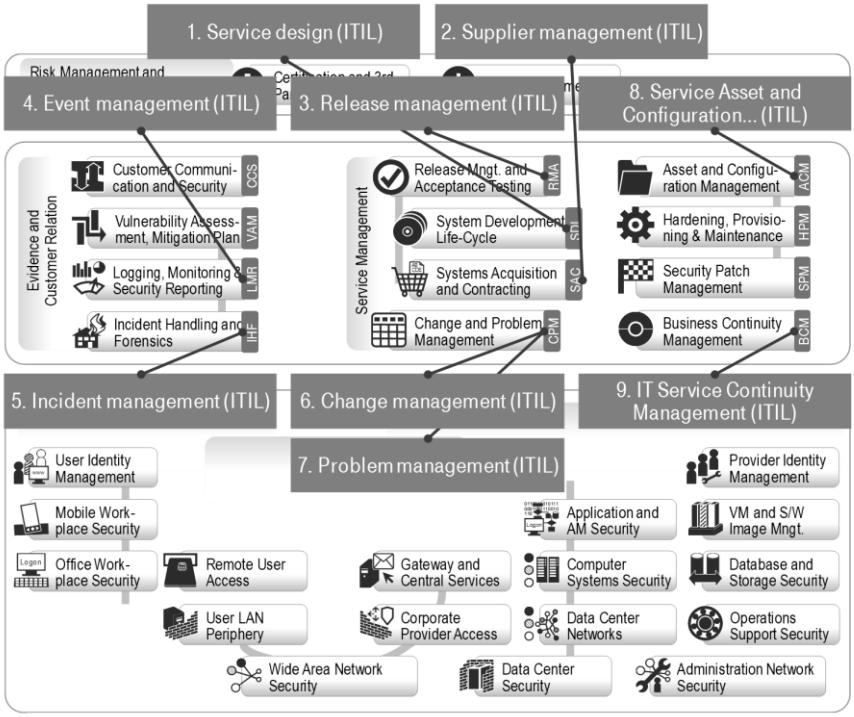


This model provides an important basis for "secured by definition". We note that, in nearly all cases, "IT production" is divided into multiple IT-business units. Each such unit is responsible for specific IT services and their quality. The "security management" (cf. Figure 1) referred to stands for a (central) IT-security-management organization that can include local structures. The model functions only because the security management referred to features clear staff separation, defined by roles, between 1, 2 and 4, on the one hand, and 3, on the other. In this light, security experts should not primarily be assigned to "topics". Instead, they should be assigned to "tasks within topics", in the context of the above-described structural separation. This is important, because otherwise IT departments might not fulfill their responsibility, and "IT security" would be

unable/unwilling to fulfill that responsibility, simply due to a lack of the necessary personnel resources. A risk of back-delegation also applies: IT departments (no. 3 in the figure) are informed, by the supervisory entity (no. 4), of the need for corrections. But the IT departments do not carry out the corrections themselves, because they see such corrections as the responsibility of security management (no. 4). This failure to act is in conflict with basic management principles, and it is certainly not useful.

Systematic analysis (cf. A1) is a necessary basis for the quality of all technical, process-related and organizational security standards. The separation between task no. 1 and the other tasks supports such analysis. The separation between planning and implementation (cf. A2) is facilitated by the separation of task no. 2. In addition, it is common practice (cf. A3) to view monitoring (no. 4) as a separate task that should not be combined with the other tasks. Additional reasons for such separation are set forth in [7].

Figure 2: Taxonomy with 8+4 areas on ITSM activities



3.2 IT-production processes (ITSM)

IT service management (ITSM) comprises all activities and underlying methods that are needed for large-scale provision of IT services. Most IT-services providers structure and organize such activities and methods, within their IT production, with the help of processes such as those specified in the Information Technology Infrastructure Library (ITIL®) [1] or the standard ISO/IEC 20000 [8]. To the processes defined in those references, "secured by definition" adds specific aspects of IT security, along with a number of new security areas. In so doing, it primarily implements the two remaining requirements, A4 and A5.

For the purposes of security management, copying the ITSM process landscape would be an overly complex task. Both areas are complex in themselves, and there would be little use in simply combining them. The *ESARIS Security Taxonomy* [7] shown in Figure 2 reduces the process landscape to its essential features. About half of the system refers to activities involved in developing, implementing and operating IT services, including managing, servicing and upgrading them. The core area consists of the 12 areas, with icons, that are shown in Figure 2. It should be noted that 8 of these areas refer to 9 ITSM core processes. Cf. Figure 2.

Since an IT-production environment uses multiple technologies, the other, lower half of the figure refers to typical technology areas, and related work-sharing, within an IT-services provider's structures, and including all the provider's partners and suppliers. In the following, this second half is not considered.

What in this overview, then, is "secured by definition"? For each of the defined areas, there exist detailed descriptions and standards that specify how IT security is taken into account in the framework of the ITSM activities.[2] IT personnel conform to the ITSM requirements, thereby "automatically" implementing the predefined security measures. In this manner, IT security management is integrated within IT-services management.

The *ESARIS Security Taxonomy* is easily comprehensible for IT experts and IT-security experts alike. Consequently, it is a suitable scheme and vehicle for communication. The taxonomy, which has been published by the "Zero Outage Industry Standard" association [10], has been in use for years and has been proven in practice [9].

It is not enough to simply upgrade ITSM processes by adding IT security aspects. In Figure 2, four of the twelve "service areas" are not labelled with ITSM processes. These other areas are: "Hardening/configuration, provision and maintenance", "security-patch management", "customer process", and "vulnerability management". The "customer process" comprises all activities involved in sales, in contract design and in business transition. The following section describes, by way of example, a) vulnerability management (as an additional process) and b) release management (as a known ITSM process).

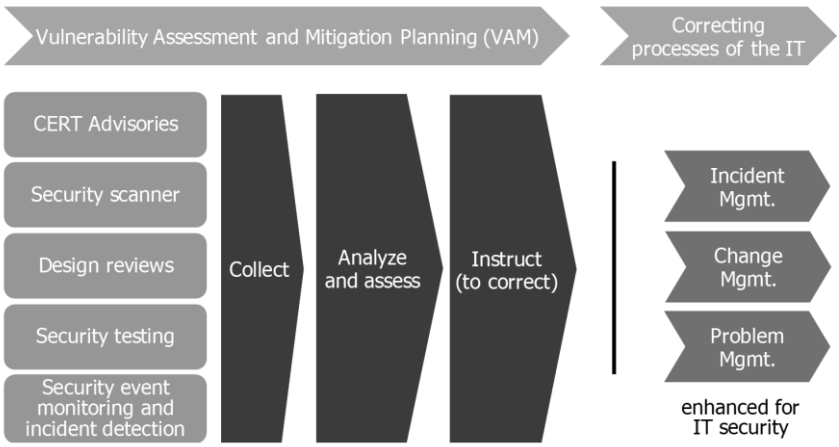
[1] "ITIL" and "IT Infrastructure Library" are registered trademarks of Axelos Limited; all rights reserved.

[2] Note the phrase "is taken into account." The wording is not "should be taken into account" or some other, similar phrase.

3.3 Vulnerability management and release management (two examples)

Integration of IT security within core processes of IT production can be effectively illustrated in terms of the additionally defined vulnerability management process (Vulnerability Assessment and Mitigation Planning, VAM) [11]. Cf. Figure 3. In the framework of the VAM process, any deficiencies that could result in security vulnerabilities are identified by collecting data from various sources. The deficiencies are then analyzed and assessed in terms of their impacts. This process yields reliable instructions for remediation (cf. Figure 1) that are provided to the IT-business units. The IT-business units then carry out remediation – i.e. repair measures – by applying their core processes (incident, change and problem) in keeping with the instructions.

Figure 3: VAM process and subsequent ITSM remediation processes



This example illustrates how IT security is implemented via an additional vulnerability-management process, and how existing ITSM core processes are used in order to eliminate IT-security deficiencies. The simplicity of this example is deceptive, since the actual implementation will normally be complex and time-consuming.

The “secured by definition” principle is a big step beyond the well-known “security by design” principle. While “security by design” simply refers to the observance of security requirements in (unspecified) development processes, “Security by definition” integrates security management within IT-services-management processes and subordinates security management to such processes. As a result, "secured by definition" makes IT security part of provision and operational processes, and this plays a key role in the maintenance of IT security, as the preceding example makes clear.

The traditional approach to design in IT, which begins with a blank sheet of paper and looks at applications primarily in connection with their pertinent IT stacks, is now hardly used. This is one reason why activities oriented to IT security tend to be carried out later during design and production processes. This happens, for example, when components prefabricated during the provision process for cloud services are combined, in various ways, into IT services. Another reason is that IT systems and their security tend to be anything but error-free – and have to be continually repaired or improved (see above). A third reason is that IT-security requirements are normally not clear in the early stages of design and production. Often, they have to be adapted to changed circumstances. IT systems change as business processes change, and IT security has to keep pace with new and newly emerging threats.

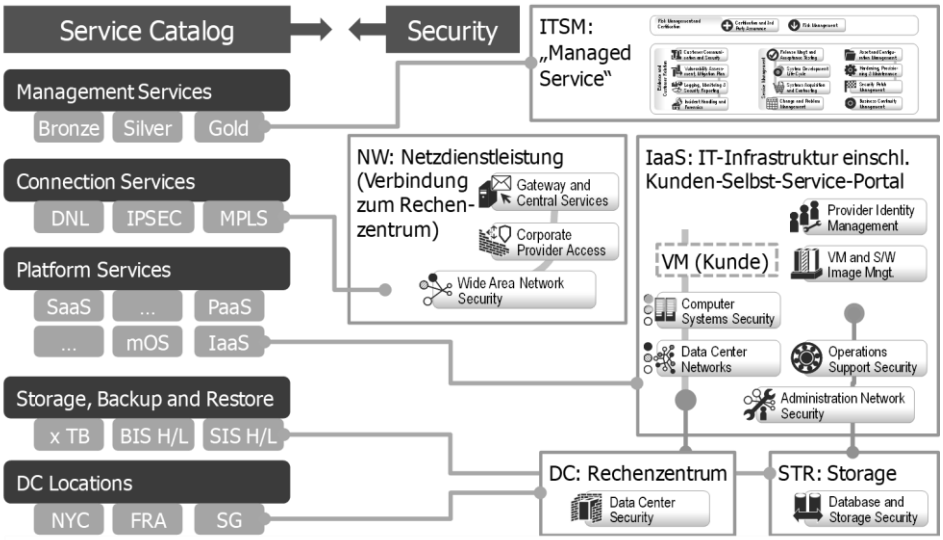
Below, we provide additional details about the above-mentioned modern process for providing cloud-based services. That process is described in the “Release Management” area, because the *ESARIS Security Taxonomy* includes also portfolio and service-catalog management in this area.

IT-services providers' offering portfolios are modularly structured. On the one hand, this is a consequence of standardization. On the other, it is a means of retaining required flexibility, since customized IT services can be produced by combining prefabricated modules. The conceptual work for such a combination is normally carried out while the contract with the customer is being worked out. In general, such combinations consist of modules from the service catalog (shown on the left in Figure 4). At the technical level, the time to create such combinations can range from a few minutes' worth of mouse clicks in an online shop to weeks of work by IT architects and solution developers.

User organizations require information about the IT security implemented in their systems. Without such information, they cannot carry out operational risk management, nor can they provide their customers and auditors with any details about the security of the IT services and about the risks involved in using those services. For such information provision to be possible, security standards (shown on the right in Figure 4) must be structured in keeping with the service modules' structures. The lower half of the above-mentioned *ESARIS Security Taxonomy* sets forth and categorizes the technical security standards involved. In the figure, individual areas of the Taxonomy are arranged so as to highlight their connections to the service modules. The upper half, referring to ITSM, is shown, as an unchanged block, in the upper-right-hand part of the figure.

This example illustrates the extent to which monolithic catalogs of IT-security measures are far from the reality of modern IT production. For auditors, such catalogs can serve as general overviews and as catalogs of relevant questions. They cannot function as the security basis for a broadly diverse portfolio of IT services that an IT-services provider offers to a wide range of customers (user organizations), however. In this context, it makes no difference whether the customers involved are business units within the same company (to which the provider belongs) or are independent companies or government agencies.

Figure 4: Catalog components (on the left) and security standards (on the right) – Flexibility, illustrated with the example of IaaS



The process of dynamically combining modules, within the provision process, takes place in a number of steps. First, small elements are combined into larger elements. Then, such larger elements are combined to form IT platforms. Such platforms are often multi-tenant (capable of serving multiple clients). Finally, individual modules will be added, replaced or modified in keeping with the specific customer's needs.

4 Further details about the implementation process

This chapter discusses additional aspects of implementation. Its first section covers the scope of, and required overhead for, such implementation. Its second section discusses the relationship between resources management and quality, with the help of an example. In a third section, it then highlights the importance of standardization and, using examples, explains in detail how the necessary basis for standardization can be created.

4.1 Scope

In a large organization, implementation of "secured by definition" takes time. In part, this is so because such processes have to be adapted to the company's specific situation. Such adaptation is required for any new framework that is introduced. This also applies to an ISMS conforming to ISO/IEC 27001 [1].

Needless to say, it is not feasible, in the present article, to cover all of the details involved in such implementation. For this reason, we provide a short summary, using examples that illustrate the scope of the measures involved.

The elements required for implementation include a diagram of the architecture involved, with charts or schematics that provide necessary overviews. Text-only descriptions do not suffice for this purpose. Such descriptions were already inadequate in connection with older systems, and they are completely unsuitable nowadays characterized by Internet snippets and short messages). As noted, all important IT Service Management (ITSM) processes have to be conceptually expanded to include suitable security measures. This means that ITSM processes, along with their descriptions and their supporting IT tools, such as ticketing and workflow systems, have to be adapted. In a first step, certain core processes – Release Management, Change Management and Incident Management – have to be supplemented with measures (practices) to ensure that the application of other technical security standards is verified, that security risks are assessed and that security vulnerabilities are identified and eliminated. In sum, traditional-style IT security management tasks become part of IT-based tasks.

As such changes are made at a company, the company needs to begin changing its corporate culture, and various procedures and approaches, in keeping with the complexities of the model (shown in Figure 1). If it has not already done so, the company needs to deemphasize the processing of *topics* and emphasize the execution of specific *tasks*. Training events should be oriented to changed processes and work methods. In addition, the company requires a model for the structuring of tasks within the supply chain, and a concept for the roles and responsibilities needed for IT security. Such a model must include a collaboration model.

Responsible security managers could find this outline of tasks rather disquieting – and the prospect of its implementation rather daunting. If so, the following should be remembered:

- Other industrial sectors have also found the process of assuring quality to be anything but easy. Aircraft makers have had to learn painful lessons in this area. Regardless of the company and the product involved, quality is never a by-product. It has to be achieved through targeted effort. The providers who enjoy long-term success have development and production processes of especially high quality. In most cases, the resulting products will also feature such quality.
- It is important to ask whether alternatives are available. Three questions can serve as a guide in this regard: Can we in the IT industry provide adequate IT security by other means? Can we abandon our goal of providing suitable security for IT services? In our security management, do we have the personnel resources we need in order to manage all aspects of security ourselves? Most companies will answer all three questions with "no".

4.2 Shortages and the waiting-line theory

Organizations are already encountering significant difficulty in recruiting and retaining the IT-security experts they require. That said, practice has shown that absolute numbers – numbers of experts – are not the deciding factor in this regard. Having enough highly motivated "thought leaders" who can successfully guide the security management organization as a whole is more important.

In the author's view, most organizations manage their best experts wrongly. The reasons for this are ultimately mathematical in nature. (1) Organizations want fast processing, and thus turn primarily to their best experts. (2) They manage processes in the wrong way. Functioning processes are used to capacity, and filled with orders, because they appear to be efficient. Both of these practices are wrong, as the waiting-line theory explains [12].

The relevant model is very simple. First, it assumes that there will be enquiries, tasks, etc. that occur at very irregular intervals. This always applies, for example, to security incidents. Second, the number of operators involved is limited. The operators are the experts who process enquiries and execute the relevant tasks. If enquiries reach an operator faster than the operator can process them, the parties submitting the enquiries will experience waits. To shorten such waiting time, one must increase capacity – i.e. add more operators. The number of available experts is limited, however.

What's more, there is a relationship between waiting time and capacity utilization. This relationship, which is easy to appreciate and has been confirmed by observation, is as follows: The higher the capacity utilization, the longer the waiting time. And the more that efficiency tends toward zero. Once a certain threshold for the utilization of operators' capacity is reached, throughput can no longer be increased.

This means that there is absolutely no point in increasing capacity utilization beyond a certain critical point. In fact, it can become necessary to reduce capacity utilization, in the interest of more-rapid processing. This relationship applies both to processes and to the work of specialists. To enable experts to work efficiently, one must ensure they are not overtaxed.

Response times and efficiency – such as incident-management efficiency – are quality parameters that have a direct impact on IT security. Once capacity utilization surpasses a certain threshold, people tend to become sloppy in their work, and this can have an adverse effect on IT security. For this reason, capacity utilization issues have to be considered in connection with any implementation of "secured by definition".

4.3 The role of standardization

Standardization is an important means of addressing shortages and achieving quality. In this area as well, a detailed discussion is beyond the scope of this article. In standardization, one seeks to standardize processes and solutions, and to eliminate all types of waste (in Japanese: muda). To this end, processes and solutions have to be broken down into smaller modules, to safeguard flexibility and diversity.

In modularization, one subdivides standards for solutions (including technical measures) into small, reusable units (cf. also Figure 4). Use of standardized elements is the key to any effort to significantly increase quality and, in particular, significantly enhance security. Use of standardization reduces experts' workloads, and it improves service quality. In addition, it speeds up the process of providing and adapting IT services. Furthermore, it provides harmonization that extends to the security standards of IT services from different production sites.

In the following, we provide examples of the elements necessary for implementation. One such key element is an architecture that can serve as a classification and organization scheme. In particular, it must support storing and management of security standards. Security measures have to be specified on various levels of detail, and refined step-by-step. As part of standardization, the manner in which specifications are written must also be standardized. In the interest of safeguarding flexibility and diversity, the scope, reach and degree of detail that individual measures are to have – and not exceed – have to be defined. All relevant document types have to be defined. Document IDs should be used for encoding documents' topics and purposes and their locations within the architecture.

In addition, a concept/process has to be defined for collection and analysis of requirements, and for translation of requirements into solutions. Such a concept/process must also define procedures for flexible reuse of individual solutions (modules). Furthermore, specifications for the creation and description of standards are required, along with a system for enactment and maintenance of standards. In some cases, this can also entail expansion of existing document-management systems. In any case, it is always necessary to check and review conformance with all applicable standards, and to keep proper records of all such checks and reviews. Also, such actions must be carried out in connection with a system for management of deviations from standards, and with a correction procedure that interfaces with risk management. The security characteristics of the various IT services have to be documented in all IT-services catalogs, as well as in the underlying development documents. A concept for such procedures is also required.

Finally, the organization should seek to change its culture, within the sense of emphasizing industrial production of IT services and application of the "secured by definition" principle. A culture of standardization provides the basis for such change. In the area of IT security (as in a number of other areas), there is a tendency to focus on things that are special or unusual, and not on what is normal. In this sense, "firemen" are seen as more important than "fire-safety experts" who define and implement fire-safety measures. Needless to say, to achieve adequate IT security, one needs both perspectives. In detecting attacks, and defending against them, one must identify things that are anomalous and conspicuous. However, the key to good defenses is quality. Quality should be the rule, and not the exception.

5 Summary and outlook

The “secured by definition” approach looks at IT security as an aspect of quality. Quality management is a relatively new discipline. At the beginning of industrialization, a decline in quality was noticed, along with quality's strong dependence on individual worker performance. These factors were addressed by separating planning and preparatory processes from production itself. Workers were given specifications, and quality improved significantly. Later, this approach led to an orientation to business processes, and measures for end-to-end quality management were invented. The IT industry has processes, but it still lacks seamless, end-to-end quality management. Quality is achieved not by carrying out checks and corrections, but by ensuring that people throughout the entire value chain observe predefined rules. IT security is a quality aspect of IT systems. Consequently, IT security needs to be integrated within all IT-production processes. In industrialized IT, the key processes in this regard are IT-service-management processes (including plan-build-run processes), such as those described in the ITIL and in the ISO/IEC 20000 standard.

The “Business Process Reengineering” (1993) method was used extensively in the 1990s. While that method is not focused directly on IT security, it does hold a number of lessons with regard to IT security. The same can be said of the “Core Competencies” (1990) approach. A principle espoused in that method and that approach, namely the principle of orientation to results, and not to tasks, can serve as an aid in correcting the way IT-security providers see their role. Security is “only” one aspect of quality (among others). With respect to an IT service provided by an IT-services provider, it will be just one of the IT service's characteristics. Core competencies make enormous contributions to customer benefit. To provide adequate IT security, an IT producer must integrate IT security within his core competency area, i.e. within his IT-service management (ITIL, ISO 20000 [8]).

The “Business Process Reengineering” method also calls for integration of parallel activities, as opposed to simple integration of parallel activities' results. This is an open invitation for integration of IT-security management and IT-service management, in the sense required by “secured by definition”. One of the key ideas in “Total Quality Management” (1951) is that quality should be produced; it shouldn't simply be checked after the fact.[3] As a result, IT security should focus on processes for production (of products or services), and not on control measures within a separate security process, as is still often the case.

Information technology and telecommunications technology have evolved rapidly in recent decades. In particular, new business models and types of utilization have emerged in the past ten years. The IT sector is reinventing itself. Given the current threat situation (extensive interconnection; the value inherent in processed data) and the importance of IT systems for successful business, the value of IT security can hardly be overstated. Along with technical measures to provide IT security, methods and procedures are needed that can ensure that technical measures are actually implemented. The conventional security management methods used to date are not equal to the challenges presented by modern IT systems and by the provision and use of such systems. Such methods emerged in a bygone era and, conceptually and developmentally, are still caught in that era. The task now is to address the following question: How can IT security, and information security in general, be permanently integrated within the “DNA” of modern IT business, and what will such integration require? “Secured by definition” is seen as an important component of the answer to this question.

[3] Phil Cosby, who helped popularize a method in the U.S. that Americans had brought to Japan.

References

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

[2] ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security management

[3] ISO/IEC 27005 – Information technology — Security techniques — Information security risk management

[4] ISO/IEC 27017 – Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; also published as ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security

[6] Eberhard von Faber: Organisation der Absicherung einer industriellen IT-Produktion, Drei Handlungsfelder jenseits von Protection, Detection, Reaction; Datenschutz und Datensicherheit (DuD), Issue (Heft) 10, 2016, pages 647-654

[7] 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, Springer-Vieweg, 2017, ISBN- 978-3-658-16481-2, XIV + 368 pages – 2d EXPANDED and UPDATED edition

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

[9] Eberhard von Faber: Changing the security mode of operation in a global IT organization with 20000+ technical staff; in: ISSE 2015 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe 2015 Conference, Springer Vieweg, Wiesbaden, 2015, ISBN 978-3-658-10934-9, pages 286 – 304

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

[11] Eberhard von Faber, Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln, Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion; Springer 2018, ISBN 978-3-658-20833-2, X+234 pages, Wiesbaden

[12] TU Clausthal: Das Grundmodell der Warteschlangentheorie; http://www.mathematik.tu-clausthal.de/arbeitsgruppen/stochastik/public-relations/das-grundmodell-der-warteschlangentheorie/; downloaded on Feb. 1, 2019