Translation using DeepL.com of the article originally published in: Datenschutz und Datensicherheit - DuD, 46, pp. 45-51 (2022), Springer, ISSN 1614-0702, https://doi.org/10.1007/s11623-022-1559-x

Eberhard von Faber

Concept for Improving Cloud Security Standards

Consideration of the very diverse Service and Deployment Models with only two requirements

Widely used cloud security standards define general security measures/controls for securing clouds while not differentiating between the many, well-known implementations that differ with respect to the Service and/or Deployment Model they implement. Users are thus lacking guidance for decision-making and for preparing to ensure end-to-end security. This paper proposes a concept for cloud security standards to really cover and consider virtually all possible Service Models and Deployment Models and, as a result of this, supports differentiating between offerings and improve the support for user organizations for which the standards are also built for.

1 Problem: The effect of different clouds is not really considered yet

Different implementations of cloud computing services entail differences in their risk profile. If risks are different, users (Cloud Service Consumer, CSC) should be informed about this to be enabled to take a sound purchasing decision and later to use the cloud appropriately. However, well-known cloud security standards ([1], [2], [4]) are not sufficiently differentiating between different cloud computing implementations. Little differentiation between different cloud computing services leaves many questions open but it also doesn't say much about the security gain for the customers when preferring one cloud to another.

What are such differences that lead to a specific risk profile and why are different IT security measures implemented?

- Gartner predicted in 2015 for the next five years that about 95% of security failures would be caused by the party setting-up and configuring the cloud service and not by the Cloud Service Provider (CSP) providing the cloud computing core services and additional optional components. It can be assumed that the CSP would not make these security failures if he would also take responsibility for the set-up and final configuration of the users' individual cloud service. This example demonstrates that the division of labor does have an influence on the level of security of the cloud service. In a wider sense, the distribution of responsibility and work is subject to the Service Model. That's why the *cloud's Service Model* must be detailed. Otherwise, there is the danger of having gaps in the overall course of activities and no party feels responsible or is appropriately prepared for or capable of ensuring security.
- It is also well known that the *cloud's Deployment Model* has an influence on the risk profile. Users (Cloud Service Consumer, CSC) are concerned putting some of their applications and data into a Public Cloud. The organization of the access to and the use of the cloud computing service, the location of data processing and storage etc. are important factors that influence the risk profile, compliance issues and maybe also the level of IT security. There are many ways to deploy a cloud computing service. That's why the *cloud's Deployment Model* must be detailed and made transparent. Otherwise, users (Cloud Service Consumer, CSC) cannot judge the security implications of using the provided cloud service.

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

Cloud security standards such as the CSA Cloud Controls Matrix (CCM) of the Cloud Security Alliance (CSA) [1] refer to different Service Models though only three typical models are used (IaaS, PaaS and SaaS). ISO/IEC 27017 [2] provides details but it can only refer to typical cases such as IaaS and discuss options. Though, reality is much more complex. Service Models in the wider sense of division of labor is not analyzed and treated in detail. At least users (Cloud Service Consumer, CSC) require more detail.

Moreover, e.g. the CSA shared responsibility model [3] often assigns the responsibility to neither the user organization (Cloud Service Consumer, CSC) nor to the IT service provider (Cloud Service Provider, CSP) alone but to both parties ("shared"). This more or less means that, before closing the contract, a security concept must be developed, communicated and negotiated between the parties. That seems to put us back since the cloud started with the customer promise of high standardization and rapid deployment/provision.

Cloud security standards such as the Cloud Computing Compliance Controls Catalogue (C5:2020) of the Federal Office for Information Security (Germany) [4] do mostly not differentiate between different Deployment Models. Nevertheless, the different models such as the Private, the Virtual Private and the Public Cloud considerably differ in their risk profile. Customers are left alone without being informed about such differences and their possible consequences.

Not differencing between the different Service and Deployment Models also causes another problem: Publicly available standards sometimes contain security measures that simply cannot be implemented, or state requirements that cannot be met. Frequently, the authors have a Public Cloud environment in mind when it comes to e.g. customer self-service. Even if a self-service is provided in Private or Virtual Private Cloud environments, this would be solved slightly different. Also, all transparency requirements (information from logging, monitoring etc.) strongly depend on the division of labor (extended Service Model). The party being responsible for actively managing the cloud or a part of it requires much more information than the party only consuming the cloud computing service. This is also often mixed, or a Public Cloud which is not fully managed by the provider is assumed to be the standard for all other implementations which is by far not the case.

2 Solution: specifying and implementing Service and Deployment Model Patterns

It is the aim of the following proposal to ensure that the Cloud Service Provider (CSP) delivers enough information to user organizations (Cloud Service Consumers, CSC) allowing the latter to take an informed and sound purchasing decision. Delivering comprehensive information is also required to ensure that the user organization is willing and prepared to contribute to IT security so that the operated cloud service is and remains an overall integrated secure whole [5].

It is, however, not possible to exactly specify each of the possible cloud computing services together with their security features in one document or standard. The diversity is too high, and IT service providers are presenting new models regularly.

- ▶ With this paper it is proposed that the Cloud Service Providers (CSP) must specify "patterns" that specify the Service and the Deployment Model in appropriate detail (refer to below). It is furthermore proposed that the cloud standard requires the Cloud Service Provider (CSP) to implement and operate the cloud computing service according to and in line with the Patterns just mentioned. This also means that other security measures (controls) defined in the standard are implemented according to the Pattern and maybe modified if required.
- ▶ This paper defines rules and proposes templates for Service Model Patterns and for Deployment Model Patterns. Patterns from different Cloud Service Providers (CSP) should have a similar structure and perhaps use a similar language. If so, the Pattern are compatible and support the comparison of different cloud computing services. This also means that cloud security standards should specify design rules for the Patterns.

The proposed Patterns are deemed sufficient to inform the user organization (Cloud Service Consumer, CSC) about important security related aspects of different Deployment models. They are also deemed sufficient to inform the user organization (Cloud Service Consumer, CSC) about the sharing of responsibilities or the division of labor between the user organization and the IT service provider (Cloud Service Provider, CSP). These Patterns also deliver the context for all other information about the cloud's IT security.

Using the Patterns, user organizations (Cloud Service Consumer, CSC) can differentiate between the different cloud service offerings and make an informed decision, now also knowing exactly what is delivered and what is left to them. Cloud Service Providers (CSP) can generate competitive advantages by delivering detailed Patterns. By doing so, they also ensure that IT security is treated by both parties (see [5]) in order to achieve an overall integrated secure whole.

3 Foundation: Models that need to be considered

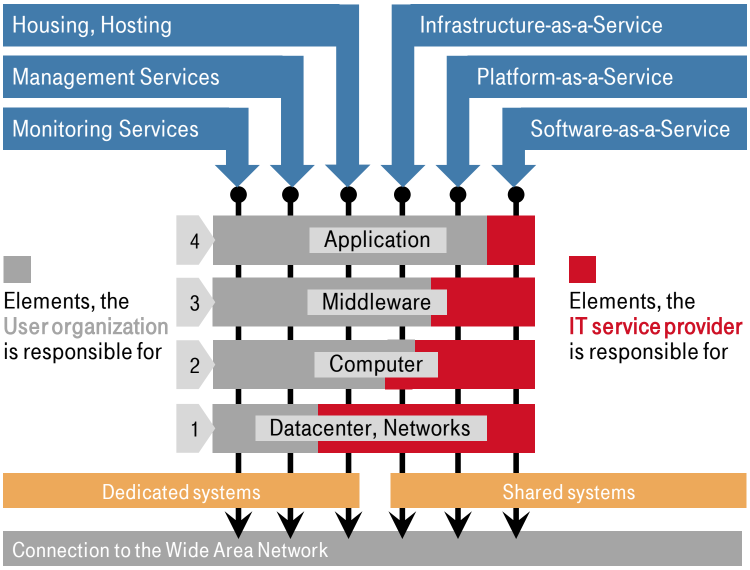
This chapter provides some foundational information about Service Models in a wider, extended sense (3.1.) and Deployment Models (3.2) that are used later to provide a structure for the Patterns.

3.1 Different Service Models: Who is responsible for what?

Service Models are characterized by a specific division of work or labor within the IT stack. Figure 1 shows six IT stacks each referring to a specific Service Model (top of figure). The division of labor is indicated by different color of the elements in the IT stack (center of figure). The figure does not cover cloud computing services only, since the term Service Model is used for IT service provision in general.

The figure gives a general overview about some existing Service Models in regard to whom (user organization or IT service provider) is responsible for what part of the IT stack. The user organization is responsible for the bright areas (shown on the left-hand side of the figure). The IT service provider is responsible for the dark areas (shown on the

Figure 1: Service models: division of work within the IT stack (source: [6])



right-hand side of the figure). Further, this figure shows which Service Model is typically based on dedicated systems and shared systems.

The three models on the left are services which the IT service provider provides for IT components/systems that are owned by the user organization. Refer to Figure 1. The three models on the right refer to cloud computing:

- Infrastructure-as-a-Service (IaaS),
- Platform-as-a-Service (PaaS), and
- Software-as-a-Service (SaaS).

In their plain form these Service Models simply describe what party (CSC or CSP) is supplying and therefore taking responsibility for the IT components running on computer systems which are provided by the Cloud Service Provider (CSP). In case of bare metal virtualization, the "IT components running on computer systems" constitute the Virtual Machines (VM).

This structure is not very granular. Also, management activities (updates, monitoring etc.) are not assigned at all. That's why we extend the meaning of Service Model. In the wider sense, the Service Model shall also determine the division of work and assignment of responsibility during implementation and operations including the IT service management activities as stipulated in ITIL® and ISO/IEC 20000.

Performing e.g. maintenance activities requires access to components in the IT infrastructure. Consequently, different service models require different access rights, connectivity etc. This shall also be considered by the Service Model (provided that different assignments are possible). Note that these aspects are not shown in Figure 1.

The main differences between the different cloud Service Models are the source of the IT components constituting the Virtual Machines (VM) and/or which are used by the VMs. The extended Service Model would require defining which party is responsible for and doing what activity in the overall lifecycle from provisioning and configuration all the way to the operations phase (covering management activities including incident management etc.) till decommissioning and/or transfer or deletion of data. Note that, depending on this division of labor, the cloud computing infrastructure may need to be architected differently. Even performing monitoring tasks and also executing management activities require having access which in turn may require a specific form of connectivity.

3.2 Different Deployment Models: For whom and how is it provided?

Cloud computing environments can be constructed and implemented differently while organizing the access to and the use of the cloud computing service in different ways. These different models are referred to as Deployment Models. The most commonly known Deployment Models are

- Private Cloud,
- Virtual Private Cloud,
- Public Cloud, and
- Community Cloud.

Hybrid Cloud is a mixture of such models. To show their differences they are often compared with a solution which is implemented and operated by the user organization in its own datacenter. This model (which is not a cloud computing service) is often referred to as "on premise". Figure 2 shows three Deployment Models of cloud computing and the "on-premise" solution for the sake of comparison. For each Deployment Model some characteristics are given. Note that the term "user" rather refers to the contracting party of the Cloud Service Provider (CSP), i.e. to organizations and not to individuals using the cloud.

Different Deployment Models differ in their risk profile. If a cloud computing service is offered to everyone, it must be accessible publicly. Private environments entail lower risks than public ones. Moreover, restricting the users may reduce risks. Sharing the environment with trusted neighbors

Figure 2: Deployment Models (cloud) plus on-premise (source: [6])

Model → Property ↓	On-premise (in-house operation)	Private Cloud	Virtual Private Cloud	Public Cloud
User	operator/provider	associated with operator/provider	associated with operator/provider	unbound or loosely connected
	trustworthy	trustworthy	trustworthy	unknown
Users share cloud instance with	nobody	nobody	several	many
Access (network)	local network, campus network, etc.	Wide area network with restricted access	Wide area network with restricted access	public Internet
Place of production	user organization	IT service provider (defined location)	IT service provider (defined location)	IT service provider (location often not defined)

entails lower risks than sharing it with a great number of unknown parties. So, the Deployment Model does matter when it comes to IT security and risks. Moreover, different Deployment Models may require implementing security measures in a different way.

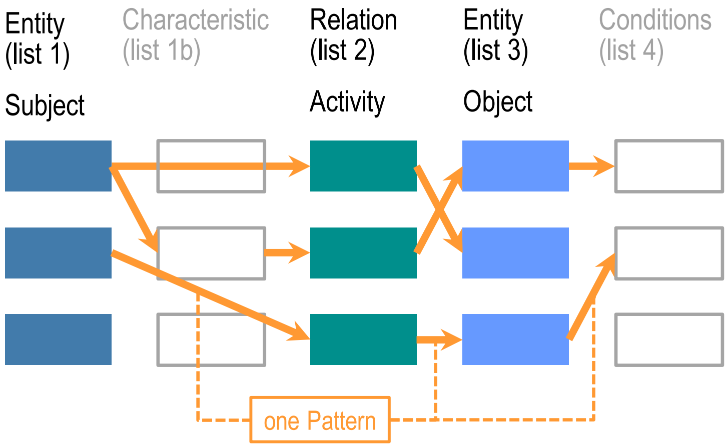
Different Deployment Models do not differentiate with respect to the functionality provided by the core cloud computing service. They differentiate with respect to its use and provisioning. Different Deployment Models require the cloud computing environment to be configured differently. Accesses require connectivity. Networks and accesses are configured differently. Specific components may be required additionally while not be present in other models. Size, products and other technical parameters can be different as well. Though, the cloud computing core service may not differ significantly, other areas are affected and implemented in a different manner.

4 Specification of the patterns

4.1 Format, use and implementation

Format and use:
A Service and a Deployment Model Pattern is a simple expression. It most cases, such a Pattern is a sentence. The Patterns are constructed similarly to statements in an Entity Relation Model know from databases as shown in Figure 3.

Figure 3: The Patterns are similar to Entity Relation Models



It has a simple construction rule: SPO, what in many cases mean “subject – activity – object”. Sometimes, characteristics may be added, and conditions formulated. In Figure 3, a Pattern is represented by a chain of arrows combining entities, activities, and other descriptions.

How are these Patterns produced and used? They are developed for each cloud computing service and describe its essential characteristics. A cloud architect knows these (often) simple facts, and it is easy for him and others to put these facts into such a formal structure. The expressions in form of simple sentences are then used by the user organizations (Cloud Service Consumer, CSC) to understand the nature of the cloud computing service. Based on this, users are able to understand the differences between different offerings and to take a sound decision and prepare for activities left to the user organizations (Cloud Service Consumer, CSC).

Implementation:
The Service and Deployment Model Patterns must obviously reflect reality. They must be observed during design, implementation, and operations.

- To ensure this, two security measures are defined in a cloud security standard which are to be observed and implemented by the Cloud Service Provider (CSP). There are two security measures, one relating to the Service and one to the Deployment Model.
- The security measures are formulated in a general way not being specific to any cloud service. As a result, they can be stated in a general cloud security standard. Examples will be given below in this paper.
- The cloud security standard also defines the structure of the Patterns and rules for building them. It defines entities, relations and, if required, also characteristics and conditions. Structure and level of detail can differ between cloud security standards, but minimum requirements are fixed within one standard to guarantee comparability.
- Guidance for creating such Patterns shall be given. Their structure can be strictly formalized or allow more freedom. Examples for the content will be given below in this paper.
- The two security measures request the Cloud Service Provider (CSP) to characterize the cloud computing service by means of Service and Deployment Model Patterns.
- The two security measures also request the Cloud Service Provider (CSP) to implement, operate and deliver the cloud computing service according to the Patterns he has defined.
- Compliance with the two security measures means that Cloud Service Consumers (CSC) can rely and build on the statements.

The next two sections propose texts for the two security measures and provide more detail about the Service and Deployment Model Patterns. Section 4.2 covers the security measure (security control) relating to the Deployment Model and explains how the Deployment Model Patterns can look like. Section 4.3 delivers this content relating to the Service Model.

4.2 Deployment Model Patterns

Security Measure or Security Control:
This is what the Cloud Service Provider (CSP) shall guarantee (proposed text for security measure): “The cloud computing service is designed and implemented according to predefined Deployment Model Patterns. These Patterns describe characteristics of the cloud computing service’s Deployment Model. As a minimum the following is defined: The Patterns characterize the contracting parties of the Cloud Service Provider (CSP) (which purchase and consume the service) and the level of trustworthiness of these parties

for the CSP. The Patterns also specify if and how many parties are utilizing the same cloud service instance. The Patterns furthermore specify the connectivity used by the parties to access the cloud computing services and specify the location of the cloud computing components."

Explanation:
The Patterns are simply a set of rules or of statements that characterize a specific implementation. Refer to Section 4.1 above and the descriptions below.

The above security measure requires a) the definition of Deployment Model Patterns and b) that these Patterns are adhered to during design, implementation and for planning the cloud's operations.

Different Deployment Models differ in their risk profile. Different Deployment Models may also require implementing other security measures in a different way.

Figure 2 in Section 3.2 above shows three Deployment Models together with the "on-premise" solution for the sake of comparison. For each Deployment Model some characteristics are given that can help to develop the Deployment Model Patterns and/or compile existing material accordingly.

▶ Figure 4 (in the current section) shows how the different Deployment Models can be characterized by Deployment Model Patterns. Compare this Figure 4 with the Entity Relations Schema shown in Figure 3. Four Patterns are shown, each with an example for a Private Cloud offering. It may be necessary to define more or less Patterns and to add more details. The numbered lines contain four templates where the texts in brackets need to be replaced. For each template an example is given how such a Pattern may look like.

Here is some background information about the proposed four Patterns:

Remark on Pattern No. 1: The closer the relation between the Cloud Service Consumer (CSC) and the Cloud Service Provider (CSP)

- the better security responsibilities can be aligned,
- the better security issues can jointly be solved, and
- the more likely possible abuse of the cloud service can be excluded.

Remark on Pattern No. 2: A cloud computing instance, dedicated to and used by one user organization (Cloud Service Consumer, CSC) only, entails a lower risk and perhaps also a higher level of control for the user organization in comparison with a cloud computing instance used by many unknown and maybe unreliable parties.

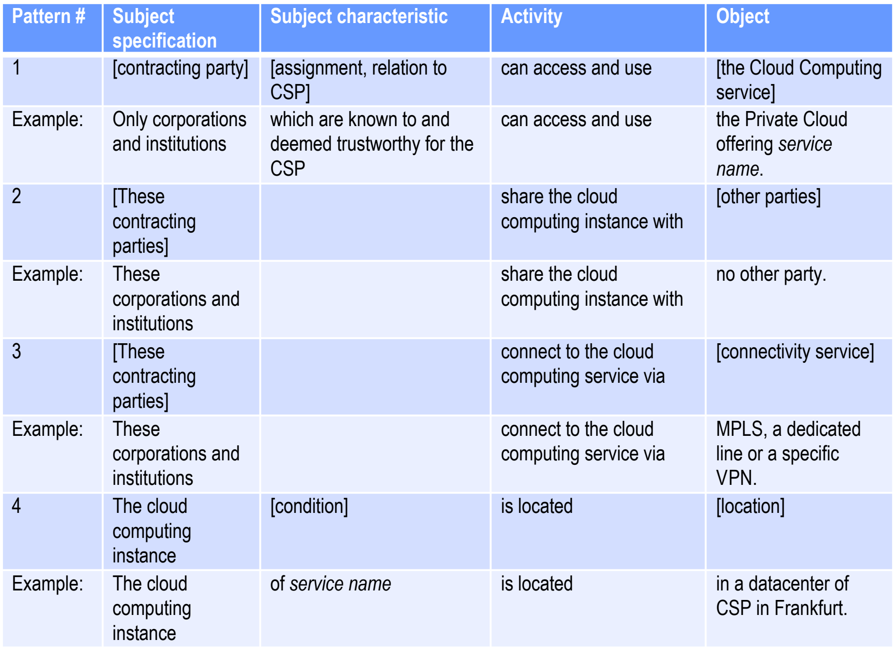
Remark on Pattern No. 3: Obviously, risk exposure is different and depend on the way the users are connected to the cloud computing core service. The chosen connectivity is often a direct consequence of Pattern 1 and 2.

Remark on Pattern No. 4: In many cases, the cloud computing core service resides in datacenters of the Cloud Service Provider (CSP). But there are also models where the technology is located in the user organization's datacenter. These models often use Hyperconverged Systems. Obviously, physical protection and connectivity are different which is affecting IT security and risk profile.

The Deployment Model Pattern are used during design, implementation and for planning the cloud's operations. Whenever required, other security measures are implemented in a way that the Patterns are observed and/or implemented.

The Deployment Model Patterns ensure that the cloud computing service is designed, implemented and planned for operations in a way that access, connectivity, functionality etc. are exactly in line with the Deployment Model's characteristics.

Figure 4: Example for building Deployment Model Patterns (illustrative)



Pattern #	Subject specification	Subject characteristic	Activity	Object
1	[contracting party]	[assignment, relation to CSP]	can access and use	[the Cloud Computing service]
Example:	Only corporations and institutions	which are known to and deemed trustworthy for the CSP	can access and use	the Private Cloud offering *service name*.
2	[These contracting parties]		share the cloud computing instance with	[other parties]
Example:	These corporations and institutions		share the cloud computing instance with	no other party.
3	[These contracting parties]		connect to the cloud computing service via	[connectivity service]
Example:	These corporations and institutions		connect to the cloud computing service via	MPLS, a dedicated line or a specific VPN.
4	The cloud computing instance	[condition]	is located	[location]
Example:	The cloud computing instance	of *service name*	is located	in a datacenter of CSP in Frankfurt.

4.3 Service Model Patterns

Security Measure or Security Control:
This is what the Cloud Service Provider (CSP) shall guarantee (proposed text for the security measure): "The cloud computing service is designed and implemented according to predefined Service Model Patterns. These Patterns describe characteristics of the cloud computing service's Service Model. As a minimum the following is defined: The Patterns identify all user groups accessing the cloud's resources (e.g. normal users, administrators) and characterize the purpose and activities (e.g. end-user access, cloud management, administration of IT infrastructure) as well as the means

used for this (e.g. Internet network connectivity, self-service portal, CSP's admin infrastructure)."

Explanation:
The Patterns are simply a set of rules or of statements that characterize a specific implementation. Refer to Section 4.1 above and the descriptions below.

The above security measure requires a) the definition of Service Model Patterns and b) that these Patterns are adhered to during design, implementation and for planning the cloud's operations.

Service Models are characterized by a specific division of work within the IT stack. Service Models are about distributing responsibility. This in turn requires having the necessary accesses and rights to perform actions. As a result, a Service Model describes "which party or user group is doing what". The Patterns reflect this.

E.g., in case of IaaS and PaaS, the creation and management of the VMs can be performed by Cloud Service Provider (CSP) or by its customers. In case of SaaS, this is usually performed by the Cloud Service Provider (CSP). Implementing connectivity and granting accesses is a security topic. That's why, the Patterns describe a) what party b) does what c) by using what. By implementing the Patterns, it is ensured that connectivity, accesses etc. are intentionally designed and implemented in a secure way.

The identification of means and other IT services that are combined with the cloud computing core service and their characteristics ensures that configurations that are insecure are not used.

▶ Figure 5 (in the current section) shows how Service Model Patterns can be built and look like. The table shows lists of three factors. A Pattern is created by combining items from the three lists. Compare Figure 5 with the Entity Relations Schema shown in Figure 3. Each Pattern has the following structure: A "user group" is enabled and responsible for performing "an activity" and uses "tools and means" for this. Other circumstances can be added as appropriate.

Create as much pattern as required to describe the Service Model being implemented.

The Service Model Patterns are used during design, implementation and for planning the cloud's operations. Whenever required, other security measures are modified or implemented differently to implement the Patterns.

Whenever appropriate, the Patterns may also specify additional IT services (such as connectivity) that are intended and approved for being combined with the cloud computing core service.

Different Service Models are characterized by a specific division of work. This in turn requires having the necessary accesses and rights to perform actions. By implementing the Service Model Patterns, it is ensured that connectivity, accesses etc. are intentionally designed, implemented in a secure way and in line with the Service Model.

5 Summary

Cloud security standards such as the CSA Cloud Controls Matrix (CCM) of the Cloud Security Alliance (CSA) [1] refer to different Service Models though only three typical models are used (IaaS, PaaS and SaaS). Often the standard refers to the CSA shared responsibility model which leaves details open. Service Models in the wider sense of division of labor are not analyzed and treated in detail. Cloud security standards such as the Cloud Computing Compliance Controls Catalogue (C5:2020) of the Federal Office for Information Security (Germany) [3] do mostly not differentiate between different Deployment Models. Nevertheless, the different models such as the Private, the Virtual Private and the Public Cloud considerably differ in their risk profile.

User organizations (Cloud Service Consumer, CSC) do not get all information they require to understand and rate the cloud service when it comes to IT security. They may not have enough information to prepare for the performance of activities which the Cloud Service Provider (CSP) has left to its customers.

Obviously, cloud security standards cannot specify all detail of specific cloud computing services. They must generalize which result in the shortcomings just mentioned.

Figure 5: Example for building Service Model Patterns (illustrative)

List of user groups (UG)		List of purpose and activities (PA)		List of tools and means used for this (TM)
UG1: Privileged users from the CSP (admins)	assign the user group (left) to an purpose/activity (right)	PA1: provision and de-provision admin user accounts and entitlements	assign the purpose/activity (left) to a tool/means (right)	TM1: from within the CSP's internal administration network
UG2: Privileged users from the CSC (admins)		PA2: configure and assign hosts, clusters and resource pools		TM2: via a dedicated WAN access
UG3: Users from the CSC (no admins)		PA3: configure storage		TM3: via a self-service portal connected to the Internet
UG4: …		PA4: create, configure, deploy, copy etc. VMs		TM4: via the Internet
		PA5: start, stop, suspend etc. VMs		TM5: …
		PA6: manage resources and delete VMs		
		PA7: monitor VMs and perform analytics		
		PA8: monitor and control security (SOC)		
		PA9: manage backups		
		PA10: use services provided by VMs		
		PA11: …		
Example:				
Admins from the CSP (UG1)		manage resources and delete VMs (PA7)		from within the CSP's internal administration network (TM1)

This paper proposes a way out using Service and Deployment Model Patterns.

- The Patterns are specific for a certain cloud computing service and provide the information required by Cloud Service Consumers (CSC).
- The Patterns must be observed by the Cloud Service Provider (CSP) during design, implementation, and operations of the cloud computing service.
- Cloud security standards shall comprise two additional security measures (security controls) which require the Cloud Service Provider (CSP) a) to define the Service and Deployment Model Patterns and b) to adhered to these Patterns during design, implementation and for planning the cloud's operations.
- Cloud security standards shall also define rules and provides templates for Service Model Patterns and for Deployment Model Patterns. Then, the Pattern are compatible and support the comparison of different cloud computing services.

Using the concept described in this paper, cloud security standards can really cover and consider virtually all possible Service Models and Deployment Models and, as a result of this, support differentiating between offerings and improve the support for Cloud Service Consumers (CSC) for which the standards are also build for.

The author likes to thank Thomas Hecht for discussing the idea and his feedback. It's always a pleasure working with you, Thomas.

Literature

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

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

[3] Cloud Security Alliance (CSA): Enterprise Architecture to CCM Shared Responsibility Model; 2020

[4] Cloud Computing Compliance Controls Catalogue (C5:2020) of the Federal Office for Information Security (Germany)

[5] 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.

[6] 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.

Cite the original article using
https://doi.org/10.1007/s11623-022-1559-x