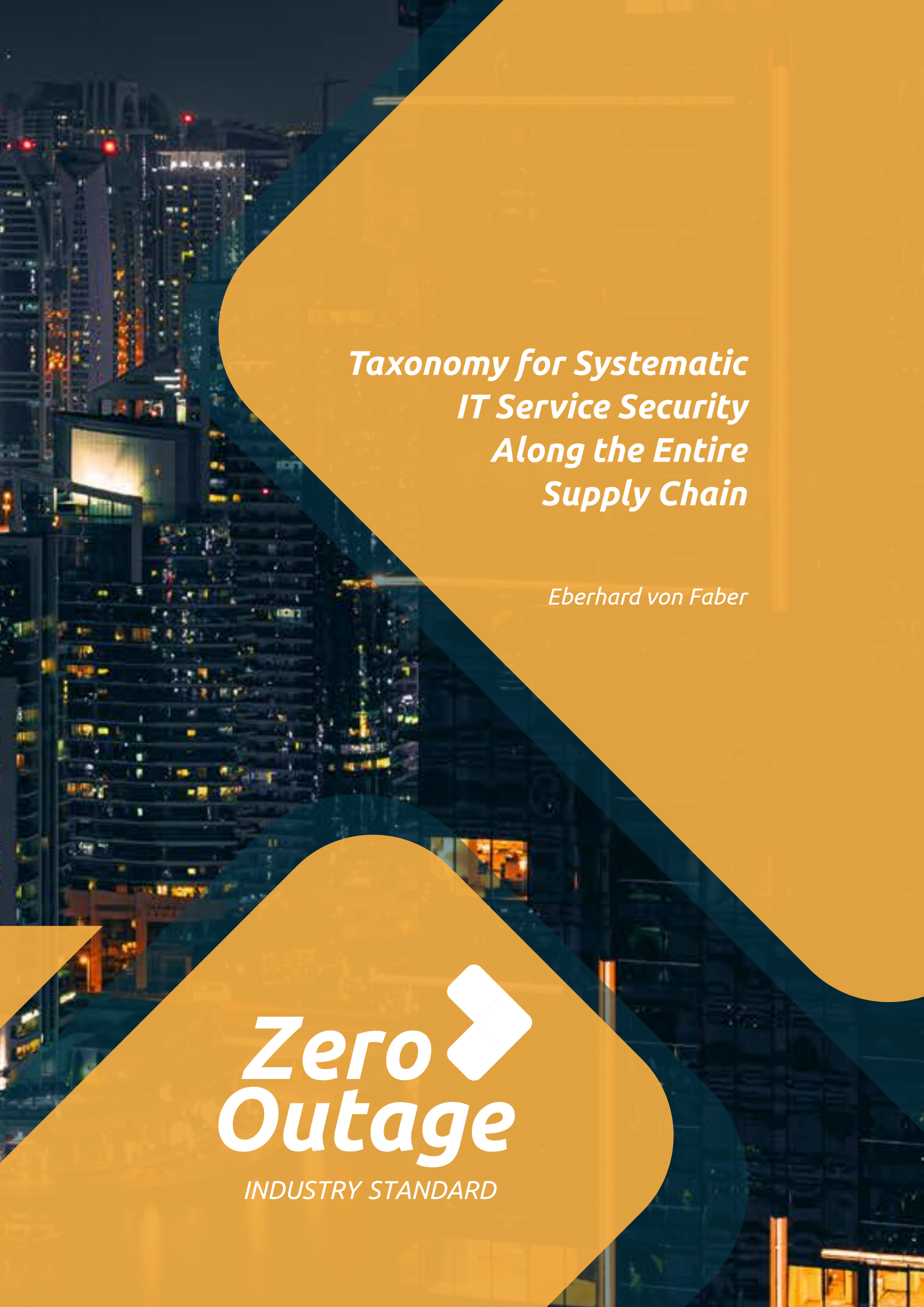


Taxonomy for Systematic IT Service Security Along the Entire Supply Chain

Eberhard von Faber

Zero Outage

INDUSTRY STANDARD

CONTENT

3 I. Introduction

3 II. Goals and principles

6 III. Overview

8 IV. Application

10 V. Details

24 VI. Summary and outlook

25 A. References and applicable documents

I. Introduction

An ordering and organisation scheme (Taxonomy) is presented that supports information security management in gaining an overview of technical solutions and process-related activities for securing IT and, based on this, in assigning responsibilities and tasks and orchestrating activities. The Taxonomy is based on the technical and operational reality of IT service provisioning. It builds largely on what is known and refrains from using trends and fashionable terms to enable its long-lasting use as an classification and organisational scheme. Of course, all modern solutions can be found and assigned just as established solutions and common practices. The Taxonomy promotes understanding and creates clarity. This paper uses definitions from [1].

II. Goals and principles

A primary task of information security management is certainly to assign responsibilities and tasks and to orchestrate activities. This is made much easier if, instead of monolithic documents and technical terms, graphical diagrams are used to illustrate the fields of activity and relate them to one another. Therefore, a Taxonomy is presented below that has been improved compared to the original version [2].

The Taxonomy shall:

- provide a small-size picture showing all subject areas (areas of activity),
- unify terms and the understanding of subject areas (areas of activity),
- support the division of labor and guide the cooperation of stakeholders to create an overall secure whole.

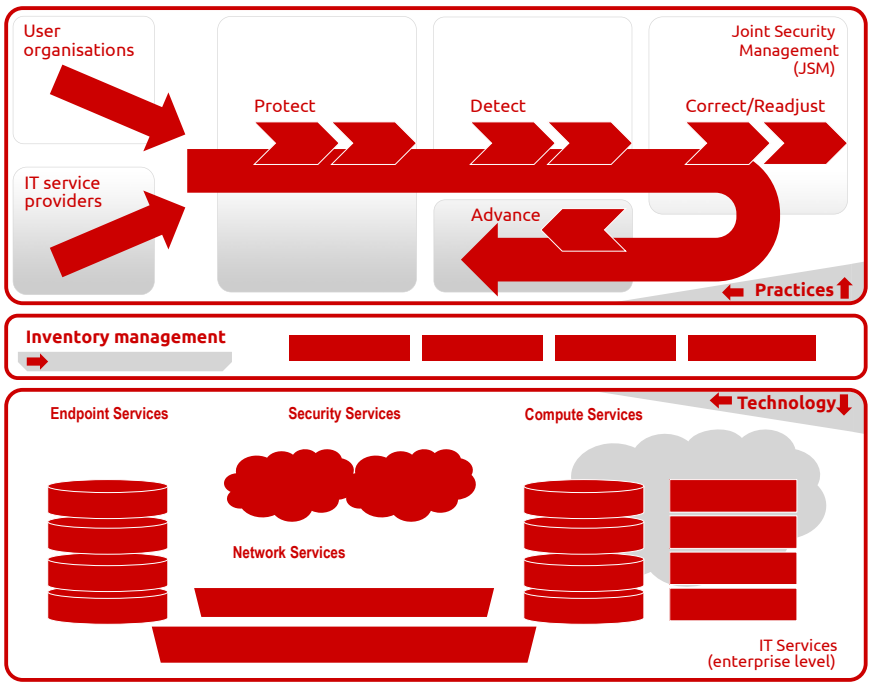
There are some principles that shall determine the structure of the Taxo-nomy. They are summarised now whereby the situation is explained first and the principle thereafter.
When the areas of activity to be orchestrated by information security management are detailed, IT security solutions or product groups are looked at and selected such as firewalls, encryption or access control. However, it is not these solutions or product groups that deserve our primary attention. Rather, it is about securing the IT and the data that is stored, processed and transmitted there. Moreover, in almost all cases it is not the IT security experts who use, install and maintain these products, but architects and administrators. (1) To ensure that the protection of IT and data comes to the fore and that IT personnel can also find their way around, the Taxonomy (classification scheme, graphical diagram) should primarily start from IT and use its structure.
In order to save costs and increase quality, as many activities as possible should run in the same way and be defined independently of the IT systems to be protected. The IT

> **"It is about securing the IT and the data that is stored, processed and transmitted there.**

described in ISO/IEC 20000 [3] provide a good model for this approach. Also, in many processes such as Incident Management, it is not initially known what type of IT components are involved. Monitoring and software updates (patching) should also follow similar procedures, since it is the overall system or IT service that is involved, which must have and retain assured IT security properties. (2) Therefore, the Taxonomy presented in the following will separate technology and practices and thus support the implementation of the principle "Secured by Definition" [4]. The choice of technology areas should be made in such a way that, as far as possible, all relevant IT services can be composed from them. This is very important because the focus should be on IT service security and not on protecting the enterprise. This brings us to the point that IT services are nowadays often purchased and produced by third parties. So, we are dealing with two parties: the user organisation or a business unit such as HR on one side and an IT service provider or IT department on the other. The fact is that both parties have to do their part in IT security. The activities are interrelated and must be coordinated with each other in terms of a Joint Security Management (JSM), which must be defined across organisations [5]. (3) The Taxonomy presented in the following supports this by defining and ordering fields of activity along a life cycle, for which tasks are in turn defined in most cases for both the user organisation and the IT service provider.

Based on these goals and principles, the Taxonomy gets the principal structure shown in Figure 1. The structure is briefly justified and explained on the right-hand side of the figure.

With regard to the IT service provider, the Taxonomy focuses not only on producing secure IT services, but also on providing security-related information. For internal purposes of the IT service provider, this is taken for granted, but user organisations also require detailed information - not only during procurement, but throughout the entire lifecycle. The task is so complex that one can speak of “Assurance Management” as a discipline in its own right, added to the classic “IT security management” [6]. (4) This is also taken into account in the design of the Taxonomy.



Practices (processes, activities)

- uniquely applied to all technology areas
- based on IT service lifecycle
- jointly carried out with division of labor by IT service provider and user organization

Inventory management

- discovery, inventorying and managing (processes + systems)

Technology areas (components)

- based on simple IT architecture: endpoints and servers each with IT stacks connected by networks plus separate IT security services
- responsibility assigned according to the Service Model of the respective IT service

Figure 1: Visualization of the general structure of the Taxonomy

III. Overview

The Taxonomy consists of three groups: Practices (upper half, see Figure 2), technologies (lower half) and combinations of practices and technologies for capturing, inventorying and managing ("Inventory management" in the figure). The groups contain clusters ("Inventory management" is its own) and each of the eleven clusters contains subject areas. There are 41 in total.

The practices (upper half, see Figure 2) are arranged in five columns, with the fifth column below the third to save space. Following the arrows, the five columns form a lifecycle of the business relationship between the user organisation and the IT service provider, while addressing cycles inspired by PDCA. PDCA (plan-do-check-act), the Deming cycle, is a universal model for managing quality. The five columns are Initiate (unlabeled), Protect, Detect, Correct/Readjust, and Advance.

Only at the very beginning (column/phase 1 "Initiate") do both parties act largely independently. In the further course, there is hardly any activity that does not require the cooperation and coordination of both parties as well as the definition of concrete tasks with interfaces and responsibilities. This logic and structure originate from Joint Security Management (JSM) and is described in detail in [5]. 18 subject areas with practices have been defined.

The arrangement of the technology areas (lower half, see Figure 2) is based on a simple technical IT architecture or division of IT services into Workplace or Endpoint Services (user devices) on the left, Compute or Computing Services

(applications with underlying IT infrastructure from the data center/cloud) on the right and the connecting Network Services (network connections) in the bottom center. The latter take into account that wide area connections are also offered virtualised as SD-WAN. Added to this are Security Services (center above Network Services) as a fourth cluster since security services are increasingly centralised and moving "into the cloud". There are 19 topic areas for technologies.

The four subject areas of "Inventory management" (discovery, inventory and managing items and IDs) can be found in the center of Figure 2. At their core, these are practices, but they not only require various specific IT systems (technologies), but are also closely related to both other practices (upper half) and other technologies (lower half). This explains their location in the middle between practices and technologies. At the same time, their central importance as a basis for operational IT security management is emphasised.

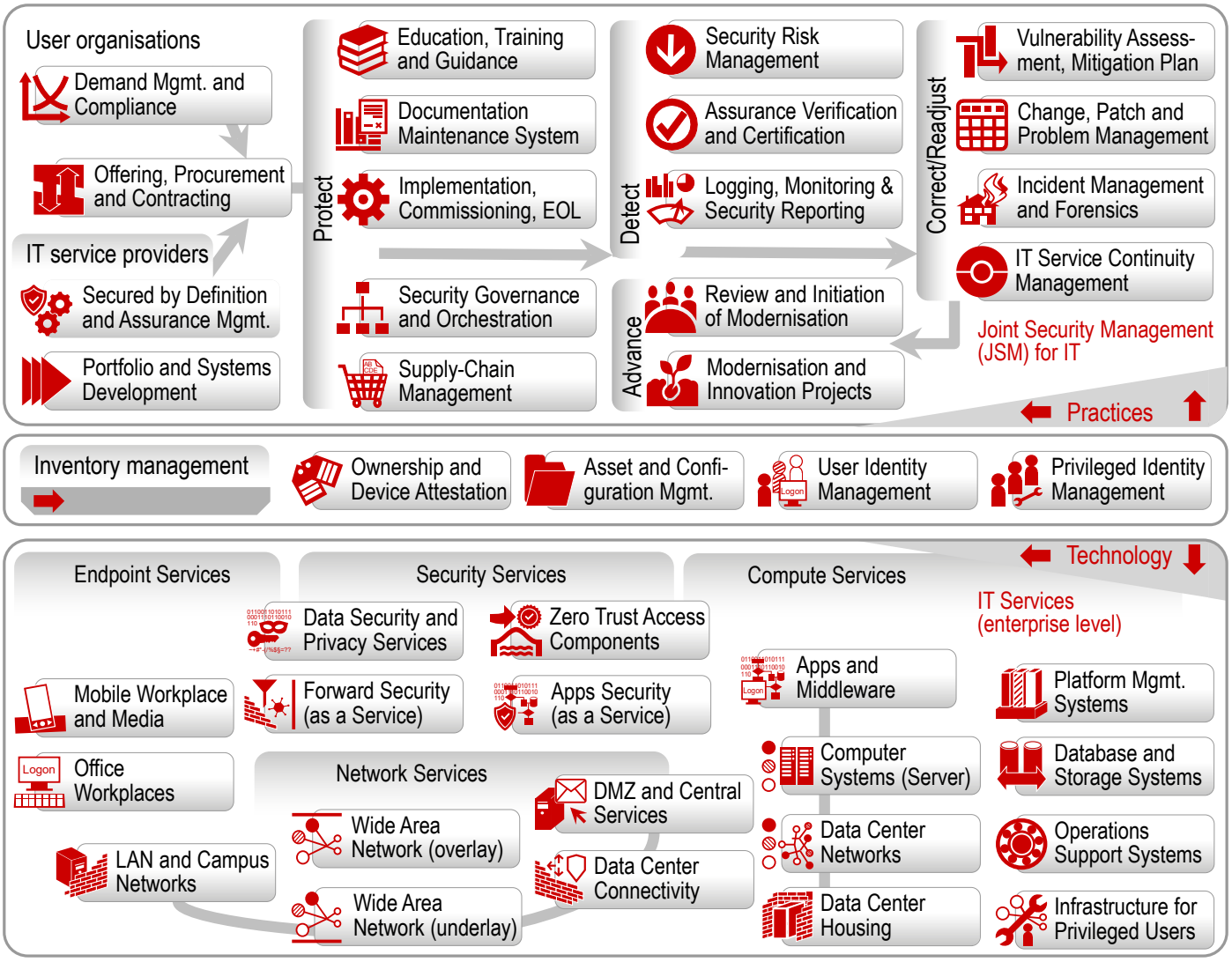


Figure 2: Taxonomy IT service security (enterprise level)

IV. Application

The Taxonomy contains a total of 41 topics. It consists of two halves (practices and technologies) and is further divided into clusters: six in the practices, four in the technologies plus one between the two halves.

Each specific IT service builds on or uses different technologies. Therefore, depending on the IT service, technology areas may or may not be relevant. For example, a desktop or mobile device is not always part of the IT service provided by the IT service provider and covered by the contract. If the devices are required, which is usually the case, the user organisation bears the responsibility for its procurement and use. This case is considered separately in another contract. I.e., a technology area can be relevant for the IT service provider or for the user organisation. Responsibility for the application software is another common example. It is often provided by the user organisation (possibly with the help of another IT service provider). Only in the case of Software-as-a-Service (SaaS) does the cloud service provider also bear responsibility for the application.

> **"Looking at each individual subject area thus helps to determine the exact distribution of responsibilities and tasks.**

In the case of practices, responsibility also arises from the contractually agreed or offered IT service. As a rule, the IT service provider also manages the technology areas for which it is responsible, i.e., which are relevant to it. However, there are also "unmanaged" services for which this does not apply or only to a limited extent. What is more, the IT service provider can take over certain "management" services for technology areas without being responsible for the technology area itself, because the user organisation (possibly with the help of another IT service provider) selects and installs the relevant IT systems and components.

Looking at each individual subject area thus helps to determine the exact distribution of responsibilities and tasks and to establish which parts are assumed by the user organisation and which by the IT service provider. Other parties (such as suppliers) may also be considered. The internal and external supply chain is organised accordingly. If a topic area in the Taxonomy falls within the IT service provider's area of responsibility, the provider must apply the standards/documents assigned to the subject area. The selection procedure just described is called *Provider Scope of Control* [2].

For an "unmanaged service", for example, some of the practices describing the maintenance of IT security do not apply or apply only to a limited extent because they are not the subject of the contractually agreed service. And obviously, certain technology areas are only relevant if the corresponding technology is installed in the IT

service in question. If a subject area is relevant, the standards/documents assigned to it must be applied. At the same time, clarity is created for contracts to be concluded.

The main applications of the Taxonomy are:

- Gain an overview and support communication and understanding,
- Organise documentation (documents) and find them more easily,
- Identify tasks and assign responsibilities,
- Understand division of labor in IT service delivery and manage supply chains internally and with suppliers and customers (refer e.g. to [7]),
- Organise collaboration between IT service provider and user organisation in terms of Joint Security Management (JSM),
- Compilation of documents/ standards relevant (to be applied) for a specific IT service as a basis for implementation, operations and contractual agreements in the supply chain.
- Orchestrate activities.

In this way, the Taxonomy becomes a practical tool for information security management (more precisely information service security management).

V. Details

The following sections describe each subject area in the form of a brief profile. The individual security aspects and measures are not described. This is reserved for the documents/standards of the respective organisation detailing the subject area in corporate standards. In order to achieve a common understanding and facilitate coordination, only a brief outline is given of the processes, tasks, products, solutions, etc. covered by each area.

Note: A simple structure with user organisation and IT service provider is used throughout the paper. Of course, the IT service provider has suppliers, and the user organisation may use IT services from more than one IT service provider. This is not discussed further here. The structure and descriptions must be adapted accordingly to also reflect these cases.

V. I. Practices

The practices (upper half of the taxonomy, see Figure 2) are organised into five phases that follow the lifecycle of the business relationship between the user organisation and the IT service provider. The five phases (and thus clusters of the Taxonomy) are: Initiate (not labeled), Protect, Detect, Correct/Readjust, and Advance.

Following the idea and logic of Joint Security Management (JSM) [5], almost all subject areas require both parties to collaborate and coordinate, as well as define the specific tasks with interfaces and responsibilities. Eighteen subject areas with practices have been defined, which are outlined in Table 1.

Table 1: Brief profiles of the "Practices" subject areas

Cluster: Initiate	Relevant for the user organisation
Demand Mgmt. and Compliance **» DMC «**	In the business initiation phase, the user organisation is primarily concerned with knowing its own requirements and documenting them. The need for security and the general security requirements are identified by analysing legal regulations, industry-specific requirements and internal corporate specifications. Procurement is prepared by investigating possible suppliers and their offerings (market analysis) and developing plans for organizing procurement.
Cluster: Initiate	**Relevant for the IT service provider**
Secured by Definition and Assurance Mgmt **» SDA «**	Before customers come into play, the IT service provider must align its security management with the core business of its industrialised IT production ("Secured by Definition" principle). However, the actual and central task in the context of Joint Security Management (JSM) is to align security management with IT services and customers. To this end, service and security specifications for customers are developed and marketing, sales, and contract management are aligned toward meeting customers' information needs about IT security ("Assurance Management").
Portfolio and Systems Development **» PSD «**	The IT services offered (offerings) and their descriptions form a basket called service offering portfolio or simply portfolio. The service catalog which describes the offerings is made available to the user organisations. The Systems Development Lifecycle is a process for the development of evidently reliable and secure IT systems and IT services. It includes activities that are carried out with the aim of ensuring that the IT systems and IT services meet the requirements by correctly providing the required functionality and not more. This means that the requirements are implemented correctly without creating vulnerabilities.

Cluster: Initiate	Relevant for the user organisation and the IT service provider
Offering, Procurement and Contracting **» OPC «**	A procurement decision is based on a thorough and comprehensive comparison between the customer's own requirements and the security measures implemented by the provider. In a more complex business or contract (deal), this can only be put into practice with a systematic approach, because more complex customer solutions are put together from various building blocks described in the service catalog. Both parties must define specific interfaces and assign roles in order to cooperate in the sense of the Joint Security Management (JSM) also in the operating phase.
Cluster: Protect	**Relevant for the IT service provider and also the user organisation**
Education, Training and Guidance **» ETG «**	Knowledge and skills are the prerequisite for achieving improvements and meeting new challenges. However, guidance, education, training and the like also enable people to make appropriate use of the resources provided, to follow guidelines, rules and procedures and to understand the consequences of deviations and violations.
Documentation Maintenance System **» DMS «**	The Documentation Maintenance System defines processes, procedures and roles for the development, modification, release, and distribution of documentation/standards for IT security. This is a continuous task. An editorial office orchestrates the maintenance of the documents, organises the necessary quality checks and approvals releases and thus ensures that they are up-to-date, correct, and consistent. All documents are accessible via a central library.
Implementation, Commissioning, EOL **» ICE «**	The planning, communication, implementation, verification (testing) and transition to operation (commissioning) is carried out in such a way that all relevant technical and non-technical security aspects are taken into account, including hardening. Prior to commissioning, operation is prepared with all related activities for maintenance and continuous improvement. Provisions are made for a secure end-of-life (EOL).
Security Governance andOrchestration **» SGO «**	Governance is achieved through a system for effective management and control that includes guidelines and methods for control (in the sense of management and auditing) as well as a corporate organisation and suitable corporate processes (ISMS). The essential tasks also include the coordination of the various activities and responsibilities among each other (orchestration).

Supply chain management **» SCM «**	The IT service provider integrates components, systems and services that it procures from suppliers. The security properties and other characteristics of these components, systems and services, as well as the possibility of corrections and the process for achieving them, must be analysed and contractually agreed. But even the selection of suppliers has an influence on IT security.
Cluster: Detect	**Relevant for the IT service provider and also the user organisation**
Security Risk Management **» SRM «**	IT security and compliance can be impaired by various circumstances. Security risk management includes the identification of risks, the analysis and categorisation of risks, and the definition of measures for risk treatment, which also includes the reduction of risks to an acceptable level.
Assurance Verification and Certification **» AVC «**	Audits and assessments lead to a higher degree of assurance that there are no non-accepted risks and that contractual commitments are being met. Audits that strive for completeness often lead to a confirmation in the form of certificate (certification). However, there is a large number of usually less formal sport checks such as design reviews, audits and penetration tests.
Logging, Monitoring & Security Reporting **» LMR «**	Logging and monitoring include all activities and tools required for central log management and analysis (SIM) as well as for monitoring (SEM) and scanning of systems, components and applications (including SAST and DAST). Security Information Management (SIM) includes log data collection, centralised storage, filtering, normalisation, correlation, and analysis. Security Event Management (SEM) comprises real-time processing of log data, event data processing, and correlation and analysis of events. SEM also includes the monitoring of IT by a security operations center (SOC), which identifies and evaluates attacks on IT. Scanners for systems, components and applications (e.g., SAST and DAST) are used to detect vulnerabilities and compliance violations. Security reporting includes the evaluation and provision of security related information to users and operators.

Cluster: Correct/ Readjust	Relevant for the IT service provider and also the user organisation
Vulnerability Assessment and Mitigation Planning **» VAM «**	This process ensures that vulnerabilities are systematically identified and tracked, that they are assessed in particular with regard to their potential impact and that remedial measures are planned. The planning of remedial actions initiates the remediation/elimination of vulnerabilities (mitigation). Remediation/elimination is performed using other operational processes (incident, change and problem management). The process includes CERT info services or their use and the processing of the results from the checks in accordance with » AVC « and logging and monitoring in accordance with » LMR «.
Change, Patch and Problem Management **» CPP «**	Changes are modifications to IT components that are primarily requested as a result of orders, inquiries, incidents or problems. Change management is the lifecycle process from request and analysis to implementation and final review. Changes also include patching. Problems are the cause of failures or incidents in the provision of IT services. Problem management is the life cycle process from occurrence, notification, analysis, and identification of the causes to the planning of remedial measures and changes. In most cases, incidents are initially handled provisionally (work around, see » IMF «), so that only the elimination of the actual problem leads to an improvement. However, customer requests etc. can also be the reason for improvements.
Incident Management and Forensics **» IMF «**	Incident management includes all procedures and means used to address and respond to security-relevant circumstances that have or may have a significant impact and require timely resolution through implementation of temporary solutions (work around) or elimination of the root cause. The search for the root cause branches into the problem management. Forensics is the reconstruction of past (security-relevant) events with the aim of finding causal agents or causes.

IT Service Continuity Management **» ISC «**	IT Service Continuity Management takes precautions to minimise the impact of possible interruptions in the provision of IT services or data loss, including the timely and complete recovery of services and data.
Cluster: Advance	**Relevant for the IT service provider and the user organisation**
Review and Initiation of Modernisation **» RIM «**	There are very many and very different reasons why renewed agreement between the user organisation and the IT service provider is necessary also in the operational phase. Both parties continuously compare what has been achieved with current expectations (review) and develop proposals for improvements. Often, however, technical progress or changes in the business environment are also the reason for initiating improvements. In the broadest sense, this is about relationship and contract management as a component of the business that must be prepared for and master such situations.
Modernisation and Innovation Projects **» MIP «**	One of the most important goals in the improvement of IT services or their security is to increase effectiveness and efficiency. It is often the case that the corresponding development and realisation projects go beyond the existing contract and are carried out additionally or lead to changes in the existing contract. While improvements in the direction of efficiency are usually initiated by the IT service provider in order to remain competitive, projects to increase effectiveness are often also initiated by the user organisation. The issue here is the project implementation initiated in accordance with » RIM «.

Note on the subject area “Secured by Definition and Assurance Mgmt (SDA)”: The “Secured by Definition” principle is described in detail in [4]. The Joint Security Management (JSM) is described in [5]. Also refer to the explanations about “Assurance Management” at the end of the paper [6].

V. II. Inventory management

The four areas related to "Inventory management" (discovery, inventory and managing items and IDs) in the middle of the Taxonomy form the basis for many of the practices in the top half of the Taxonomy. However, they are also closely related to technologies in the lower half of the Taxonomy. The four subject areas are outlined in Table 2.

Table 2: Brief profiles of the "Inventory management" subject areas

Cluster: Inventory management	Relevant for the IT service provider and also the user organisation
Ownership and Device Attestation **» ODA «**	Especially in IoT and OT environments, but also in office IT, many, often different devices, systems, components, etc. are used. They receive connections and access to other systems and components. It must therefore be ensured that they are only used after an initial check of certain parameters (device attestation), which is usually repeated on a regular basis. This presupposes that ownership is clarified.
Asset and Configuration Management **» ACM «**	Asset management is the process responsible for tracking and reporting on the value and ownership of IT systems and components throughout their lifecycle. Configuration management is the process responsible for maintaining information about all components that are required to provide an IT service, including their relationships.

User Identity Management **» UIM «**	This includes all procedures and regulations, systems and services u This includes all procedures and regulations, systems and services used to create and manage digital identities, including rights and other attributes for users. A person's digital identities are described as “personalised identity objects” that are associated with other identity objects such as location, organisation, legal entity, etc. These identities are managed throughout their lifecycle. Digital identities and their management form the basis for access management (granting of rights in the operational phase). sed to create and manage digital identities, including rights and other attributes for users. A person's digital identities are described as “personalised identity objects” that are associated with other identity objects such as location, organisation, legal entity, etc. These identities are managed throughout their lifecycle. Digital identities and their management form the basis for access management (granting of rights in the operational phase).
Privileged Identity Management **» PIM «**	This includes all procedures and regulations, IT systems and services used to create and manage digital identities, including rights and other attributes for operational staff (administrators; privileged users) and automated processes. The digital identities are described as “personalised identity objects” associated with other identity objects such as location, organisation, legal entity, etc. These identities are managed throughout their lifecycle. Digital identities and their management form the basis for access management (granting of rights in the operational phase).

V. III. Technologies

The arrangement of the technology areas (lower half of the Taxonomy, see Figure 2) is based on a simple technical IT architecture, with the "clients" on the left, the "servers" on the right and the connecting networks in the middle. Added to this are Security Services (center above Network Services) as a fourth cluster. - There are 19 subject areas of technologies, which are outlined in Table 3.

Note that the clusters are mainly used to support orientation. The networks in the data center are considered being part of the computing IT stack. The outer network interface of the data center is, however, described in the cluster "Network Services". The definition and arrangement of the areas shall allow covering as many concreate installations as possible.

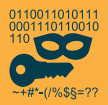
Table 3: Brief profiles of the "Technologies" subject areas

Cluster: Endpoint Services	Relevant for the IT service provider and/or the user organisation
Mobile Workplaces **» MWP «**	Computer devices and associated software with a user interface for one person that is designed for mobile use and usually also enables connection to public wireless networks. These include notebooks and various types of smart phones. The workplace software can also be virtualised and hosted as an "application" in the data center. The focus is on protecting the data stored and processed on the device.
Office Workplaces **» OWP «**	Computer devices and associated software with a user interface for one person, designed for stationary use and usually using a connection to a local fixed or wireless network. This includes desktop computers in various form factors. The workplace software can also be virtualised and hosted as an "application" in the data center. The focus is on protecting the data stored and processed on the device.

LAN and Campus Networks **» LCN «**	All devices between the users' computing devices in stationary use (see » MWP « and » OWP «) and a wide area network (» WAN «), i.e., in the users' central communications periphery. This includes site-to-site gateways, firewalls, intrusion detection/prevention solutions (IDS/IPS), domain services and the components of local networks.
Cluster: Network Services	**Relevant for the IT service provider and/or the user organisation**
Wide Area Network (underlay) **» WAN «**	Physical-logical network that covers greater geographical distances with all components for transmitting data between users and between users and IT systems in data centers. The wide-area networks include the Internet, but also leased lines and other transport networks such as MPLS and mobile communications.
Wide Area Network (overlay) **» SDW «**	This includes all components of an additional control layer (overlay: control layer, data plane), which is located above a system of physical-logical wide-area networks (see » WAN «) or wide-area network services based on them (underlay: data layer, data plane) and which are used to provide combined wide-area services. This network architecture (SD-WAN) implements network virtualisation for wide-area services on a large scale.
Data Center Connectivity **» DCC «**	This technology area forms the outer logical network interface of the data center for users (» UIM «) and contains components that connect the internal networks in the data center (» DCN «) with the wide area networks (» WAN «). The area plays an important role in connecting users with the IT systems in the data center and thus with their applications. The area includes, for example, VPN gateways, MPLS gateways, load balancers, routers, IDS/IPS solutions and DDoS protection.
DMZ and Central Services **» DCS «**	This technology area contains components that are provided centrally to support or enable users' communications via the data center's external logical network interface (» DCC «). Components included are those for email security and archiving, file sharing, and directory services, LDAP, Active Directory, other authentication servers, Web SSO and identity federation services, application-level gateways including proxies and reverse proxies, and Web application firewalls (WAF).

Cluster: Compute Services	Relevant for the IT service provider and/or the user organisation
Data Center Housing **» DCH «**	The building of the data center including the land, insofar as facilities located thereon (such as fences, surveillance systems, etc.) serve to secure the data center. The area includes all physical and environmental security aspects of the data center and its facilities. It does not include network and computing technology (IT) with the exception of facilities for access control and monitoring, i.e., those that serve physical protection.
Data Center Networks **» DCN «**	All networks and network equipment within the data center that transport user data and connect computer systems to each other, to the data center's external logical network interface (» DCC «) and central storage. The entire network and the whole network equipment is located "inside the firewall." The connectivity between data centers is also included, insofar as they are special networks used for this purpose. Not included are facilities for connecting operational personnel (administrators; privileged users) to computer systems, storage, and systems to support the operation and maintenance of the networks, computer systems, and storage. For this, see *Infrastructure for Privileged Users (» IPU «).*
Computer Systems (Server) **» CSS «**	This technology area includes all parts of the IT stack with the exception of applications (software for business process automation, for example), central storage and middleware (runtime environments and database management systems). The domain thus includes the physical computers, operating systems, system virtualisation software such as hypervisors for cloud computing, and local software for hardware abstraction and networking for distributed container solutions. The domain essentially corresponds to a "host system" on which "guest machines", "virtual machines", "workloads" or "containers" (see » APP «) are executed.
Apps and Middleware **» APP «**	This technology complex contains all the software that provides the primary IT services for users (application layer). The complex essentially corresponds to a "guest machine", a "virtual machine", a "workload" or a "container", but does not contain an operating system, as this is provided centrally as an image except in dedicated systems. The complex does not include platforms and infrastructure services. For this, see *Computer Systems (Server) (» CSS «).* Middleware such as run time environments (for example, .NET) is also included. Exceptions are those for containers (see » CSS «) and database management systems (see » DSS «).

Platform Mgmt. Systems **» PMS «**	This includes all central components such as management software, databases, archives, toolsets and utilities to provision, start, stop, move and otherwise manage "guest machines", "virtual machines", "workloads" or "containers" (see » APP «). These central components are used by operating personnel (administrators; privileged users) who manage the entire IT infrastructure. However, access can also be granted in full or in part to less privileged user groups at the user's premises, for example in the form of self-service portals. Also included in this area are all procedures, toolsets, service programs and background systems used for the creation and configuration (engineering) as well as the inventory and archiving of required software components.
Database and Storage Systems **» DSS «**	All central storage systems (storage) and associated software accessed by computer systems (» CSS «) via data center networks (» DCN «). The scope also includes database management systems (DBMS), even if they run on the computer systems. Database management systems (DBMS) have been excluded from the *Apps and Middleware* (*» APP «*) domain. The scope also includes all resources for backup and disaster recovery.
Operations Support Systems **» OSS «**	This includes all central components such as management software, data bases, archives, toolsets and utilities that are used by the operating personnel (administrators) for the basic operation of the data center and the management and maintenance of the IT infrastructure. This includes the technology (hardware, software) for IT service management (for example, ticketing systems), asset and configuration management (CMDB), release and deployment management (for example, software repositories), log management, service availability and performance management, and for ordering and project management. The processes and use of the systems are not included.
Infrastructure for Privileged Users **» IPU «**	This technical infrastructure comprises all networks and network equipment as well as other devices and equipment that enable operating personnel (administrators; privileged users) to access the data center and its components remotely in order to perform management and maintenance tasks. This includes facilities such as jump servers and centrally provided services for authentication and authorisation, for example. Not included are the workplace computers of the administrators (see » MWP «, » OWP «) and workplace extensions used for secure communication over a WAN and to gain access to networks in the data center.

Cluster: Security Services	Relevant for the IT service provider and/or the user organisation
Data Security and Privacy Services  **» DSP «**	This technology complex comprises security services that are put in front of third-party IT services and supplement the security services that these IT services (mostly cloud computing services at the application level, see » APP «) do not have themselves. Security services include data encryption, various forms of data masking, as well as authentication and authorisation services including single sign-on and the like. The solutions summarised here work as proxies and are often referred to as cloud security gateways.
Forward Security (as a Service) **» FWS «**	Combination solutions provided centrally as an IT service and not on the end-point that protect users against threats from the network and applications available there. The components include content filters and anti-malware (e.g., in the form of Secure Web Gateways, SWG), proxy services, and Firewall-as-a-Service (FWaaS) or cloud firewalls, in which all data traffic is redirected to a cloud service of the provider and checked and controlled there.
Apps Security (as a Service) **» APS «**	Combination solutions provided centrally as an IT service that protect applications (see » APP «) in reverse proxy mode against threats from the network and provide security services for these applications (see » APP «), also known as cloud app security. They include, for example, services for log management, analysis of data traffic (cloud discovery), API protection, or discovery solutions for finding unauthorised applications (shadow IT).
Zero Trust Access Components **» ZTA «**	Solutions that act as sole intermediaries to control access to specific IT services (usually applications, see » APP «) by authenticating users and, if applicable, the devices they use each time they access them, as well as checking the context and other rules. The architecture and components used differ depending on whether the Zero Trust principle is initiated by the endpoint or the IT service.

Many components and solutions, including those for IT security, were not mentioned in the brief descriptions above. But all components and solutions should be able to be assigned to the subject areas in the Taxonomy. Here are two examples of IT security solutions: CASB combines components of Forward Security (as a Service) (FWS) and Apps Security (as a Service) (APS). SASE is an architecture. It comprises various components and solutions that lie logically between the cloud services that are accessible via the Internet (Internet edge) and the user who wants to use such a cloud service or application (service edge). These components and solutions include network services and security services (see Figure 2). Network services include components from Wide Area Network (underlay) (WAN) and Wide Area Network (overlay) (SDW) domains as well as from accesses such as » LCN «, » DCN « and » DCS «). Security Services include security services in the form of Forward Security (as a Service) (FWS) and Apps Security (as a Service) (APS) as well as access control with Zero Trust Access Components (ZTA).

VI. Summary and outlook

Threat agents may not tamper with our best protected areas but look for our weakest points. That's why a comprehensive picture is required helping to create and maintain a secure integrated whole. The chain is as strong as its weakest link. This means that every activity along the in-house (self-controlled) and external value chain (with suppliers and customers) can be a source of errors (vulnerabilities) that can lead to IT security risks. To prevent this, not only are security standards required, but suitable tools are needed to gain and maintain an overview. These tools must be kept simple, so graphical representations such as the Taxonomy presented in this paper are suitable. It must be remembered that the value chain or supply chain is not rigid: Rather, it almost always depends on the IT service in question and often also on the contractually fixed division of labor (extended Service Model, see [8]) between the IT service provider and the user organisation. The Taxonomy thus also becomes a tool that helps to organise cooperation between the IT service provider and the user organisation (Joint Security Management, JSM) and allows the security standards belonging to an IT service to be located and applied.

For operational use, the Taxonomy should be part of a broader architecture. In particular, it should be associated with a hierarchy of documents/standards [2]. Furthermore, the modular and hierarchical way of describing should be continued in the individual documents/standards [2]. This not only makes information easier to find, but also allows it to be updated flexibly and with less effort. An appropriate system of identifiers (codes, IDs) facilitates referencing.

Complexity is the opponent of good IT or cybersecurity. With the help of a Taxonomy, it can be reduced and made controllable. An overview is gained, and communication and understanding are supported. Tasks can be identified more easily, gaps identified, and responsibilities assigned. This makes it an important management tool.

The author likes to thank his colleague Thomas Hecht for discussing the structure of the Taxonomy which considerably helped to elaborate it.

A. References and Applicable Documents

[1] Eberhard von Faber: IT und IT-Sicherheit in Begriffen und Zusammenhängen, Thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen; Springer Vieweg, Wiesbaden 2021, 289 pages, 64 color illustrations, ISBN 978-3-658-33430-7, https://doi.org/10.1007/978-3-658-33431-4

[2] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialised IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, pages 382, figures 159, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9

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

[4] Eberhard von Faber: Methods: "Secured by definition" and the utilization of quality management principles, Seamless IT security through integration within IT-production processes; Translation of article originally published in: Datenschutz und Datensicherheit - DuD, 43(7), July 2019, Springer Fachmedien, Wiesbaden 2019, ISSN 1614-0702, pp 410-417, https://zero-outage.com/opinion/methods-secured-by-definition-and-the-utilization-of-quality-management-principles/

[5] Eberhard von Faber and Wolfgang Behnsen: Joint Security Management: acting across organisations (More security in the age of cloud computing, IT services and industrialised IT production); Springer Vieweg, Wiesbaden 2018, 246 pages, 60 color illustrations, ISBN 978-3-658-20833-2, https://doi.org/10.1007/978-3-658-20834-9

[6] Eberhard von Faber: On the future of IT security management in the face of changes in technology and service delivery; translation of the article published in: Datenschutz und Datensicherheit - DuD, 45(10), October 2021; https://zero-outage.com/opinion/on-the-future-of-it-security-management-in-the-face-of-changes-in-technology-and-service-delivery/

[7] ISO/IEC 27036 - Information technology – Security techniques - Information security for supplier relationships - Part 1: Overview and concepts, Part 2: Requirements

[8] Enhancing Cloud Security Standards; Zero Outage Industry Standard, June 2022, 20 pages, https://zero-outage.com/the-standard/security/; based upon: Eberhard von Faber: Concept for considering different Service and Deployment Models in cloud security standards; Translation of the article published in: Datenschutz und Datensicherheit - DuD, 46, Januar y 2022, https://zero-outage.com/opinion/concept-for-improving-cloud-security-standards/

Zero Outage Industry Standard Ltd.
Suite 1, 3rd Floor
11-12 St. James's Square London
SW1Y 4LB
United Kingdom

zero-outage.com