

# IT-Grundschutz Compliance on Azure

February 1, 2022  
MICROSOFT DEUTSCHLAND GMBH

# Table of contents

- 1 Executive Summary ..... 4
- 2 Compliance Requirements ..... 5
  - 2.1 Shared Responsibility Model ..... 5
  - 2.2 Modelling Microsoft Azure ..... 7
- 3 Implementation of Module OPS.2.2 Cloud Usage ..... 11
  - 3.1 OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage ..... 13
  - 3.2 OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage ..... 14
  - 3.3 OPS.2.2.A3 Service Definition for Cloud Services by the Customer ..... 20
  - 3.4 OPS.2.2.A4 Definition of Areas of Responsibilities and Interfaces ..... 21
  - 3.5 OPS.2.2.A5 Planning a Secure Migration to a Cloud Service ..... 22
  - 3.6 OPS.2.2.A6 Planning the Secure Integration of Cloud Services ..... 23
  - 3.7 OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage ..... 23
  - 3.8 OPS.2.2.A8 Careful Selection of a Cloud Service Provider ..... 25
  - 3.9 OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider ..... 28
  - 3.10 OPS.2.2.A10 Secure Migration to a Cloud Service ..... 33
  - 3.11 OPS.2.2.A11 Drawing Up Contingency Concept for a Cloud Service ..... 34
  - 3.12 OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations ..... 35
  - 3.13 OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage ..... 37
  - 3.14 OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship ..... 38
  - 3.15 OPS.2.2.A15 Ensuring the Portability of Cloud Services ..... 39
  - 3.16 OPS.2.2.A16 Implementing Backups ..... 41
  - 3.17 OPS.2.2.A17 Use of Encryption When Using the Cloud ..... 41
  - 3.18 OPS.2.2.A18 Use of Federation Services ..... 44
  - 3.19 OPS.2.2.A19 Security Vetting of Employees ..... 45
- 4 Implementation of Minimum Standard for the Use of External Cloud Services ..... 47
  - 4.1 NCD.2.1.01 Strategy for Cloud Usage ..... 50

4.2	NCD.2.1.02 Security Policy for External Cloud Usage.....	50
4.3	NCD.2.1.03 Security Concept for External Cloud Services.....	51
4.4	NCD.2.1.04 Emergency and Continuity Management.....	51
4.5	NCD.2.2.01 Implementation of Security Requirements .....	52
4.6	NCD.2.2.02 Contractually Ensure Dealings with Subcontractors and Other External Third Parties53	
4.7	NCD.2.2.03 Ensure Jurisdiction by Contract.....	53
4.8	NCD.2.2.04 Ensure Location by Contract.....	53
4.9	NCD.2.2.05 Ensure that Disclosure Obligations and Investigative Powers are Contractually Guaranteed.....	54
4.10	NCD.2.2.06 Regulating the Termination of the Contractual Relationship.....	54
4.11	NCD.2.2.07 Ensure Data Return and Data Deletion at the Cloud Service Provider by Contract 54	
4.12	NCD.2.3.01 Integrate ISMS .....	55
4.13	NCD.2.3.02 Verify Security Certifications.....	55
4.14	NCD.2.3.03 Check Performance.....	55
4.15	NCD.2.3.04 Comply with Information Obligations .....	56
4.16	NCD.2.3.05 Enable Two-Factor Authentication .....	56
4.17	NCD.2.4.01 Perform Data Return.....	56
4.18	NCD.2.4.02 Conform Data Deletion.....	57
4.19	NCD.2.5.01 Shared Use of External Cloud Services .....	57
5	Microsoft’s Responsibilities as a Cloud Service Provider.....	59
	Appendix A Glossary of IT-Grundschutz-Terms .....	60
	Appendix B References to Further Information.....	61

# 1

## Executive Summary

Microsoft Azure is Microsoft's public cloud computing platform that enables its customers to build, deploy and manage applications and virtual machines. Azure platform is built on a multi-layered security concept that includes physical security of its data centers, hardware and firmware components with integrated security controls as well as secure operations.

The Azure infrastructure is distributed globally, divided into geographies and regions. In Germany, the two former regions (Germany Northeast and Germany Central) are closed and the new regions as part of the Azure global infrastructure are open since 2019 (Germany West Central and Germany North<sup>1</sup>). Depending on customer preference, data can be stored in one or more regions, e.g. for availability reasons.

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has published (and continues to refine) the IT-Grundschutz methodology. This consists of an ISO 27001 compatible ISMS (BSI Standards 200-1 and 200-2), a dedicated risk analysis method (BSI Standard 200-3), a business continuity management (BSI Standard 100-4; currently under review) and the IT-Grundschutz Compendium, a standard set of threats and requirements for typical business environments.

This workbook aims to support Microsoft Azure customers in applying the IT-Grundschutz methodology within the scope of their existing or planned ISO 27001 certification based on IT-Grundschutz.

Chapter 2 provides an overview of cloud computing in the context of IT-Grundschutz. An outline of how to implement the IT-Grundschutz module *OPS.2.2 Cloud Usage*<sup>2</sup> as part of the Information Domain<sup>3</sup> is given on a per-requirement-basis in chapter 3. Chapter 4 gives information about implementing the BSI minimum standard *Minimum Standard on the Usage of External Cloud Services*<sup>4</sup>, which addresses German federal authorities. Chapter 5 discusses Microsoft's responsibilities as a cloud service provider.

---

<sup>1</sup> <https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/>

<sup>2</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/04\\_OPS\\_Betrieb/OPS\\_2\\_2\\_Cloud-Nutzung\\_Edition\\_2021.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf) (German only)

<sup>3</sup> See Appendix A, Glossary of IT-Grundschutz Terms for normative terms of IT-Grundschutz that have special meanings.

<sup>4</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard\\_Nutzung\\_externer\\_Cloud-Dienste.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.html) (German only)



# 2

## Compliance Requirements

This Azure workbook is based on the revised version of the BSI IT Grundschutz Compendium<sup>5</sup> from the year 2021. This version includes the module *OPS.2.2 Cloud Usage*<sup>6</sup>. It distinguishes between the use of cloud services such as Microsoft Azure and classic IT outsourcing.

### 2.1 Shared Responsibility Model

In a cloud service environment, the responsibility for implementing and maintaining security controls for IT applications is shared between the customer and the cloud service provider, in contrast to on-premises IT infrastructure. A full transfer of responsibilities can only occur when the cloud service provider includes customers' applications in their own certification scope (i.e., a classical outsourcing scenario), including an aligned risk management. It must be pointed out that according to the IT-Grundschutz methodology, final responsibility always lies with the customer (the data owner). Recent versions of IT-Grundschutz allow a shared responsibility model that divides responsibilities between customer and cloud service provider along virtualization boundaries, ensuring that only one party is responsible for any particular aspect.







Table 1 shows a high-level overview of how such a partitioning may look for Infrastructure-as-a-Service (IaaS). The cloud computing model is divided into generalized aspects (see descriptions below). Aspects are the responsibility of the customer, the cloud service provider or both. The table also describes any available support for the customer available from Microsoft in its role as cloud service provider.

---

<sup>5</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT\\_Grundschutz\\_Kompendium\\_Edition2021.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html) (German only)

<sup>6</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/04\\_OPS\\_Betrieb/OPS\\_2\\_2\\_Cloud-Nutzung\\_Edition\\_2021.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf) (German only)

Table 1 Shared Responsibilities for Security in Cloud Computing (IaaS model)<sup>7</sup>

Aspect/Responsibility	Description
<b>Security Concept</b> 	<p>Security concepts are essential to IT-Grundschutz methodology. A security concept is a documented risk analysis with a defined scope. It includes the resulting steps to be taken to increase the security of the system or environment.</p> <p>This document helps to establish a security concept for Azure.</p>
<b>Data classification &amp; accountability</b> 	<p>The value of data can only be determined by the customer, who should therefore identify, classify and label their data and assets.</p>
<b>Client &amp; end-point protection</b> 	<p>Customers should clearly define the devices and clients that are permitted to access the cloud service.</p>
<b>Identity and access management</b> 	<p>Microsoft Azure provides multiple options for identity and access management ranging from completely cloud-based (cloud-only identity)<sup>8</sup> to a hybrid approach<sup>9</sup> where user data is managed locally. With Azure Active Directory, the customer is able to configure password guidelines and multi-factor authentication<sup>10</sup> according to their specific guidelines.</p> <p>Note that Microsoft is responsible for providing a functional and secure identity and access management, but even for the cloud-only identity option, responsibility for the identity and access management still lies with the cloud user.</p> <p>Access to customer data by Microsoft employees can be controlled via Customer Lockbox<sup>11</sup>.</p>
<b>Audits</b> 	<p>Audits carried out by independent third parties help detect breaches of contract. Microsoft Azure is continually audited by independent third parties due to requirements of multiple compliance standards and certifications. The list of compliance standards for Microsoft Azure includes BSI C5, ISO 27001, ISO 27017 and ISO 27018.</p>
<b>Portability</b> 	<p>Many services on Azure have an equivalent on-premises setup; most of them use standard formats. For example:</p> <ul style="list-style-type: none"> <li>- Azure Virtual Machines are portable back to Hyper-V</li> <li>- Azure SQL services can be migrated back to a Microsoft SQL-Server</li> </ul> <p>In addition, storage data can be imported and exported and SQL databases can be copied and imported into other environments.</p>






<sup>7</sup> <https://aka.ms/sharedresponsibility>

<sup>8</sup> <https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

<sup>9</sup> <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/resilience-in-hybrid>

<sup>10</sup> <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started>

<sup>11</sup> <https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview>

Disaster recovery		<p>Microsoft has designed its Azure services with the necessary precaution. Azure keeps multiple live copies of customer data in multiple data centers in the chosen regions to achieve the contractually guaranteed availability.</p> <p>Customers should develop a disaster recovery plan, which should include backing up data.</p>
Application level controls		<p>With Microsoft Azure, the application level control lies mainly with the customer, as they are deploying their own applications. In the case, cloud services used within the application that are provided and operated by Microsoft, the responsibility for the secure provision and operation of those services lies with Microsoft. For instance, Microsoft is responsible for secure database management while the customer must secure the database used.</p>
Network controls		<p>For customers of Microsoft Azure, network management is shared between Microsoft and the customer. For example, the network underlying the cloud is operated and managed by Microsoft. On the other hand, the virtual network set up by the customer between different virtual machines lies in the responsibility of the customer.</p>
Host infrastructure		<p>The responsibility for the host infrastructure depends on the specific Azure service. The customer is responsible for any virtual machine they deploy. However, when using other Azure services such as Active Directory, Microsoft is responsible for the host infrastructure.</p>
Physical security		<p>Physical security ensures that only authorized employees are granted physical access to servers, network devices etc. It also includes business continuity management to ensure the cloud service remains available in the event of serious incidents or disasters, for instance by failing over to another physical location.</p>

## 2.2 Modelling Microsoft Azure

In order to remain IT-Grundschutz compliant while utilizing the cloud services of Microsoft Azure, the IT security concept must be updated to include the cloud services in accordance with BSI Standard 200-2<sup>12</sup>.

<sup>12</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002\\_en\\_pdf.html](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html)

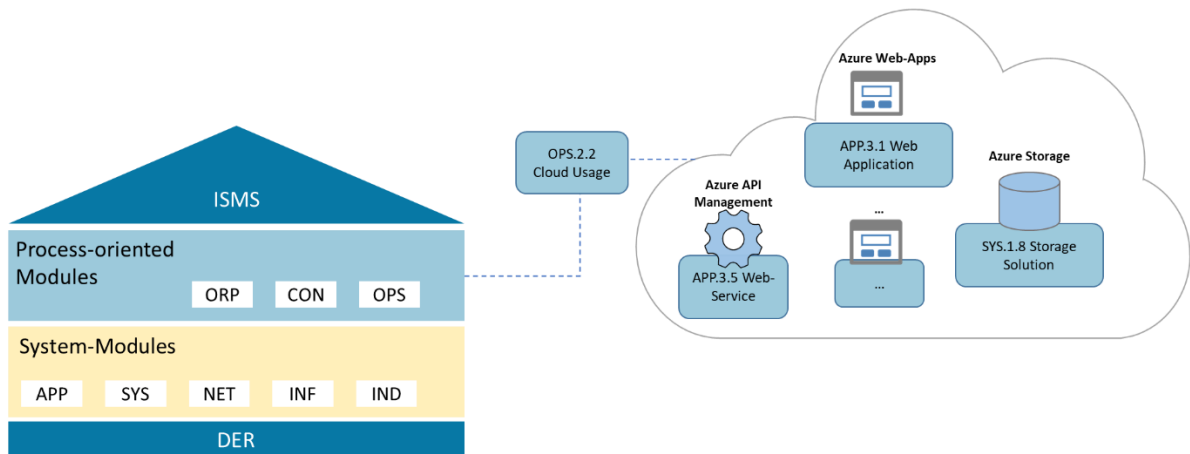


Figure 1 Multi-Layer model of BSI IT-Grundschutz Compendium with Cloud Usage as IaaS

The IT-Grundschutz Compendium takes a layered approach to modelling the information domain. The model consists of four layers: the information security management system (ISMS), process modules (OPS, CON, ORP), system modules (APP, SYS, NET, INF, IND) and detection and reaction (DER). As discussed in subchapter 2.1 the shared responsibility approach separates the responsibilities for the particular IT-Grundschutz modules and the requirements contained therein between the customer and Microsoft. Azure is covered by the Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) deployment model. This workbook discusses the shared responsibilities regarding IaaS only. According to the IT-Grundschutz approach, Microsoft, as the cloud service provider, is responsible for the management server for the cloud and the virtualization server.<sup>12</sup> On the customer site, the module *OPS.2.2 Cloud Usage*<sup>13</sup> defines the responsibilities of the customer across the entire cloud stack.

The module *OPS.2.2 Cloud Usage*<sup>14</sup> covers applications provided as a cloud service as well as their administration, which encompasses Microsoft Azure. The IT-Grundschutz Compendium<sup>15</sup> requires that the *OPS.2.2 Cloud Usage* module is always applied to a specific cloud service. If several cloud service providers are used, the module is to be applied once for each cloud service provider. The interfaces between the different cloud service providers must also be considered when implementing the module.

Further requirements for securing Microsoft Azure from the customer perspective will be on the modules of, for example, the network (NET), system (SYS) and, if applicable, the industrial (IND) layers. On the other hand, requirements will be included in new modules, such as *APP.5.3 Cloud-Applications from a Client Perspective* and *APP.3.5 Web-Services*, which are not yet published. As long as the module is not published, a risk analysis must be carried out according to the IT-Grundschutz method after 200-3<sup>16</sup>. Figure 1 shows that module *OPS.2.2 Cloud Usage* provides an interface to the customer's on premise environment.

<sup>13</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/04\\_OPS\\_Betrieb/OPS\\_2\\_2\\_Cloud-Nutzung\\_Edition\\_2021.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf) [German only]

<sup>14</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/04\\_OPS\\_Betrieb/OPS\\_2\\_2\\_Cloud-Nutzung\\_Edition\\_2021.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf) [German only]

<sup>15</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT\\_Grundschutz\\_Kompendium\\_Edition2021.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html) [German only]

<sup>16</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003\\_en\\_pdf.html](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html)

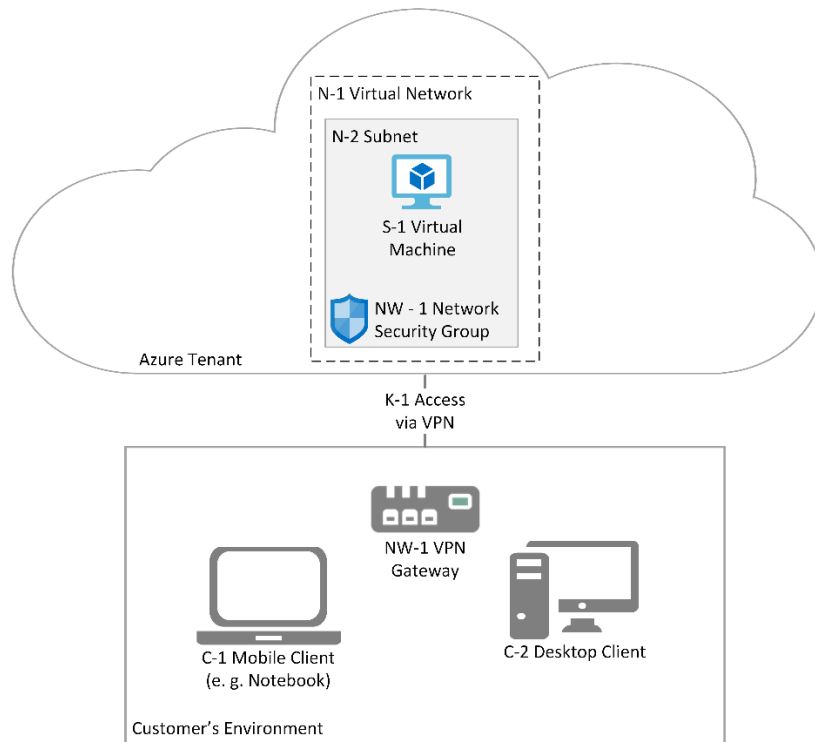


Figure 2 Reference Architecture of a virtual machine hosted on Azure<sup>17</sup>

Figure 2 presents the general structure of a virtual machine hosted in the Microsoft Azure environment within an IT-Grundschutz Information Domain. The cloud services are modelled as applications running directly in the cloud (i.e., without any underlying physical system or linked server rooms). It is also necessary to model the communication links (i.e., your Internet and/or VPN connection) as part of the system with the appropriate modules for your combination of network components and Internet service provider.

In the IaaS model, Microsoft is responsible for the completely physical infrastructure as already described in subchapter 2.1. For this reason, requirements are needed that define this responsibility.

For better understanding, the modelling is explained by example. This example is based on the reference architectures of a Microsoft Azure virtual machine running on Windows. This architecture (see Figure 2 *Reference Architecture of a virtual machine hosted on Azure*) can be used as an adjusted network diagram for the target objects of used Azure services. Afterwards the fitting modules of the IT-Grundschutz Compendium are mapped with the target objects. The modeling is just an excerpt and just the modules for the specific components of the given IaaS environment are defined, the comprehensive and organizational modules are not considered.

The customer's virtual environment within the cloud is modelled in a similar way as with standard physical or virtual infrastructure, including virtual servers, networks and applications. For IaaS, Microsoft provides no more than a virtual "shell" over a virtual network and is responsible for securing the network, whereas the cloud users are responsible for the IT systems of the cloud offering.<sup>12</sup>

<sup>17</sup> Based on <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/windows-vm>

For the components defined in the reference architecture, the modules defined in Table 2 of the IT-Grundschrift Compendium should at least be considered:

Table 2 Modules for the reference architecture

Service	Description	Modules
Virtual Machine	Virtual Machine (VM) on Windows 2012 as a custom managed image	SYS.1.2.2 Windows Server (Win2012)
Azure Active Directory	Authentication System	APP.2.1 General directory service
Virtual Network	Every VM is deployed into a virtual network that can be segmented into multiple subnets.	NET.1.1 Net architecture and design NET.1.2 Net management
VPN gateway	The VPN gateway connects the customer's environment to Azure over a virtual private network.	NET.3.1 Router and switches NET.3.2 Firewall NET.3.3 VPN

Note that the modelling process must take into account the individual scope, conditions and requirements of the cloud services and infrastructure. For this reason, this workbook considers only the generally necessary *OPS.2.2 Cloud Usage*<sup>13</sup> component based on the individual requirements. The requirements described in the following chapter 3 provide additional information referenced by the module *OPS.2.2 Cloud Usage*<sup>13</sup> and the applicable implementation notes or helpful online resources provided by Microsoft.

# 3

## Implementation of Module OPS.2.2 Cloud Usage

The following chapter describes how all requirements from module *OPS.2.2 Cloud Usage*<sup>18</sup> can be implemented for Microsoft Azure. In the revised IT-Grundschutz, the requirements were separated from the implementation instructions. The implementation instructions for *OPS.2.2 Cloud Usage*<sup>19</sup> contain concrete safeguards with which the requirements can be implemented.

While some requirements can only be fulfilled in an individual manner, Microsoft can provide information for many of the requirements. The following table gives an overview of the requirements for which Microsoft can provide supporting information.

Table 3 Information provided by Microsoft for the requirements of *OPS.2.2 Cloud Usage*

Requirement	Supporting information available from Microsoft?	Description
OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage	Yes	Microsoft has published the workbook “Enterprise Cloud Strategy” <sup>20</sup> to support users in developing a cloud usage strategy.
OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage	Yes	This requirement defines security requirements and procedures for cloud use. Microsoft supports this by providing documentation on the security safeguards in Microsoft Azure.
OPS.2.2.A3 Service Definition for Cloud Services by the Customer	Yes	This requirement is organization specific, since its purpose is to document internal requirements and the necessary level of protection in a format, which allows a simple comparison of cloud providers.

<sup>18</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium\\_Einzel\\_PDFs\\_2021/04\\_OPS\\_Betrieb/OPS\\_2\\_2\\_Cloud-Nutzung\\_Edition\\_2021.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf) (German only)

<sup>19</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/Umsetzungshinweise\\_Kompodium\\_CD\\_2019.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/Umsetzungshinweise_Kompodium_CD_2019.html) (German only)

<sup>20</sup> <https://info.microsoft.com/enterprise-cloud-strategy-ebook.html>



OPS.2.2.A4 Definition of Areas of Responsibilities and Interfaces	Yes	All responsibilities and points of interaction must be documented. The responsibilities of each party are recorded in the Shared Responsibilities document. <sup>21</sup> Microsoft offers several methods of connecting to and managing Microsoft Azure.
OPS.2.2.A5 Planning a Secure Migration to a Cloud Service	Yes	Microsoft has published the workbook “Cloud Migration Essentials” <sup>22</sup> to support users in their migration to cloud infrastructure.
OPS.2.2.A6 Planning the Secure Integration of Cloud Services	Yes	This requirement contributes to the secure integration of Azure into the customer’s environment. Microsoft offers several methods and services for integrating Azure into on-premises environments as well as for application integration. <sup>23</sup>
OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage	Yes	While there is no generic template for each specific organization’s requirements, Microsoft addresses most of the technical threats and mitigations mentioned in the safeguard.
OPS.2.2.A8 Careful Selection of a Cloud Service Provider	Yes	Microsoft provides instructions and information on how to evaluate Azure and Microsoft as a cloud service provider.
OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider	Yes	Detailed information concerning standard security requirements of Microsoft Azure is outlined in this requirement.
OPS.2.2.A10 Secure Migration to a Cloud Service	Yes	This requirement is organization specific, covering internal planning for the secure integration of existing services. Microsoft provides tools to assist with migrating current resources to Azure.
OPS.2.2.A11 Drawing Up Contingency Concept for a Cloud Service	Yes	The disaster recovery for Azure is developed individually. General guidelines, services and information are provided.
OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations	Yes	Information is made available concerning the maintenance of a high level of information security, as well as methods by which the user may test Microsoft’s claims.
OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage	Yes	Proof of information security is regularly published by Microsoft in the form of certifications, audit reports, penetration test results and other relevant reports.

<sup>21</sup> <https://aka.ms/sharedresponsibility>

<sup>22</sup> <https://azure.microsoft.com/en-us/resources/cloud-migration-simplified/>

<sup>23</sup> <https://azure.microsoft.com/en-us/product-categories/integration/>

OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship	Yes	Information and guidance regarding termination of a Microsoft Azure subscription are provided, including cancellation and data deletion policies.
OPS.2.2.A15 Ensuring the Portability of Cloud Services	Yes	The corresponding portability aspects are addressed as examples for Azure basic services.
OPS.2.2.A16 Implementing Backups	Yes	This has to be initiated by your organization; either by yourself or by using another, independent service. Microsoft provides a backup service.
OPS.2.2.A17 Use of Encryption When Using the Cloud	Yes	Microsoft Azure has made available a significant amount of information concerning encryption, where it is applied as standard and what encryption options are available to the end user.
OPS.2.2.A18 Use of Federation Services	Yes	Federated services are provided through Microsoft Azure service Azure Active Directory, and have their own set of security requirements.
OPS.2.2.A19 Security Vetting of Employees	Yes	Security checks of employees of the cloud provider and any subcontractors are necessary in the context of high security requirements.

Microsoft has published three compliance workbooks, handling compliance for IT-Grundschutz on cloud services. They are available for Microsoft 365, Dynamics 365 and Azure. As typical for cloud, Microsoft has implemented these services by leveraging synergies between online services, improving resource utilization on both sides. These synergies and common themes are also reflected in the great similarities within the three workbooks. In this way, customers using IT-Grundschutz for more than one of these services can benefit greatly from the similarities and synergies of these services by addressing certain topics in general and only adding certain specificities of the services. For example, Azure Active Directory can be used for identity and access management for Azure, Dynamics 365 and Microsoft 365.

### 3.1 OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage

In a cloud usage strategy, the objectives, opportunities and risks of cloud usage effecting the institution are considered. This also includes the consideration of legal aspects as well as technical and security related requirements. As a result, the deployment model for cloud services and initial cloud security requirements should be identified.

The approach to establish a strategy for cloud use depends on the respective scope. Microsoft has published an eBook to support the development of a cloud usage strategy. The eBook covers such topics

as the cloud deployment models and service models, cloud risk management, and security considerations.<sup>24</sup>

Microsoft also offers the *Azure Strategy and Implementation Guide* to create or strengthen a solid foundation for cloud application development and operations, service management and governance.<sup>25</sup>

Further information on compliance, privacy and security are provided in Microsoft's Trust Center.<sup>26</sup>

The customer must decide which applications or services are to be migrated to Azure. This may include partial integration of services or the integration of on-premises operational services (e.g., integration of Active Directory on-premises). There are multiple solutions with differing levels of integration and connection between cloud services, on-premises services and client applications.

### 3.2 OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage

The security policy for cloud usage is defined based on the strategy (see subchapter 3.1 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage*). The security policy covers all security requirements, which need to be established in the organization. This includes all security requirements for the provider based on the protection requirements identified for the cloud service. All technical interfaces between customer and cloud service provider are part of the security policy as well as the organizational, technical and legal framework. If cloud services from international providers are used, country-specific requirements and laws must be also taken into account.

Customers have to develop their own, suitable cloud policy concerning their security needs and legal or compliance requirements and has to choose a cloud service provider that can fulfill the requirements. Microsoft provides Azure specific information to assist organizations in establishing their security policy regarding data privacy, compliance, transparency and other individualized customer controls. The table below lists typical topics that should be considered within a cloud policy including references how the requirements are fulfilled by or can be fulfilled using Azure.

Table 4 Reference Information for Cloud Security Policy

Security Topic	Implementation on Microsoft Azure	References
Identity & Access Management	<p>Azure Active Directory is used to manage identities and authentication. Azure supports the creation of dedicated cloud-only and hybrid identity. Hybrid identities are managed on-premises and synchronized (with or without password hash) to Azure Active Directory.</p> <p>Azure Active Directory provides different ways to use hybrid identities in Azure:</p>	<p><a href="https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is">https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/</a></p>

<sup>24</sup> <https://info.microsoft.com/enterprise-cloud-strategy-ebook.html>

<sup>25</sup> [https://azure.microsoft.com/mediahandler/files/resourcefiles/efc32c2a-5c32-407c-a67d-6116cb810546/Azure\\_Strategic\\_Implementation\\_Guide\\_for\\_IT\\_Organizations\\_New\\_to\\_Azure.pdf](https://azure.microsoft.com/mediahandler/files/resourcefiles/efc32c2a-5c32-407c-a67d-6116cb810546/Azure_Strategic_Implementation_Guide_for_IT_Organizations_New_to_Azure.pdf)

<sup>26</sup> <https://www.microsoft.com/en-us/trust-center/>

Security Topic	Implementation on Microsoft Azure	References
	<ul style="list-style-type: none"> <li>• Password hash synchronization (PHS) synchronizes on-premises accounts including a hash of the password hash into Azure</li> <li>• Pass-through authentication (PTA) allows users to login to Azure using their on-premises credentials and Azure then validates the password against the on-premises Active Directory</li> <li>• Active Directory Federation Service is a trust between Azure Active Directory and on-premises Active Directory. In this case, the users are authenticated against the on-premises Active Directory.</li> </ul> <p>Role-based access control (RBAC) can be realized in Azure using various built-in roles or by defining own, custom roles. Besides internal accounts of an institution or company Azure allows to add and manage guest accounts and external partners (Business-to-Business, B2B).</p> <p>Intune can be used to realize mobile device management and thus to restrict or secure the access from mobile devices.</p> <p>Different Multi Factor Authentication (MFA) methods are provided and can be used to secure access to Azure, e. g. via mobile app, smart card or certain third party Multi Factor Authentication solutions.</p> <p>Privileged Identity Management (PIM) allows managing and monitoring administrative access to Azure. For example, with PIM privileged access can be limited in time.</p> <p>With the Conditional Access feature, Azure customers can add automated access control decisions for accessing data and apps in Azure that are based on customer specified conditions.</p> <p>The feature Just-in-time (JIT) can be used to restrict the access to virtual machines.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal">https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles">https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/b2b/index">https://docs.microsoft.com/en-us/azure/active-directory/b2b/index</a></p> <p><a href="https://docs.microsoft.com/en-us/intune/what-is-intune">https://docs.microsoft.com/en-us/intune/what-is-intune</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted">https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/pim-azure-resource">https://docs.microsoft.com/en-us/azure/role-based-access-control/pim-azure-resource</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/role-based-access-control/conditional-access-azure-management">https://docs.microsoft.com/en-us/azure/role-based-access-control/conditional-access-azure-management</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time">https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time</a></p>

Security Topic	Implementation on Microsoft Azure	References
Asset Management	<p>Azure portal allows to build, manage, and monitor everything from simple web apps to complex cloud deployments or to create custom dashboards for an organized view of resources.</p> <p>In addition, Azure resource manager provides a management layer that allows creating, updating and deleting resources in a subscription.</p> <p>Azure provides different services that allow labelling/tagging of assets.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-overview">https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview">https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/decision-guides/resource-tagging/">https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/decision-guides/resource-tagging/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags">https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags</a></p>
Protection of Data	<p>Microsoft has redesigned its processes to meet the requirements of the EU standard clauses.</p> <p>Azure ensures that customers are able to meet the requirements for notification of privacy breaches by notifying them of potential privacy breaches within 72 hours. The notice contains a description of the type of breach, the approximate impact on users, and a description of the requirements, including timings.</p> <p>In addition, Microsoft provides instructions on how the customer can implement the data protection requirements in Azure. This includes a checklist, an impact assessment on data protection and answers to questions from the affected persons.</p> <p>Customer isolation in Azure is implemented by several technical means. This includes logical isolation using role based access control, encryption and storage level isolation.</p> <p>Azure protects customer data at rest and in transit using state of the art cryptographic methods and protocols, like AES, IPsec or TLS/SSL.</p> <p>Azure allows the definition, assignment and management of security policies. They can be used to enforce rules over</p>	<p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-EU-Model-Clauses">https://docs.microsoft.com/en-us/compliance/regulatory/offering-EU-Model-Clauses</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-arc">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-arc</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics-windows">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics-windows</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Azure">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Azure</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-monitor/logs/personal-data-mgmt">https://docs.microsoft.com/en-us/azure/azure-monitor/logs/personal-data-mgmt</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy">https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-ISO-27018">https://docs.microsoft.com/en-us/compliance/regulatory/offering-ISO-27018</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/azure-isolation">https://docs.microsoft.com/en-us/azure/security/azure-isolation</a></p>

Security Topic	Implementation on Microsoft Azure	References
	<p>resources so they stay compliant with corporate standards or requirements.</p> <p>Microsoft continuously tests and monitors the security of Azure and takes actions accordingly. Corresponding reports, e.g. for penetration tests or audits, can be accessed using the trust center. The service health can be viewed on the Azure service health page.</p> <p>Azure allows the definition of (security) blueprints that allow to applying consistently and repeatedly the same configurations or policies.</p> <p>Azure provides a wide array of configurable security auditing and logging options to help identify gaps in security policies and mechanisms. This includes activity logs, event logs of virtual machines or traffic through Network Security Groups.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/security/azure-protection-of-customer-data">https://docs.microsoft.com/en-us/azure/security/azure-protection-of-customer-data</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/governance/policy/overview">https://docs.microsoft.com/en-us/azure/governance/policy/overview</a></p> <p><a href="https://servicetrust.microsoft.com/View-Page/TrustDocuments">https://servicetrust.microsoft.com/View-Page/TrustDocuments</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/service-health/service-health-overview">https://docs.microsoft.com/en-us/azure/service-health/service-health-overview</a></p> <p><a href="https://status.azure.com/en-us/status">https://status.azure.com/en-us/status</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/governance/blueprints/overview">https://docs.microsoft.com/en-us/azure/governance/blueprints/overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit">https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit</a></p>
Compliance and Audit	<p>Microsoft fulfils various national and international compliance requirements with its cloud services and has this certified or attested by third parties. The corresponding certificates or attestations are published in the trust center.</p> <p>Microsoft invested in the processes to meet the requirements of the Model Clauses for the transfer of personal data processors.</p> <p>Azure ensures that customers are able to meet GDPR's breach notification requirements, by allowing the specification of a privacy contact, which is notified about breaches within 72 hours. The notification includes a description of the nature of the breach, approximate user impact and mitigation steps including timelines.</p> <p>Additionally, Microsoft provides guidance how General Data Protection Regulation (GDPR) requirements can be realized in Azure by the customer. This includes an accountability readiness checklist, a data protection impact assessment template</p>	<p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-home">https://docs.microsoft.com/en-us/compliance/regulatory/offering-home</a></p> <p><a href="https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses">https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-arc">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-arc</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-azure">https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-azure</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-monitor/platform/personal-data-mgmt">https://docs.microsoft.com/en-us/azure/azure-monitor/platform/personal-data-mgmt</a></p> <p><a href="http://azuredatacentermap.azurewebsites.net/">http://azuredatacentermap.azurewebsites.net/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy">https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy</a></p>

Security Topic	Implementation on Microsoft Azure	References
	<p>and how to suitably answer data subject requests.</p> <p>Azure provides several auditing and reporting features that can for example be used to track user or administrator activity.</p> <p>Microsoft provides an overview of all data storage locations for Azure.</p> <p>Microsoft Defender for Cloud is a natively integrated tool for security posture management and threat protection. For example, it provides hardening recommendations based on the Azure Security Benchmark and for Azure data and PaaS services anomaly detection helps to identify attacks.</p>	<p><a href="https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27018">https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27018</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring">https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-reports">https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-reports</a></p> <p><a href="http://azuredatamap.azurewebsites.net/">http://azuredatamap.azurewebsites.net/</a></p> <p><a href="https://docs.microsoft.com/en-us/security/benchmark/azure/overview">https://docs.microsoft.com/en-us/security/benchmark/azure/overview</a></p>
Cryptography	<p>Azure provides several methods to realize secure encryption of data, which will be addressed in a dedicated requirement.</p>	<p>Subchapter 3.17 OPS.2.2.A17 <i>Use of Encryption When Using the Cloud</i></p>
Backup and archiving	<p>Azure backup service allows backing up on-premises data and certain data in Azure like virtual machines.</p> <p>Data resiliency and recoverability are built-in for Azure, to maximize reliability and minimize negative effects on customers. Additionally, Microsoft provides information for customers how they can setup a resilient environment and applications in Azure.</p> <p>Site Recovery can replicate Azure, on-premises and Azure Stack virtual machines as well as physical servers within Azure to allow machine failover (site-recovery).</p> <p>Archiving of cloud applications and data within dedicated storages in Azure can for example be realized with Azure blob storage.</p> <p>Different third party solutions are available to backup or archive data from Azure services.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/backup/backup-overview">https://docs.microsoft.com/en-us/azure/backup/backup-overview</a></p> <p><a href="https://azure.microsoft.com/en-us/features/resiliency/">https://azure.microsoft.com/en-us/features/resiliency/</a></p> <p><a href="https://azure.microsoft.com/en-us/resources/resilience-in-azure-whitepaper/">https://azure.microsoft.com/en-us/resources/resilience-in-azure-whitepaper/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview">https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers">https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers</a></p> <p><a href="https://azure.microsoft.com/en-us/solutions/architecture/backup-archive-cloud-application/">https://azure.microsoft.com/en-us/solutions/architecture/backup-archive-cloud-application/</a></p>



Security Topic	Implementation on Microsoft Azure	References
Secure Configuration	<p>Microsoft provides configuration best practices and patterns to configure securely Azure.</p> <p>The configurable blueprints and policies mentioned within the protection of data section can also be used to ensure a secure configuration.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns">https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/governance/blueprints/overview">https://docs.microsoft.com/en-us/azure/governance/blueprints/overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/governance/policy/overview">https://docs.microsoft.com/en-us/azure/governance/policy/overview</a></p>
Logging and Monitoring	<p>Azure provides different kinds of log data within its services, which can for example be used to track activity or to identify threats.</p> <p>Monitoring with different focus (resource usage, compliance, risky accounts, security issues) is possible using the different services provided within Azure.</p> <p>Using the Log Analytics Agent, Security Center collects data from Azure virtual machines (VMs), IaaS containers etc. to monitor security vulnerabilities as early as possible.</p> <p>Azure Threat Protection (ATP) monitors user behavior to identify possible attacks on Active Directory. Also, Azure Active Directory Identity Protection helps protecting and monitoring the customer's identities.</p> <p>Azure Sentinel is a cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit">https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-monitor/overview">https://docs.microsoft.com/en-us/azure/azure-monitor/overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview">https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection">https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection</a></p> <p><a href="https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp">https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview">https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/sentinel/overview">https://docs.microsoft.com/en-us/azure/sentinel/overview</a></p>
Threat protection	<p>Azure has a basic level of DDoS protection in place automatically and free, which can be sufficient for common network level attacks. A subscription for the standard DDoS protection provides protection against more sophisticated attacks and provides support of DDoS experts for customization and during DDoS attacks.</p> <p>Azure provides a free real-time malware protection to identify and remove several kind of malware like viruses or spyware.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview">https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware">https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware</a></p> <p><a href="https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp">https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp</a></p>

Security Topic	Implementation on Microsoft Azure	References
	<p>Azure provides services and views that allow the detection of anomalies, like unusual behaviour of accounts or suspicious behaviour, indicating ongoing threats.</p>	
<p>Change Management</p>	<p>Azure is constantly extended and changed to provide additional functionality or security. Microsoft provides a roadmap of ongoing and planned updates to Azure that can be used by customers to prepare for upcoming changes.</p> <p>Azure automation is a service to automate changes and consists of process automation, update management, and configuration features.</p>	<p><a href="https://azure.microsoft.com/en-us/updates/">https://azure.microsoft.com/en-us/updates/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/automation/automation-intro">https://docs.microsoft.com/en-us/azure/automation/automation-intro</a></p>

### 3.3 OPS.2.2.A3 Service Definition for Cloud Services by the Customer

For every planned and ordered cloud service a description in accordance with the defined strategy (see subchapter 3.1 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage*) and security policy (see subchapter 3.2 *OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage*) should be set out. The definition should point out benefit or targeted results of the planned or used service for the customer. Utilizing standardized ITIL style service templates may be beneficial if there is no other predefined format in the organization. As part of the service definition, the most important technical parameters should be defined.

Microsoft provides information about the cloud services themselves on various websites.<sup>27</sup> A search query at Microsoft's Azure global infrastructure website<sup>28</sup> can be used to find out whether a service is available in the chosen region. The availability commitments in form of Service Level Agreements (SLAs) are defined per cloud service.<sup>29</sup>

Besides service descriptions and guaranteed availabilities also authentication methods per service should be documented. The central identity management is handled using Azure Active Directory.<sup>30</sup>

<sup>27</sup> <https://azure.microsoft.com/en-us/services/>

<https://docs.microsoft.com/en-us/azure/#pivot=products>

<sup>28</sup> <https://azure.microsoft.com/en-us/global-infrastructure/services/>

<sup>29</sup> <https://azure.microsoft.com/en-us/support/legal/sla/>

<sup>30</sup> <https://docs.microsoft.com/en-us/azure/active-directory/>

Multifactor authentication<sup>31</sup> and role-based access control<sup>32</sup> are available for controlling access to cloud services and resources. The multifactor authentication service can be either used from Microsoft<sup>31</sup> or from an external Authentication Provider<sup>33</sup>. For the management of further security aspects, Microsoft offers several different options in the Azure to secure further access to and from cloud services. Microsoft Azure offers encryption in conjunction with a variety of cloud services. Data in storages and in transmission is automatically encrypted; this encryption cannot be disabled.<sup>34</sup> The customer can either choose to store the secrets like passwords, API keys or certifications software-based in Azure Key Vault solely or by using own Hardware Security Modules, shared Hardware Security Modules from Microsoft or dedicated Hardware Security Modules from Microsoft.<sup>35</sup>

In addition, Microsoft's customer lockbox provides an interface that allows customers to review and then approve or reject data access requests, such as when a Microsoft technician needs to access customer data during a support request.<sup>36</sup>

### 3.4 OPS.2.2.A4 Definition of Areas of Responsibilities and Interfaces

The responsibilities for secure cloud operation and usage are shared between the cloud service provider and the customer. Thereby, the exact responsibilities can vary from cloud service to cloud service, especially when different delivery models are included such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS). It is important that the responsibilities can clearly be distinguished from each other; otherwise this might lead to different understandings of responsibilities resulting in security weaknesses.

Microsoft provides various information on their approach and view on this shared responsibility model.<sup>37</sup> For further information on the shared responsibility model, refer to subchapter 2.1 *Shared Responsibility Model* at the beginning of this document.

After the responsibilities are identified, it is important to define clearly the interfaces between the customer and the cloud service provider so both sides can fulfill their responsibilities adequately.

---

<sup>31</sup> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

<sup>32</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/>

<sup>33</sup> <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-additional-authentication-methods-for-ad-fs>

<sup>34</sup> <https://docs.microsoft.com/en-us/azure/security/security-azure-encryption-overview>

<sup>35</sup> <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-hsm-protected-keys>

<https://docs.microsoft.com/en-us/azure/dedicated-hsm/>

<sup>36</sup> <https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview>

<sup>37</sup> <https://aka.ms/sharedresponsibility>

<https://azure.microsoft.com/mediahandler/files/resourcefiles/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20nboarding%20Guide%20for%20IT%20organizations.pdf>

<https://www.microsoft.com/security/blog/2018/06/19/driving-data-security-is-a-shared-responsibility-heres-how-you-can-protect-yourself/>

The defined responsibilities and interfaces should be documented within the context of the service definition of the user, which is addressed in subchapter 3.3 *OPS.2.2.A3 Service Definition for Cloud Services by the Customer*. Afterwards, the secure migration to and integration of the cloud service can be planned.

### 3.5 OPS.2.2.A5 Planning a Secure Migration to a Cloud Service

The development of a migration concept forms an important foundation for a secure and sustainable migration to the cloud. Above all, organizational regulations and task assignments must be taken into account. Including responsibilities, test and transfer procedures, which are of particular importance to ensure resilient and secure business operation. In the following the company-owned IT should be considered adequate within the migration process.

For a secure migration to the cloud various, customer specific conditions have to be considered. This especially applies, if other, already used cloud services should be considered for the migration. Thereby, the portability features provided by the cloud service is of importance, which will be addressed in subchapter 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*.

To ensure a continuous and high level of security, the migration from a local environment, potentially including other cloud services, to Azure must be appropriately planned.

Microsoft offers a workbook<sup>38</sup> to support customer in migration planning. The workbook combines answers to important questions and experience-based recommendations concerning a migration to the cloud. An additional workbook covering the migration of SQL Server databases is also available.<sup>39</sup> Microsoft also provides further information and guidelines on migration at the Azure migration center<sup>40</sup>, which includes subpages and links for training in cloud migration and getting help by finding migration experts, partners and tools.<sup>41</sup>

To realize an orderly and secure migration while maintaining a normal operation for the existing environment, the enhanced resource requirements (financial, know-how and human) have to be considered for planning, migrating, testing and the early operation phases.

The migration planning has to consider how data and services can be securely transferred to the cloud. For Azure, this is addressed in subchapter 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*.

In addition to the migration to a cloud service, its integration in the existing IT infrastructure during and after the migration has to be considered. This is addressed in subchapter 3.6 *OPS.2.2.A6 Planning the Secure Integration of Cloud Services*.

---

<sup>38</sup> <https://azure.microsoft.com/en-us/resources/cloud-migration-simplified/>

<sup>39</sup> <https://azure.microsoft.com/en-us/resources/migrating-sql-server-to-azure-sql-managed-instance-step-by-step/>

<sup>40</sup> <https://azure.microsoft.com/en-us/migration/>

<sup>41</sup> <https://azure.microsoft.com/en-us/migration/migration-partners/>

## 3.6 OPS.2.2.A6 Planning the Secure Integration of Cloud Services

In addition to planning a secure migration (see subchapter 3.5 *OPS.2.2.A5 Planning a Secure Migration to a Cloud Service*), the secure integration of Azure is essential for secure, continuous IT operations. This requirement considers aspects beyond planning the migration.

There are various methods to prepare the integration of cloud-based features. The organization shall establish and document a security concept that considers the security requirements affecting the following aspects:

- Required adaptations of the existing IT landscape
- Suitability of existing interfaces (e.g., proxy) for the usage with Azure
- Definition of the administration model for cloud, e.g., usage of Azure Active Directory (Azure AD) vs. Active Directory Federation Services (ADFS)
- Information management (data backup and data retention strategy) regarding information stored in the cloud and on-premises

For application integration, it is often necessary to connect several independent systems. This process can be very complex. The whitepaper *Azure Integration Services*<sup>42</sup> describes the components of Azure Integration Services (API Management, Logic Apps, Service Bus and Event Grid) and how they interact to provide a complete solution for integrating on-premises applications and cloud applications.

To secure the connection between cloud services and on-premises a Cloud Access Security Broker (CASB) like Microsoft's Cloud App Security can be used. A CASB can for example function as a reverse proxy, provide enhanced visibility of data, control access to cloud services or can be used to detect threats related to cloud services in use.<sup>43</sup>

Additionally, a learning platform is offered, where many specific supporting contents can be found for training.<sup>44</sup>

With the Evergreen approach, Microsoft aims to keep all Azure services and the entire platform secure, compliant and always up to date with ongoing updates. This approach brings new responsibilities for customers in the area of change management, as they have to consider changes in the use or, if necessary, in their business processes.<sup>45</sup>

## 3.7 OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage

Based on the identifiable requirements (see subchapter 3.2 *OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage*), a security concept for the use of cloud services should be developed. Threats arise from contractual deficiency, dependencies or unclear responsibilities. They cause loss of control and inefficient performance. Several parties are involved, particularly in connection with cloud services. At

---

<sup>42</sup> <https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-integration-services/Azure-Integration-Services-Whitepaper-v1-0.pdf> (Whitepaper „Azure Integration Services“)

<sup>43</sup> <https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security>

<sup>44</sup> <https://docs.microsoft.com/en-us/learn/azure/>

<sup>45</sup> <https://azure.microsoft.com/en-us/updates/>

least the following parties should be taken into account: cloud service customer, cloud service provider and network provider.

While there is no generic template for your organization's requirements, Microsoft Azure addresses many of the threats and mitigations mentioned in the official implementation recommendations of IT-Grundschutz as follows.

Table 5 Reference information for a cloud security concept

Cloud-specific threats	Information for Microsoft Azure	References
Pre-emptive or compulsorily contract ending	Contract ending is addressed in detail within a dedicated requirement.	Subchapter 3.14 OPS.2.2.A14 <i>Orderly Termination of a Cloud Service Relationship</i>
Lack of portability, e.g. because of proprietary data formats	Portability is addressed in detail within a dedicated requirement.	Subchapter 3.15 OPS.2.2.A15 <i>Ensuring the Portability of Cloud Services</i>
Missing knowledge about physical data storage location	<p>Azure provides an overview of data centers within a geolocations and allows choosing the geolocation within a subscription. Data will then be maintained within the data centers located in this geolocation.</p> <p>All Azure data centers are physical protected against unauthorized access and several other threats.</p>	<p><a href="https://azure.microsoft.com/en-us/global-infrastructure/">https://azure.microsoft.com/en-us/global-infrastructure/</a></p> <p><a href="http://azuredatacentermap.azurewebsites.net/">http://azuredatacentermap.azurewebsites.net/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure">https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure</a></p>
High mobility of information: Information stored in the cloud can be accessed from various locations using different types of devices or software (PC, laptop, smartphone, browser, apps, etc.)	Mobile device management (MDM) or Intune can be used to secure and configure mobile devices, if and under which circumstances they are allowed to access Azure. Together with conditional access, this can be used to restrict access to certain data or services within Azure, based on several conditions, like the device location, authentication method used, state of the device or whether the device used is configured compliant to the customer's requirements.	<p><a href="https://docs.microsoft.com/en-us/intune/get-started-evaluation">https://docs.microsoft.com/en-us/intune/get-started-evaluation</a></p> <p><a href="https://docs.microsoft.com/en-us/windows/client-management/mdm/azure-active-directory-integration-with-mdm">https://docs.microsoft.com/en-us/windows/client-management/mdm/azure-active-directory-integration-with-mdm</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview">https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview</a></p>
Unauthorized access (e.g. by cloud provider admins or other cloud customers)	By default Microsoft personnel has no access to customer data. When access is required, Multi Factor Authentication is mandatory and least privilege and permanent logging and monitoring is applied. Additionally the customer lockbox can be used to view and approve or deny access by Microsoft in support cases.	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data">https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data</a></p> <p><a href="https://www.microsoft.com/en-us/trust-center/privacy/data-access">https://www.microsoft.com/en-us/trust-center/privacy/data-access</a></p>

Isolation between customers (multitenancy) is realized on access, compute, storage, data base and network level to ensure that no access to other customer's data is possible, even when running on the same hardware.

To prevent unauthorized access to customer data, data is encrypted at rest and during transfer, including transfer between data centers, using state of the art protocols and cryptography like AES and TLS.

<https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview>

<https://docs.microsoft.com/en-us/azure/security/fundamentals/isolation-choices>

<https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview>

### 3.8 OPS.2.2.A8 Careful Selection of a Cloud Service Provider

Subsequent to the planning and conception process, a detailed requirement profile for cloud service providers should be developed. These requirements should be defined in accordance with the service definitions (see subchapter 3.3 *OPS.2.2.A3 Service Definition for Cloud Services by the Customer*) and should also include contract specifications.

Using the defined requirements as a starting point, a service catalog or a requirement specification can be created. This catalog can then be used to compare the competing cloud service providers and rate them using a point's matrix.

Before migrating into the cloud, a cost-value-analysis should aid the decision process of selecting a cloud provider. The focus of the analysis needs the realistic costs, especially taking into account growing service requirements. Is the benefit of the cloud solution small or even negative the whole migration should be questioned or the service definition reviewed and potentially adjusted. Upon assessing the costs, additional capital and operational expenditures need to be separated, hence the costs for own infrastructure and services keeps existing for a specific period during and after migration.

The basic aspects must be investigated and appropriate answers need to be obtained before the offers are evaluated. If the results are not satisfactory, a cloud service provider may be removed from further consideration.<sup>46</sup> Microsoft supports due diligence evaluations with a checklist<sup>47</sup> that is based on international standard ISO/IEC 19086-1, the Cloud Computing Service Level.

The following table lists information, which should be gathered and assessed ahead of migrating to the cloud, including corresponding information for Microsoft Azure.

---

<sup>46</sup> Further aspects and assistance in choosing a cloud service provider is available from Microsoft at <https://azure.microsoft.com/en-us/overview/choosing-a-cloud-service-provider/>

<sup>47</sup> <https://www.microsoft.com/en/trust-center/compliance/due-diligence-checklist>



Table 6 Reference information for diligent selection

Consideration to be made	Conditions on Microsoft Azure	References
<p>Publicly available information about the provider (reputation, ratings and rankings, core business, performance, cloud experience)</p>	<p>Cloud belongs to the core businesses of Microsoft and Microsoft belongs to the best rated cloud services providers according to various ratings</p> <p>Microsoft provides a general overview about important topics on Azure that can be used as a baseline for diligence verification.</p> <p>Microsoft provides the Service Health feature. The dashboard can be customized and provides users with the ability to track relevant events or configure event alarms.</p> <p>Azure is constantly extended and updated. Microsoft publishes roadmaps and further information about planned updates on their webpage.</p> <p>Exchange with other customers is possible in the Microsoft Azure community to receive further information about Azure.</p> <p>Microsoft provides customer stories on their usage of Azure.</p>	<p><a href="https://www.microsoft.com/en-us/investor/default.aspx">https://www.microsoft.com/en-us/investor/default.aspx</a></p> <p><a href="https://azure.microsoft.com/en-us/overview/what-is-azure/">https://azure.microsoft.com/en-us/overview/what-is-azure/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/service-health/service-health-overview">https://docs.microsoft.com/en-us/azure/service-health/service-health-overview</a></p> <p><a href="https://status.azure.com/en-us/status">https://status.azure.com/en-us/status</a></p> <p><a href="https://azure.microsoft.com/en-us/updates/">https://azure.microsoft.com/en-us/updates/</a></p> <p><a href="https://techcommunity.microsoft.com/t5/Azure/ct-p/Azure">https://techcommunity.microsoft.com/t5/Azure/ct-p/Azure</a></p> <p><a href="https://azure.microsoft.com/en-us/case-studies/">https://azure.microsoft.com/en-us/case-studies/</a></p> <p><a href="https://customers.microsoft.com/en-us/home">https://customers.microsoft.com/en-us/home</a></p>
<p>Due-Diligence</p>	<p>Microsoft provides a checklist for Due-Diligence activities</p> <p>Microsoft provides a wide set of compliance offerings that can be used as a baseline for Due-Diligence activity.</p>	<p><a href="https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist">https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-home">https://docs.microsoft.com/en-us/compliance/regulatory/offering-home</a></p>
<p>Access through cloud provider or third parties</p>	<p>Microsoft personnel has no access by default. When access is required, multi factor authentication is mandatory and least privilege and permanent logging and monitoring is applied.</p> <p>The access can be denied or approved by the customer using the customer lock-box features.</p> <p>The customer isolation implemented in Azure ensures that different customers cannot access the data of others, even if they are computed or stored on the same hardware.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data">https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data</a></p> <p><a href="https://www.microsoft.com/en-us/trust-center/privacy/data-access">https://www.microsoft.com/en-us/trust-center/privacy/data-access</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview">https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/isolation-choices">https://docs.microsoft.com/en-us/azure/security/fundamentals/isolation-choices</a></p>

Consideration to be made	Conditions on Microsoft Azure	References
	Data is encrypted during transfer and is encrypted at rest using state of the art cryptographic methods and protocols so unauthorized parties cannot access the information contained.	<a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview">https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview</a>
Installation of additional software	Azure can be accessed using a browser or by using an API. When a service requires additional software to be installed this is typically stated together with relevant installation information.	<a href="https://docs.microsoft.com/en-us/rest/api/azure/">https://docs.microsoft.com/en-us/rest/api/azure/</a>
Locations of cloud provider	<p>Data at rest is stored in the chosen geographical location. However, customer data might be moved outside of the chosen geolocation for data processing reasons. For backup purposes customer data is replicated to other data centers within the same geolocation.</p> <p>By the end of 2022, data storage and processing for Azure, among others, will take place exclusively within Europe.</p>	<p><a href="https://azure.microsoft.com/en-us/global-infrastructure/">https://azure.microsoft.com/en-us/global-infrastructure/</a></p> <p><a href="http://azuredatadcentermap.azurewebsites.net/">http://azuredatadcentermap.azurewebsites.net/</a></p> <p><a href="https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked-questions/p/2329098">https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked-questions/p/2329098</a></p>
Subcontractors of cloud provider	Microsoft publishes and regularly updates a list of subcontractors and additionally a list of subcontractors, which handle the data of customers. Subcontractors working for Microsoft are required to join the Microsoft Supplier Security and Privacy Assurance Program. This program assures that the rules and processes implemented in Microsoft are followed by subcontractors. It helps to standardize and strengthen data handling practices. For example, those subcontractors who have or could have access to customer data must agree to the European Union Model Clauses.	<p><a href="https://www.microsoft.com/en-us/trust-center/privacy/data-access">https://www.microsoft.com/en-us/trust-center/privacy/data-access</a></p> <p><a href="https://go.microsoft.com/fwlink/?LinkId=2096306&amp;clid=0x407">https://go.microsoft.com/fwlink/?LinkId=2096306&amp;clid=0x407</a> (Microsoft Online Services Subprocessors List)</p> <p><a href="https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426">https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426</a> (Microsoft Commercial Support Subcontractors)</p> <p><a href="https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx">https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx</a></p>
Consideration of contractual basis and regulations	The Service Level Agreements and Microsoft's Online Services Terms are the standard stipulations governing the use of Microsoft Azure services. The standard SLAs, prices and online service terms are published on the webpage and	<p><a href="https://azure.microsoft.com/en-us/support/legal/">https://azure.microsoft.com/en-us/support/legal/</a></p> <p><a href="https://www.microsoft.com/licensing/terms/productoffering">https://www.microsoft.com/licensing/terms/productoffering</a></p> <p><a href="https://www.microsoft.com/licensing/docs/view/Service-">https://www.microsoft.com/licensing/docs/view/Service-</a></p>

Consideration to be made	Conditions on Microsoft Azure	References
	<p>accessible without Microsoft subscription or Azure account.</p> <p>In addition, Microsoft publishes a FAQ with recent questions concerning the pricing and SLAs.</p>	<p><a href="#">Level-Agreements-SLA-for-Online-Services</a></p> <p><a href="https://azure.microsoft.com/en-us/support/legal/sla/">https://azure.microsoft.com/en-us/support/legal/sla/</a></p> <p><a href="https://azure.microsoft.com/en-us/pricing/faq/">https://azure.microsoft.com/en-us/pricing/faq/</a></p>
Evaluation of services including warranties	<p>Service descriptions, documentation and pricing information are published on the webpage of each service.</p> <p>Additionally, interested customers have the possibility to use the cost calculator from Microsoft for cost comparisons.</p>	<p><a href="https://azure.microsoft.com/en-us/services/">https://azure.microsoft.com/en-us/services/</a></p> <p><a href="https://azure.microsoft.com/en-us/pricing/calculator/">https://azure.microsoft.com/en-us/pricing/calculator/</a></p>

### 3.9 OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider

Following the selection of a suitable cloud service provider, the relevant aspects should be defined in contractual ways. The contractual agreements between the customer and the cloud service provider should be appropriate in type, scope and detail level of the informational protection requirements in context of data to be stored or used in Azure. The previously defined requirements must also be considered here. At a minimum, the following points require an answer with respect to Microsoft Azure.

Table 7 Cloud contract documents

Consideration to be made	Conditions on Microsoft Azure	References
Physical location of the services and cloud service provider	<p>The cloud services are run from data centers located in the region that was chosen by the customer.</p> <p>Data at rest is stored in the chosen geographical location. However, customer data might be moved outside of the chosen geolocation for data processing reasons. By the end of 2022, data storage and processing for Azure, among others, will take place exclusively within Europe.</p> <p>All data centers are physical protected against unauthorized access and other typical threats data centers.</p> <p>Microsoft implemented and provides several different safeguards to ensure availability of services.</p>	<p><a href="https://azure.microsoft.com/en-us/global-infrastructure/">https://azure.microsoft.com/en-us/global-infrastructure/</a></p> <p><a href="https://azure.microsoft.com/en-us/global-infrastructure/geographies/">https://azure.microsoft.com/en-us/global-infrastructure/geographies/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure">https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability">https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability</a></p> <p><a href="https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked-questions/ba-p/2329098">https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked-questions/ba-p/2329098</a></p>

Consideration to be made	Conditions on Microsoft Azure	References
Subcontractors and third parties involved with service delivery	<p>Microsoft employs subcontractors for specific, limited support tasks. A list with all subcontractors and a separated list with subcontractors with access to customer data is published.</p> <p>Subcontractors working for Microsoft are required to participate in the Microsoft Supplier Security and Privacy Assurance Program. This program ensures that the rules and processes implemented in Microsoft are also followed by subcontractors. It helps to standardize and strengthen data handling practices. For example, subcontractors who have or may have access to customer data must also act in accordance with EU standard clauses.</p>	<p><a href="https://go.microsoft.com/fwlink/?LinkId=2096306&amp;clid=0x407">https://go.microsoft.com/fwlink/?LinkId=2096306&amp;clid=0x407</a> (Microsoft Online Services Subprocessors List)</p> <p><a href="https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426">https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426</a> (Microsoft Commercial Support Subcontractors)</p> <p><a href="https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx">https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx</a></p>
Rules concerning the personnel of the Cloud Service Provider	The personnel (both internal and external) of Microsoft has the required competencies and is cleared in accordance with internal policies.	<p><a href="https://www.microsoft.com/en-us/corporate-responsibility/empowering-employees">https://www.microsoft.com/en-us/corporate-responsibility/empowering-employees</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-human-resources">https://docs.microsoft.com/en-us/compliance/assurance/assurance-human-resources</a></p> <p>Subchapter 3.19 OPS.2.2.A19 Security Vetting of Employees</p>
Communication channels, contact persons and support	<p>The account manager is the primary contact point for customer.</p> <p>Microsoft provides several sources for communication and support regarding Azure. This includes supportive documentation for all services, a knowledge center, Azure portal, a FAQ-list or the Azure community supported by Microsoft.</p> <p>Additionally, Microsoft provides different levels of support that can be chosen for the subscriptions.</p>	<p><a href="https://azure.microsoft.com/en-us/resources/knowledge-center/">https://azure.microsoft.com/en-us/resources/knowledge-center/</a></p> <p><a href="https://azure.microsoft.com/en-us/support/faq/">https://azure.microsoft.com/en-us/support/faq/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/azure-portal/">https://docs.microsoft.com/en-us/azure/azure-portal/</a></p> <p><a href="https://azure.microsoft.com/en-us/support/community/">https://azure.microsoft.com/en-us/support/community/</a></p> <p><a href="https://azure.microsoft.com/en-us/support/options/">https://azure.microsoft.com/en-us/support/options/</a></p>
Network security (of Azure)	Implemented security mechanisms for the production network (customers and support personnel) as well as the overall network within Azure, e.g. between data centers.	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/production-network">https://docs.microsoft.com/en-us/azure/security/fundamentals/production-network</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-network">https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-network</a></p>

Consideration to be made	Conditions on Microsoft Azure	References
	<p>Network security is also achieved by cryptographic means.</p>	<p><a href="https://azure.microsoft.com/en-us/blog/azure-network-security/">https://azure.microsoft.com/en-us/blog/azure-network-security/</a></p> <p><a href="https://azure.microsoft.com/en-us/blog/how-microsoft-builds-its-fast-and-reliable-global-network/">https://azure.microsoft.com/en-us/blog/how-microsoft-builds-its-fast-and-reliable-global-network/</a></p> <p>Subchapter 3.17 OPS.2.2.A17 <i>Use of Encryption When Using the Cloud</i></p>
<p>Rules concerning processes, working procedures, changes and responsibilities</p>	<p>Azure includes the provision as an online cloud service and underlies a comprehensive set of rules, including information security policies (e.g., asset management, malware protection).</p> <p>The division of responsibilities, processes and procedures are generally defined in the particular agreements.</p> <p>Furthermore, multiple possibilities for support, service monitoring and further information exchange are offered to the customer of Azure.</p> <p>Microsoft provides an overview about security relevant information regarding Azure, like physical infrastructure, network, monitoring or malware protection.</p> <p>Microsoft is publishing information about updates, features and planned developments on their webpage. Change management and test policies are defined in an internal policy document.</p>	<p><a href="https://www.microsoft.com/licensing/terms/productoffering">https://www.microsoft.com/licensing/terms/productoffering</a></p> <p><a href="https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services">https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services</a></p> <p>Subchapter 2.1 <i>Shared Responsibility Model</i></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/">https://docs.microsoft.com/en-us/azure/security/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-monitoring">https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-monitoring</a></p> <p><a href="https://azure.microsoft.com/en-us/updates/">https://azure.microsoft.com/en-us/updates/</a></p>
<p>Provisions for ending the contractual agreement</p>	<p>Azure is offered on a subscription basis, but an early termination may be possible.</p> <p>More information regarding the end of contract is provided in the related requirement.</p>	<p><a href="https://www.microsoft.com/licensing/terms/productoffering">https://www.microsoft.com/licensing/terms/productoffering</a></p> <p><a href="https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services">https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cancel-azure-subscription">https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cancel-azure-subscription</a></p>

Consideration to be made	Conditions on Microsoft Azure	References
<p>Secure deletion of data by the cloud service provider</p>	<p>When a non-preview paid subscription is terminated or ends, the Azure customer account is changed to a limited-function account. Then customers have 90 days to export their data. After these 90 days the account will be disabled and customer data will be deleted. The account itself will be deleted no more than 180 days after it was terminated or the subscription ended.</p> <p>Physical storage media will be securely destroyed on-site at the end of their service life.</p> <p>Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. All Azure services use approved media storage and disposal management services.</p>	<p>Subchapter 3.14 OPS.2.2.A14 <i>Orderly Termination of a Cloud Service Relationship</i></p> <p><a href="https://docs.microsoft.com/en-us/azure/billing/billing-how-to-cancel-azure-subscription">https://docs.microsoft.com/en-us/azure/billing/billing-how-to-cancel-azure-subscription</a></p> <p><a href="https://www.microsoft.com/en-us/trustcenter/privacy/data-management">https://www.microsoft.com/en-us/trustcenter/privacy/data-management</a></p> <p><a href="https://aka.ms/DPA">https://aka.ms/DPA</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security#data-bearing-devices">https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security#data-bearing-devices</a></p>
<p>Emergency preparedness</p>	<p>Azure has defined rules for continuation of services to the level set out by the SLA. Corresponding safeguards include the geographical separation of data centers and continuous replication between them.</p> <p>Azure provides services to deploy replication, failover, and recovery processes such as Azure Backup and Site Recovery.</p>	<p><a href="https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services">https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/architecture/reliability/disaster-recovery">https://docs.microsoft.com/en-us/azure/architecture/reliability/disaster-recovery</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/backup/backup-overview">https://docs.microsoft.com/en-us/azure/backup/backup-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview">https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview</a></p>
<p>Legal requirements</p>	<p>Microsoft complies with laws and rules concerning its provision of the cloud service. Microsoft publishes data about law enforcement requests from law enforcement agencies around the world and how they were handled twice a year.</p>	<p><a href="https://www.microsoft.com/en-us/corporate-responsibility/lerr">https://www.microsoft.com/en-us/corporate-responsibility/lerr</a></p> <p><a href="https://www.microsoft.com/en-us/trust-center/privacy">https://www.microsoft.com/en-us/trust-center/privacy</a></p> <p><a href="https://servicetrust.microsoft.com/View-Page/TrustDocumentsV3">https://servicetrust.microsoft.com/View-Page/TrustDocumentsV3</a></p>

Consideration to be made	Conditions on Microsoft Azure	References
	<p>Microsoft provides information about their handling of personal identifiable information and the General Data Protection Regulation (GDPR).</p> <p>The overall legal information can be accessed using the legal support webpage.</p>	<p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-EU-Model-Clauses">https://docs.microsoft.com/en-us/compliance/regulatory/offering-EU-Model-Clauses</a></p> <p><a href="https://azure.microsoft.com/en-us/support/legal/">https://azure.microsoft.com/en-us/support/legal/</a></p>
<p>Rules governing checks and audits</p>	<p>Azure is continuously audited due to the requirements of multiple standards and certifications. Microsoft provides information about its compliances, audits and certifications, including publicly available reports and results.</p> <p>Microsoft Azure offers customers the ability to monitor SLA compliance with the “Service Health” module.</p> <p>Cloud users have the ability to carry out penetration tests or vulnerability scans against their cloud services without notifying Microsoft, if the corresponding rules of engagement are adhered. The main restriction is that no Denial of Service tests are allowed and that no other customers must be disturbed by the tests performed.</p> <p>For controlling own services, Azure provides a wide range of logging and monitoring capabilities</p>	<p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-home">https://docs.microsoft.com/en-us/compliance/regulatory/offering-home</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/service-health/">https://docs.microsoft.com/en-us/azure/service-health/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing">https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing</a></p> <p><a href="https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement">https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit">https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit</a></p>
<p>Supervision of service delivery</p>	<p>The service delivery can be monitored using the „Service health” module in azure portal, on the azure status website or by customizing the monitoring capabilities provided by Azure.</p>	<p><a href="https://azure.microsoft.com/en-us/documentation/articles/insights-how-to-customize-monitoring/">https://azure.microsoft.com/en-us/documentation/articles/insights-how-to-customize-monitoring/</a></p> <p><a href="https://azure.microsoft.com/en-us/features/azure-portal/">https://azure.microsoft.com/en-us/features/azure-portal/</a></p> <p><a href="https://azure.microsoft.com/en-us/status/">https://azure.microsoft.com/en-us/status/</a></p>
<p>Data Protection</p>	<p>The contractual regulations on data protection may differ from organization to organization and should therefore be evaluated together with the data protection officer or the legal department.</p> <p>Microsoft offers customers the EU Standard Contractual Clauses (SCC) (also known as EU Model Clauses),</p>	<p><a href="https://aka.ms/DPA">https://aka.ms/DPA</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses">https://docs.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses</a></p> <p><a href="https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview">https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview</a></p>



Consideration to be made	Conditions on Microsoft Azure	References
	<p>which provide specific safeguards for the transfer of personal data for services included in the scope to contractually ensure that all personal data leaving the EEA is transferred in compliance with the GDPR.</p> <p>As a result of the European Court of Justice (ECJ) ruling in July 2020 that invalidated the EU-US Privacy Shield Agreement, the <i>Microsoft Products and Services Data Protection Addendum</i> was supplemented by the <i>Appendix C Additional Safeguard Addendum</i>. This appendix specifies additional security measures with regard to the processing of personal data.</p> <p>Microsoft provides information about how the GDPR requirements are handled and also gives information on how cloud-customer can handle the GDPR requirements. Furthermore, Microsoft signed up to the EU Cloud Code of Conduct (EU Cloud CoC) and therefore certifies that their cloud services adhere to the rigorous European data protection requirements.</p>	<p><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr</a></p> <p><a href="https://eu-coc.cloud/en/home.html">https://eu-coc.cloud/en/home.html</a></p>

### 3.10 OPS.2.2.A10 Secure Migration to a Cloud Service

This requirement focusses on the actual migration to a cloud service according to the considerations given in the migration security concept (see subchapter 3.5 *OPS.2.2.A5 Planning a Secure Migration to a Cloud Service* and 3.6 *OPS.2.2.A6 Planning the Secure Integration of Cloud Services*) discussed previously. The migration must be continuously monitored to detect and react to required changes or problems that may prevent or hinder the migration. If necessary, the migration should be cancelled and an investigation into the issues carried out. To reduce the risk of significant issues, a test or pilot migration should first be carried out.

Microsoft FastTrack can help with the migration to Microsoft Azure. FastTrack is a service included in Azure subscriptions. When using Microsoft FastTrack, your organization gets access to experts from

Microsoft specialized in migrating to Microsoft Azure. Likewise, Microsoft lists many of its external partners as cloud experts on its website.<sup>48</sup>

Microsoft provides tools to assist with migrating current resources to Azure.<sup>49</sup>

Microsoft Azure offers several services for developing and testing applications<sup>50</sup>, ranging from code sharing and collaboration to automated builds and test environments.

### 3.11 OPS.2.2.A11 Drawing Up Contingency Concept for a Cloud Service

A business continuity concept should be developed as a preventive safeguard for Azure. Especially, the absence of a disaster recovery plan can cause long downtimes, including productivity limitations and cloud services limitations. The disaster recovery plan should contain organizational and technical aspects. On the one hand, responsibilities should be defined and on the other hand, fail-safe infrastructures with redundancies should be set out.

This requirement does not cover any of the specifics of disaster recovery for the cloud service itself – that is Microsoft’s task and is covered by way of the applicable service levels<sup>51</sup> which are defined contractually. Instead, it covers the individual plan for your organization in the event of the loss of the cloud service itself or a loss of access to it. It also addresses situations where the applicable service levels do not cover your requirements.

Should the online services be unavailable, the disaster recovery plan may include carrying out data backups as described in subchapter 3.16 *OPS.2.2.A16 Implementing Backups*.

Furthermore, business continuity plans concerning the relevant business processes, which depend on Azure should consider specifically and in detail the loss of availability. This should be planned for independently of the reason for the availability loss (e.g., outage of Internet access in the local network, outage at the Internet service provider).

Table 8 Azure support for Business Continuity

Implementation guideline	Support by Microsoft	References
Organizational aspects of disaster prevention while using the cloud	Microsoft provides guidance for implementing a disaster recovery plan within Microsoft Azure.	<a href="https://docs.microsoft.com/en-us/azure/architecture/reliability/disaster-recovery">https://docs.microsoft.com/en-us/azure/architecture/reliability/disaster-recovery</a>
Technical aspects of disaster prevention while using the cloud	Azure Backup and Site Recovery or similar services from an external	<a href="https://azure.microsoft.com/en-us/services/site-recovery/">https://azure.microsoft.com/en-us/services/site-recovery/</a> <a href="https://azure.microsoft.com/en-us/services/backup">https://azure.microsoft.com/en-us/services/backup</a>

<sup>48</sup> <https://azure.microsoft.com/en-us/partners/>

<sup>49</sup> <https://azure.microsoft.com/en-us/downloads/>

<sup>50</sup> <https://azure.microsoft.com/en-us/product-categories/devops/>

<sup>51</sup> <https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services>

Implementation guideline	Support by Microsoft	References
	<p>backup provider can be used to implement a backup concept and recover lost data.</p> <p>Further protection in a hybrid cloud environment is offered by Azure Stack. Azure Stack enables consistent execution of hybrid applications at the local level without cloud boundary limitations.</p> <p>For systems with a very high protection requirement, a hybrid environment using Azure Stack can be considered.</p>	<p><a href="https://azure.microsoft.com/en-us/overview/azure-stack/">https://azure.microsoft.com/en-us/overview/azure-stack/</a></p>

### 3.12 OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations

The purpose of this requirement is to maintain a comparable or enhanced level of information security after migrating to a cloud service. Accordingly, guidelines and documentation should be kept up to date and compliance with standards should be regularly checked, by both the customer as well as the cloud service provider.

Table 9 Maintenance of information security

Requirements	Details	References
Documentation and policies (for example instruction manuals and procedures) need to be updated at regular intervals.	<p>The review and update of policies at regular intervals is part of an effective information security management system (ISMS). This process should be implemented within the document management process.</p> <p>Microsoft provides evidence of compliance to this requirement through certifications. The certificates can be accessed via the Service Trust Portal (STP).</p>	<p><a href="https://servicetrust.microsoft.com/">https://servicetrust.microsoft.com/</a></p>
The rendering of services should be checked regularly.	<p>Microsoft Azure includes an integrated SLA Monitoring system ("Service Health"), which can be used to review the compliance of the cloud services.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/azure-monitor/data-platform">https://docs.microsoft.com/en-us/azure/azure-monitor/data-platform</a></p> <p><a href="https://azure.microsoft.com/en-us/features/azure-portal/">https://azure.microsoft.com/en-us/features/azure-portal/</a></p>

Requirements	Details	References
	Microsoft reserves the right to perform audits of contractors in accordance with the applicable terms and conditions that are agreed upon with the service providers.	<a href="https://azure.microsoft.com/en-us/status/">https://azure.microsoft.com/en-us/status/</a> <a href="https://www.microsoft.com/licensing/terms/productoffering">https://www.microsoft.com/licensing/terms/productoffering</a> <a href="https://www.microsoft.com/en-us/procurement/contracting-terms-conditions.aspx">https://www.microsoft.com/en-us/procurement/contracting-terms-conditions.aspx</a>
Security certificates supplied by the cloud service provider.	Microsoft Azure offers in this respect a variety of publications and verifications as well as applicable certifications. This can be verified by a user of Microsoft Azure on the public website as well as in the form of an audit, which can be viewed in the Service Trust Portal (STP).	<a href="https://servicetrust.microsoft.com">https://servicetrust.microsoft.com</a> <a href="https://servicetrust.microsoft.com/Documents/ComplianceReports">https://servicetrust.microsoft.com/Documents/ComplianceReports</a>
Coordination talks should be held regularly between the cloud service provider and the organization using the cloud.	Microsoft Azure offers a variety of support options. Customers will be contacted in the event of significant service disruption.	<a href="https://azure.microsoft.com/en-us/support/options/">https://azure.microsoft.com/en-us/support/options/</a>
Exercises and tests should be carried out to practice responding to system failures.	Microsoft Azure has set out rules for continuation of services to the level set out by the SLA. Additionally, Microsoft provides a guideline for building a reliable application in Azure.	<a href="https://www.microsoft.com/licensing/terms/productoffering">https://www.microsoft.com/licensing/terms/productoffering</a> <a href="https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/overview">https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/overview</a>
Ensure proper administration of cloud services	<p>Incorrect cloud administration can lead to considerable security problems (service failure, data loss, etc.) due to the very high complexity. Even minor errors or failures can have a major impact (not just on security) on a cloud infrastructure.</p> <p>Microsoft offers blueprints as an instrument to define a repeatable set of cloud resources with a rule set. Such a rule set can include configurations, but also security constraints.</p>	<a href="https://docs.microsoft.com/en-us/azure/governance/blueprints/overview">https://docs.microsoft.com/en-us/azure/governance/blueprints/overview</a>
Ensuring interoperability of cloud services	When using multiple cloud services, interoperability tests should be performed for each service to ensure	<a href="https://www.microsoft.com/en-us/legal/interoperability">https://www.microsoft.com/en-us/legal/interoperability</a>

Requirements	Details	References
	proper collaboration between the different cloud services.	
Proper execution of data backups	<p>A proper performance of data backup must be ensured so that no critical business processes can be endangered by a failure.</p> <p>Backups can be performed either by using a backup service from Azure, a backup services provided by an external provider or backup system of the customer. If an external provider is decided upon, the customer must ensure that all the requirements for backup and data security are fulfilled.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/backup/backup-overview">https://docs.microsoft.com/en-us/azure/backup/backup-overview</a></p> <p>Subchapter 3.16 OPS.2.2.A16 Implementing Backups</p>
Control of technical safeguards to prevent the use of unauthorized services	<p>This requirement is the responsibility of the cloud user.</p> <p>The IT organization should control the technical safeguards, for example with the help of proxies or cloud access security brokers (CASB), to prevent the unauthorized use of services.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task">https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task</a></p> <p><a href="https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps">https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps</a></p>
Performing audits, security checks, penetration tests or vulnerability analyses	<p>Customers have the ability to carry out penetration tests or vulnerability scans against their cloud services without notifying Microsoft, if the corresponding rules of engagement are adhered. The main restriction is that no Denial of Service tests are allowed and that no other customers must be disturbed by the tests performed.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing">https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing</a></p> <p><a href="https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement">https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement</a></p>

### 3.13 OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage

As part of an efficient information security management, the regular review of the established safeguards should be carried out. This ensures that customers satisfy their auditing requirements and also that agreements are being up-held on both sides. This may be achieved through, for instance, on-site audits or specific questionnaires, independent of the cloud service model.

Microsoft Azure is audited continually, due to the requirements of multiple international and national compliance standards and certifications and provides corresponding compliance reports and several

certification assessment reports<sup>52</sup>. These include the reports for ISO 27017, ISO 27018 and SOC (see chapter 4 for further details). These audits or reviews are conducted by accredited audit companies, with additional internal audits being carried out controlled by Microsoft. Information about these audits are available online in the Microsoft Trust Center. In addition, contracted enterprise and government customers can opt-in to the Service Trust Portal (STP)<sup>53</sup>, which provides direct access to many of the compliance reports and attestations.

The responsibility of reading and assessing the reports lies with the cloud customer. The customer should ensure that the assessment of the reports is carried out by qualified personnel.

### 3.14 OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship

Prior to concluding a contract with a cloud service provider, the relevant aspects for the termination of the cloud services agreement should be defined. In a critical situation, the absence of contractual provisions prevents the termination of the service relationship. Upon termination of the service agreement, business operations should not be affected negatively. This requirement aims to make clear that a move either to another cloud service provider or back to an on-premises infrastructure model must be planned as thoroughly as the initial integration. The planning and migration concept should take into account the security concept in much the same way as in the original move to the cloud.

The preparation of an exit strategy helps to minimize the risks associated with a short-term change of one or more cloud services. Microsoft provides the guide "Exit Planning for Microsoft Cloud Services"<sup>54</sup> to its customers.

Azure provides several ways to export data from Azure that are addressed in subchapter 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*. When terminating the Azure contract as an online service, your organization should, among other things, ensure the following:

- All relevant working data has been transferred completely to the new environment.
- All relevant data to be preserved or archived has been transferred to appropriate storage.
- The new environment offers all necessary features and functions as required.

In Microsoft Azure customer data will be deleted at most 90 or 180 days after the end of the agreed usage period or the cancellation of the user agreement<sup>55</sup>.

---

<sup>52</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

<sup>53</sup> <https://servicetrust.microsoft.com/>

<sup>54</sup> [https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913\\_FAQ\\_and\\_White\\_Papers](https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_FAQ_and_White_Papers)

<sup>55</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cancel-azure-subscription>  
<https://aka.ms/DPA>

## 3.15 OPS.2.2.A15 Ensuring the Portability of Cloud Services

This requirement aims to ensure a high degree of flexibility when changing cloud service provider, bringing data into the cloud or bringing a cloud service back in-house. A number of requirements must be considered in this case, in particular concerning file formats and portability testing.

Microsoft has shown a commitment to interoperability and portability. Azure supports a broad selection of operating systems, programming languages, frameworks, tools, databases, and devices, so that customer can choose the most suitable solutions.<sup>56</sup> Additionally third party tools support the import and export of data to different Azure services.

Further portability considerations are listed in the table below for selected cloud services.

Table 10 Portability of Azure cloud services

Cloud service	Portability	References
Azure Active Directory	<p>Using Azure Active Directory enables the use of Single-Sign-On across thousands of cloud services and applications.</p> <p>With Azure AD Connect, local profiles can be integrated into Azure Active Directory and synchronized across the cloud.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is">https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/what-is-hybrid-identity">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/what-is-hybrid-identity</a></p>
Azure KeyVault	<p>Key Vault is a cloud service for secure secrets management on Microsoft Cloud Germany. Portability is not provided for Azure Key Vault.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/key-vault/general/overview">https://docs.microsoft.com/en-us/azure/key-vault/general/overview</a></p>
Azure Portal	<p>Azure Portal is a web application provided by Microsoft. There are no portability considerations.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-overview">https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-overview</a></p>
Blob Storage	<p>The Azure Blob Storage allows the customer to import and export data by using the import/export functionality.</p> <p>The Azure Storage Import-Export REST API provides an API to manage automatic transfers of data to or from blob storages.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-overview">https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service">https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service</a></p> <p><a href="https://docs.microsoft.com/en-us/rest/api/storageimportexport/">https://docs.microsoft.com/en-us/rest/api/storageimportexport/</a></p>

<sup>56</sup> <https://docs.microsoft.com/en-us/azure/#pivot=products>  
<https://docs.microsoft.com/en-us/azure/#pivot=sdkttools>  
<https://docs.microsoft.com/en-us/azure/containers/>

Cloud service	Portability	References
Cloud Services	Cloud Services is a platform for developing and deploying your own cloud services and applications. There are no portability considerations.	<a href="https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-choose-me">https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-choose-me</a>
Cosmos Databases	Cosmos Databases offers a choice of APIs to work with your data stored in your database. It allows migrating application while preserving significant portions of your application logic. It is designed to keep applications portable and thus vendor-agnostic.	<a href="https://docs.microsoft.com/en-us/azure/cosmos-db/introduction">https://docs.microsoft.com/en-us/azure/cosmos-db/introduction</a>
Kubernetes	With Kubernetes containerized workload can be moved seamlessly from local development machines to different environments.	<a href="https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes">https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes</a>
Service Fabric	Service Fabric is a platform for developing and deploying micro service-based applications and managing their life cycles. There are no portability considerations.	<a href="https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview">https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview</a>
SQL Databases	The Azure SQL Databases can be copied to a BACPAC file and simply deployed in other environments.	<a href="https://docs.microsoft.com/en-us/azure/sql-database/sql-database-technical-overview">https://docs.microsoft.com/en-us/azure/sql-database/sql-database-technical-overview</a> <a href="https://docs.microsoft.com/en-us/azure/sql-database/sql-database-export">https://docs.microsoft.com/en-us/azure/sql-database/sql-database-export</a>
Virtual Machines	Virtual machines can be imported to Azure by importing the generalized or specialized virtual hard disk (VHD).  Migration of VMware Virtual machines to Azure is possible agentless or agent-based.  Virtual machines can easily be exported, by downloading the virtual hard drive (VHD) and loading the VHD to another virtual machine.	<a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image</a>  <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/on-prem-to-azure">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/on-prem-to-azure</a>  <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/upload-generalized-managed">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/upload-generalized-managed</a>  <a href="https://docs.microsoft.com/en-us/azure/migrate/server-migrate-overview">https://docs.microsoft.com/en-us/azure/migrate/server-migrate-overview</a>



Cloud service	Portability	References
		<a href="https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware">https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware</a> <a href="https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware-agent">https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware-agent</a> <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/download-vhd">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/download-vhd</a> <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/linux/download-vhd">https://docs.microsoft.com/en-us/azure/virtual-machines/linux/download-vhd</a>
Virtual Networks	Azure Virtual Network offers an isolated, secure environment for virtual machines and applications. A network configuration file can be imported to and exported from Azure to configure virtual networks.	<a href="https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview">https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview</a>

### 3.16 OPS.2.2.A16 Implementing Backups

This requirement aims to ensure data availability when access to Azure data is lost, cloud services themselves are unavailable or when data is lost due to user action (e.g., inadvertent deletion of data).

Microsoft offers the cloud service Azure Backup. For example, virtual machines located either on-premise or in Azure can be backed up using this service.<sup>57</sup> In addition, third-party solutions for backups are also available. For example, some providers provide a solution involving a local backup or a backup to another cloud provider.

### 3.17 OPS.2.2.A17 Use of Encryption When Using the Cloud

For encryption and other cryptographic protection it is necessary to identify and define suitable safeguards including algorithms, protocols or key-length, because insufficiently protected data could be accessed by unauthorized third parties. Microsoft Azure provides different encryption options and thereby employs encryption in a number of different areas.<sup>58</sup> Customers have the option to enable encryption, dependent on the chosen service, using standard or individual encryption technologies. The different options for encryption are dependent on the actual service and thus have to be evaluated by

<sup>57</sup> <https://docs.microsoft.com/en-us/azure/backup/backup-overview>

<sup>58</sup> <https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview>  
<https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data>

the customer on a case-to-case basis making use of the documentations and guidelines provided by Microsoft for each of the services.

The following table exemplarily outlines functionalities provided by Azure to encrypt data-at-rest, in-transit and how corresponding secrets can securely be managed.

Table 11 Encryption and key management

Category	Microsoft's Offer	References
Encryption of data at-rest	<p>In general client-side encryption, (customer) and/or server-side encryption (within cloud) for data at-rest is possible for Azure services. For client-side encryption, the customer maintains the control of the encryption and related keys, but might lose functionality of the cloud service.</p> <p>Azure provides disk encryption for virtual machines via BitLocker for Windows or via DM-Crypt for Linux. The corresponding keys can be stored in Azure Key Vault.</p> <p>Azure storage service provides encryption for Azure blob storage and Azure file shares using Azure Storage Service Encryption with an AES256 encryption. The corresponding encryption is transparent for users.</p> <p>For the different kinds of databases in Azure several encryption methods are provided. Transparent Data Encryption is used for server-side encryption. For Azure SQL also client-side encryption via the "Always Encrypted" feature is possible.</p> <p>Additionally, Azure provides cell-level or column level encryption for certain databases that allow the usage of different symmetric or asymmetric keys per cell or column.</p> <p>Azure Data Lake Store provides transparent encryption for the customer.</p> <p>Different third party encryption solutions for Azure exist that realize client side encryption while maintaining certain cloud service functionality like search features.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest">https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest</a></p> <p><a href="https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption">https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss">https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption">https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations">https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations</a></p> <p><a href="https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption">https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption</a></p> <p><a href="https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine">https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine</a></p> <p><a href="https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/encrypt-a-column-of-data">https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/encrypt-a-column-of-data</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-encryption">https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-encryption</a></p>

Category	Microsoft's Offer	References
Encryption of data in-transit	<p>Microsoft uses the Transport Layer Security (TLS) protocol with Perfect Forward Secrecy (PFS) to protect data when it is traveling between the cloud services and customers.</p> <p>The access to Azure Storage via Azure Portal and via REST API can be protected via HTTPS. The usage of HTTPS can be enforced by enabling the secure transfer option.</p> <p>Data in-transit to, from and between virtual machines in Azure can be encrypted. Access to Windows virtual machines can be secured using RDP over TLS. Access to Linux is based on SSH that is encrypted by default.</p> <p>Azure virtual networks can be accessed using VPN over a secure tunnel. Thereby, Azure provides different ways for VPNs:</p> <ul style="list-style-type: none"> <li>• Point-to-Site VPN allows individual clients to access an Azure virtual network using Secure Socket Tunnel Protocol (SSTP). Thereby, customers can use their own PKI certificates.</li> <li>• Site-to-Site and Multi-site can be used for cross-premises and hybrid virtual network configurations. The connection is realized over IPsec/IKE (IKEv1 or IKEv2).</li> <li>• VNet-to-VNet can be used to connect different virtual networks over IPsec/IKE (IKEv1 or IKEv2).</li> </ul> <p>Data in transit to Data lake store is encrypted using HTTPS.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview#encryption-of-data-in-transit">https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview#encryption-of-data-in-transit</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview#in-transit-encryption-in-vm">https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview#in-transit-encryption-in-vm</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways">https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-encryption">https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-encryption</a></p>
Encryption of data-in-use	<p>Azure is able to encrypt data during processing. With Azure Confidential Computing, Microsoft offers functions for data security through trusted execution environments (TEEs) or encryption mechanisms to protect data during use. TEEs are hardware or software implementations that protect the data being processed from access from outside the TEE.</p>	<p><a href="https://azure.microsoft.com/en-us/solutions/confidential-compute/">https://azure.microsoft.com/en-us/solutions/confidential-compute/</a></p> <p><a href="https://www.microsoft.com/en-us/research/uploads/prod/2018/08/Confidential_Computing_Mark-Russinovich_Manuel-Costa.pdf">https://www.microsoft.com/en-us/research/uploads/prod/2018/08/Confidential_Computing_Mark-Russinovich_Manuel-Costa.pdf</a></p>

Category	Microsoft's Offer	References
Key management	<p>Azure provides the capabilities to store certificates and other secret information securely and provides different methods to realize a secure key management, for example:</p> <ul style="list-style-type: none"> <li>• Azure Key Vault stores secrets in a virtual key vault or a Hardware Security Module shared with other customer.</li> <li>• A dedicated HSM ensures that the Hardware Security Module for key management is only used by the one customer.</li> </ul> <p>Bring-your-own-key allows the key generation in the customer's HSM. The key is then transferred to a HSM within Azure.</p>	<p><a href="https://docs.microsoft.com/en-us/azure/key-vault/about-keys-secrets-and-certificates">https://docs.microsoft.com/en-us/azure/key-vault/about-keys-secrets-and-certificates</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/key-vault/general/overview">https://docs.microsoft.com/en-us/azure/key-vault/general/overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys">https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys">https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/information-protection/configure-adrms-restrictions">https://docs.microsoft.com/en-us/azure/information-protection/configure-adrms-restrictions</a></p>

### 3.18 OPS.2.2.A18 Use of Federation Services

In context of cloud computing projects, the use of federated services should be reviewed. Using federated services, user information or other personal information of employees may be securely transmitted outside of the company. The key trait is the separation of authentication (identity provider) and authorization (service provider).

The primary safeguard is to ensure that only the minimum necessary information is sent in the SAML<sup>59</sup> ticket to the cloud service provider. Additionally, user rights and roles must be regularly checked to ensure that only authorized users have access.

Microsoft offers the possibility to make use of hybrid on-premises and cloud accounts/identities for azure through Azure Active Directory for the management of users and groups in Azure.<sup>60</sup> There are three general ways to realized hybrid accounts with different advantages and disadvantages:<sup>61</sup>

- **Password hash synchronization (PHS):**<sup>62</sup> For PHS Azure Active Directory Connect synchronizes a hash of user password hashes from a customer local Active Directory to Azure Active Directory, allowing Azure Active Directory to validate directly user passwords.

<sup>59</sup> SAML (Security Assertion Markup Language) is a standard authentication and authorization protocol

<sup>60</sup> <https://docs.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings>

<sup>61</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity>

<sup>62</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs>

- **Pass-through authentication (PTA):**<sup>63</sup> PTA allows users to sign in on-premises and to Azure using the same password. If a user signs in using Azure Active Directory, PTA validates the password directly against your on-premises Active Directory, allowing enforcing on-premises Active Directory security and password policies.
- **Active Directory Federation Services (ADFS):**<sup>64</sup> ADFS established a federation between the on-premises environment with Azure Active Directory that can be used for authentication and authorization. ADFS ensures that all user authentications occur on-premises and allows administrators to implement more rigorous levels of access control. PHS can optionally be implemented as a backup for the case of ADFS or network failure.

Azure Active Directory, supports the SAML 2.0 protocol<sup>65</sup> as well as WS-Federation and OpenID Connect.<sup>66</sup> The information contained in the SAML<sup>65</sup> tickets can be configured according to organizational requirements or the requirements of each application.<sup>67</sup>

The user rights should be regularly checked and it should be ensured, that a SAML<sup>65</sup> ticket can only be granted to privileged users. Checking assignment of privileges should be part of a well-defined process of identity and access privilege assignment. IT-Grundschutz module *ORP.4 Identity and access management*<sup>68</sup> offers the guidelines for implementing the necessary procedures. The Azure Active Directory service Access Reviews can be used regularly to check permissions. This service can be used to initiate automated access reviews.<sup>69</sup>

Furthermore, checking the correct ticket issuing process of SAML<sup>65</sup> to authorized users should be part of audits and technical tests as part of the established ISMS. The fulfillment of this requirement is the responsibility of the customer.

### 3.19 OPS.2.2.A19 Security Vetting of Employees

The customer should be aware that the service provider is performing employee background checks within the legal constraints.

Microsoft conducts security checks and background verification of all employees, internal and external, who have access to the data of cloud customers.

In addition, Microsoft pursues a strict supplier policy. For successful supplier collaboration, Microsoft's Supplier Program (MSP) defines the way key business-critical and strategic suppliers do business with

<sup>63</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

<sup>64</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

<sup>65</sup> <https://docs.microsoft.com/en-us/azure/active-directory/develop/single-sign-on-saml-protocol>

<sup>66</sup> <https://docs.microsoft.com/en-us/azure/active-directory/develop/id-tokens>

<sup>67</sup> <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-saml-claims-customization>

<sup>68</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium\\_Einzel\\_PDFs\\_2022/02\\_ORP\\_Organisation\\_und\\_Personal/ORP\\_4\\_Identitaets\\_und\\_Berechtigungsmanagement\\_Editon\\_2022.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2022.pdf)  
[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompodium/bau-steine/ORP/ORP\\_4\\_Identit%C3%A4ts- und\\_Berechtigungsmanagement.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompodium/bau-steine/ORP/ORP_4_Identit%C3%A4ts- und_Berechtigungsmanagement.html)(German only)

<sup>69</sup> <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

Microsoft, including the requirements and expectations of Microsoft and its customers.<sup>70</sup> Additionally, suppliers are invited to the MSP program only if they meet Microsoft compliance requirements.

Furthermore, the Microsoft Supplier Code of Conduct (SCoC) requires the supplier to conduct a background screening, to the extent allowable by applicable law, prior to any assignment of the supplier's employees to provide services to Microsoft.<sup>71</sup> For Microsoft's internal personnel, background screening depends on the role and the necessary access privileges and is prescribed in the Microsoft Personnel Screening Standard.<sup>72</sup> Microsoft also offers the SCoC Training Program to provide training to supplier employees.<sup>73</sup>

---

<sup>70</sup> <https://www.microsoft.com/en-us/procurement/msp-overview.aspx?activetab=pivot1:primaryr4>

<sup>71</sup> <https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr7>

<sup>72</sup> <https://www.microsoft.com/en-us/procurement/msp-overview.aspx?activetab=pivot1:primaryr4>  
<https://docs.microsoft.com/en-us/compliance/assurance/assurance-human-resources>

<sup>73</sup> <https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr7>

# 4

## Implementation of Minimum Standard for the Use of External Cloud Services

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has published a minimum standard<sup>74</sup>, which applies to federal authorities. It sets requirements for the procurement, use and termination of cloud services. In this context, external cloud services are cloud services not provided by federal authority.

If the demand for an IT service cannot be met by the federal authority's own IT resources, but can be covered e.g. by Azure, the federal authority can decide to use the external cloud service instead of internal IT resources. This is defined as the use of external cloud services. In contrast, the co-use of external cloud services describes the use of external cloud services by users of a federal authority without a contractual relationship between the federal authority and the cloud service provider.

This chapter describes how all requirements of the *BSI minimum standard for the use of external cloud services*<sup>74</sup> can be implemented for Azure. While some requirements can only be fulfilled individually by the institution, Microsoft can provide information for all requirements.

The *BSI's minimum standard for the use of external cloud services*<sup>74</sup> often refers to IT-Grundschutz requirements with regard to the requirements to be implemented. The following table provides an overview of the references to IT-Grundschutz requirements.

Table 12: Overview of interfaces to IT-Grundschutz requirements

Requirement	Links
NCD.2.1.01 Strategy for Cloud Usage	Subchapter 3.1 <i>OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage</i>
NCD.2.1.02 Security Policy for External Cloud Usage	Subchapter 3.2 <i>OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage</i>
NCD.2.1.03 Security Concept for External Cloud Services	Subchapter 3.7 <i>OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage</i>

<sup>74</sup> [https://www.bsi.bund.de/DE/Themen/Deffentliche-Verwaltung/Mindeststandards/Externe\\_Cloud-Dienste/Externe\\_Cloud-Dienste\\_node.html](https://www.bsi.bund.de/DE/Themen/Deffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html) (German only)

Requirement	Links
NCD.2.1.04 Emergency and Continuity Management	<p>Subchapter 3.11 <i>OPS.2.2.A11 Drawing Up Contingency Concept for a Cloud Service</i></p> <p>Subchapter 3.15 <i>OPS.2.2.A15 Ensuring the Portability of Cloud Services</i></p> <p>Subchapter 3.16 <i>OPS.2.2.A16 Implementing Backups</i></p>
NCD.2.2.01 Implementation of Security Requirements	<p>Subchapter 3.2 <i>OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage</i></p>
NCD.2.2.02 Contractually Ensure Dealings with Subcontractors and Other External Third Parties	<p>Subchapter 3.8 <i>OPS.2.2.A8 Careful Selection of a Cloud Service Provider</i></p> <p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p>
NCD.2.2.03 Ensure Jurisdiction by Contract	<p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p>
NCD.2.2.04 Ensure Location by Contract	<p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p>
NCD.2.2.05 Ensure that Disclosure Obligations and Investigative Powers are Contractually Guaranteed	<p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p>
NCD.2.2.06 Regulating the Termination of the Contractual Relationship	<p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p> <p>Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i></p>
NCD.2.2.07 Ensure Data Return and Data Deletion at the Cloud Service Provider by Contract	<p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p> <p>Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i></p> <p>Subchapter 3.15 <i>OPS.2.2.A15 Ensuring the Portability of Cloud Services</i></p>



Requirement	Links
NCD.2.3.01 Integrate ISMS	<p>Subchapter 3.7 <i>OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage</i></p> <p>Subchapter 3.12 <i>OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations</i></p>
NCD.2.3.02 Verify Security Certifications	<p>Subchapter 3.13 <i>OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage</i></p>
NCD.2.3.03 Check Performance	<p>Subchapter 3.12 <i>OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations</i></p>
NCD.2.3.04 Comply with Information Obligations	<p>Subchapter 3.4 <i>OPS.2.2.A4 Definition of Areas of Responsibilities and Interfaces</i></p> <p>Subchapter 3.12 <i>OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations</i></p>
NCD.2.3.05 Enable Two-Factor Authentication	<p>No reference</p>
NCD.2.4.01 Perform Data Return	<p>Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i></p> <p>Subchapter 3.15 <i>OPS.2.2.A15 Ensuring the Portability of Cloud Services</i></p>
NCD.2.4.02 Conform Data Deletion	<p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p> <p>Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i></p>
NCD.2.5.01 Shared Use of External Cloud Services	<p>Subchapter 3.1 <i>OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage</i></p> <p>Subchapter 3.2 <i>OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage</i></p> <p>Subchapter 3.7 <i>OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage</i></p> <p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p>

## Requirement

## Links

Subchapter 3.17 *OPS.2.2.A17 Use of Encryption When Using the Cloud*

### 4.1 NCD.2.1.01 Strategy for Cloud Usage

The institution must create a cloud usage strategy in accordance with the BSI IT-Grundschutz requirement *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage* (see subchapter 3.1). As part of the cloud usage strategy, the institution must decide how it will deal with the risks associated with outsourcing to the cloud. After the cloud usage strategy has been created, it must be checked whether the use of Azure meets the requirements. The use of Azure should be reviewed as part of a risk analysis.

Microsoft provides information on creating a cloud usage strategy, for example, in the form of the "Enterprise Cloud Strategy"<sup>75</sup> guide. Further information on creating a cloud usage strategy is provided in subchapter 3.1 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage*.

For the risk analysis, Microsoft provides extensive information on its own security measures<sup>76</sup> and security measures per cloud service used, which can be carried out by the cloud customer. For example, the Always Encrypted<sup>77</sup> functionality can be activated for some types of database-services, so that individual database columns are encrypted.

### 4.2 NCD.2.1.02 Security Policy for External Cloud Usage

In accordance with the BSI IT-Grundschutz requirement *OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage* (see subchapter 3.2), the institution planning to use Azure must create a security policy by the responsible persons. The *BSI's minimum standards for the use of external cloud services*<sup>78</sup> stipulate that the implementation of and compliance with the basic criteria according to the BSI's Cloud Computing Compliance Criteria Catalogue (C5)<sup>79</sup> must be specified as special security requirements for the cloud service provider in the security policy.

---

<sup>75</sup> <https://info.microsoft.com/enterprise-cloud-strategy-ebook.html>

<sup>76</sup> <https://docs.microsoft.com/en-us/azure/security/fundamentals/overview>

<sup>77</sup> <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

<sup>78</sup> [https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe\\_Cloud-Dienste/Externe\\_Cloud-Dienste\\_node.html](https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html) (German only)

<sup>79</sup> [https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance\\_Criteria\\_Catalogue/C5\\_NewRelease/C5\\_NewRelease\\_node.html](https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html)

External auditors have determined compliance with the basic criteria according to the BSI's Cloud Computing Compliance Criteria Catalogue (C5)<sup>79</sup> for Azure. The SOC 2 report on the audit can be viewed in the Service Trust Portal (STP)<sup>80</sup>.

### 4.3 NCD.2.1.03 Security Concept for External Cloud Services

In addition to the cloud usage strategy (see subchapter 4.1 *NCD.2.1.01 Strategy for Cloud Usage*) and a cloud security policy (see subchapter 4.2 *NCD.2.1.02 Security Policy for External Cloud Usage*), a security concept must also be drawn up in accordance with the IT-Grundschutz requirement of BSI *OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage* (see subchapter 3.7).

As part of the IT security concept, the level of protection required for the business data processed in the cloud must be considered in a risk analysis. For the risk analysis, Microsoft provides extensive information on its own security measures<sup>81</sup> and security measures per cloud service used, which can be carried out by the cloud customer. For example, the Always Encrypted<sup>82</sup> functionality can be activated for some types of database-services, so that individual database columns are encrypted.

Via tagging<sup>83</sup>, cloud customers can apply the data classification to the individual cloud services and use this data classification to enforce security requirements via Azure Policy<sup>84</sup> or Azure Purview<sup>85</sup>, such as that a database must never be deployed unencrypted. In addition, different database services<sup>86</sup> come with their own data classification mechanisms.

Further information on developing a cloud security concept is given in subchapter 3.7 *OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage*.

### 4.4 NCD.2.1.04 Emergency and Continuity Management

As in the IT-Grundschutz requirement *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage* (see subchapter 3.1), the *BSI's minimum standard for the use of external cloud services*<sup>87</sup> also requires an assessment by the institution of how a failure of Azure would affect the institution. In addition, it should be checked together with the responsible emergency officer whether the use of Azure affects the previous disaster management and thus the previous preventive / reactive measures can be adapted.

---

<sup>80</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

<sup>81</sup> <https://docs.microsoft.com/en-us/azure/security/fundamentals/overview>

<sup>82</sup> <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

<sup>83</sup> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources>

<sup>84</sup> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>  
<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

<sup>85</sup> <https://docs.microsoft.com/en-us/azure/purview/overview>

<sup>86</sup> <https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview>

<sup>87</sup> [https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe\\_Cloud-Dienste/Externe\\_Cloud-Dienste\\_node.html](https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html) (German only)

With its own architecture and infrastructure of the data centers and the cloud services operated in them, Microsoft ensures that a defined level of failure resistance is available. In addition, data storage<sup>88</sup>, for example, can be designed redundantly so that applications operated on Azure can be switched to other regions.

The preparation of a contingency concept is described in more detail in subchapter 3.11 *OPS.2.2.A11 Drawing Up Contingency Concept for a Cloud Service*. Further information can be found in subchapters 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services* and 3.16 *OPS.2.2.A16 Implementing Backups*.

## 4.5 NCD.2.2.01 Implementation of Security Requirements

Before concluding a contract, it must be assessed whether Azure can meet the requirements specified in the security policy (see subchapters 3.2 *OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage* and 4.2 *NCD.2.1.02 Security Policy for External Cloud Usage*) and, as part of the use of Azure, it must be regularly checked whether the security measures that can be implemented and the existing security evidence continue to comply with the security policy.

Microsoft provides extensive information on its own security measures<sup>89</sup> and security measures per cloud service used, which can be carried out by the cloud customer. For example, the Always Encrypted<sup>90</sup> functionality can be activated for some types of database-services, so that individual database columns are encrypted.

Microsoft permits audits by customers under terms and conditions set forth in the Microsoft Online Services Data Protection Addendum (DPA)<sup>91</sup>. If customer's audit requirements under the Standard Contractual Clauses or the Privacy Requirements cannot be adequately met by audit reports, documentation, or other compliance information that Microsoft makes generally available to Customer, Microsoft will provide the option to satisfy customer's additional audit requirements. Before an audit begins, Microsoft will determine with customer the scope, timing, duration, control and evidence requirements, and audit fees.

Microsoft constantly carries out its own audits in accordance with several national and international standards and has published corresponding certifications, proofs or audit reports in the Service Trust Portal (STP)<sup>92</sup>. The current SOC 2 report on the audit of the Cloud Computing Compliance Criteria Catalogue (C5)<sup>79</sup> can also be accessed there.

---

<sup>88</sup> <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

<sup>89</sup> <https://docs.microsoft.com/en-us/azure/security/fundamentals/overview>

<sup>90</sup> <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

<sup>91</sup> <https://aka.ms/DPA>

<sup>92</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

## 4.6 NCD.2.2.02 Contractually Ensure Dealings with Subcontractors and Other External Third Parties

The institution should ensure that it receives information on Microsoft subcontractors and their business relationships. Updates should be announced via a web portal or push notification by the cloud provider.

Microsoft provides a list of subcontractors and offers access to standardized service agreements, guidelines and codes of conduct.<sup>93</sup> External auditors have determined compliance with the basic criteria according to the BSI Cloud Computing Compliance Criteria Catalogue (C5)<sup>94</sup> for Azure. The SOC 2 report on the audit can be viewed in the Service Trust Portal (STP)<sup>95</sup>.

Further information can be found in subchapters 3.8 *OPS.2.2.A8 Careful Selection of a Cloud Service Provider* and 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*.

## 4.7 NCD.2.2.03 Ensure Jurisdiction by Contract

If possible, the place of jurisdiction should be Germany. It should be ensured that there is no loss of time and no loss of action if legal protection is required.

The country of the customer is defined as the place of jurisdiction in the data protection regulations.<sup>95</sup>

Information and links to the contract draft and the documents can be found in the subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*.

## 4.8 NCD.2.2.04 Ensure Location by Contract

The location where the data is processed should be contractually agreed. The authorization to process data in the secured regions depends on the data categorization according to the minimum standard, the risk analysis and the access possibilities of a foreign state.

Microsoft publishes the regions in which Azure services are operated.<sup>96</sup> However, for data processing reasons, customer data may be processed outside the selected region. The geographical storage region for data can be freely selected by the customer.<sup>97</sup> By the end of 2022, data storage and processing for Azure, among others, will take place exclusively within Europe.<sup>98</sup>

---

<sup>93</sup> <https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx>  
<https://www.microsoft.com/licensing/docs>

<sup>94</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

<sup>95</sup> <https://aka.ms/DPA>

<sup>96</sup> <https://azure.microsoft.com/en-us-de/global-infrastructure/services/>

<sup>97</sup> <https://azure.microsoft.com/en-us/global-infrastructure/regions/>

<sup>98</sup> <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098>

In addition, Microsoft publishes statistics on law enforcement requests from around the world twice a year.<sup>99</sup>

Information and links to the contract draft and the documents can be found in the subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*.

#### 4.9 NCD.2.2.05 Ensure that Disclosure Obligations and Investigative Powers are Contractually Guaranteed

As a cloud provider, Microsoft should report security incidents (and any other incidents) to the customers. This requirement should be contractually regulated. The *BSI's minimum standard for the use of external cloud services*<sup>100</sup> also requires the agreement of contractual penalties in the event of non-fulfilment.

Microsoft has an internal policy<sup>101</sup> on notifying affected parties during an information security incident. Information about obligations to inform subjects under the GDPR are published as well<sup>102</sup>. In addition, Microsoft publishes statistics on law enforcement requests from around the world twice a year.<sup>103</sup>

Information and links to the contract draft and the documents can be found in the subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*.

#### 4.10 NCD.2.2.06 Regulating the Termination of the Contractual Relationship

Termination of the contract should be possible with a notice period appropriate to the deployment scenario. In this context, short-term unilateral rights of termination or retention of the agreed services at the expense of the institution should be contractually excluded.

Microsoft's standard SLAs offer the customer the right to terminate the contract at any time. Further information and links to the termination of the contract can be found in the subchapters 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* and 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*.

#### 4.11 NCD.2.2.07 Ensure Data Return and Data Deletion at the Cloud Service Provider by Contract

When drafting the contract (see also subchapters 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* and 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*), the

---

<sup>99</sup> <https://www.microsoft.com/en-us/corporate-responsibility/lerr>

<sup>100</sup> [https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe\\_Cloud-Dienste/Externe\\_Cloud-Dienste\\_node.html](https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html) (German only)

<sup>101</sup> <https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification>

<sup>102</sup> <https://servicetrust.microsoft.com/ViewPage/GDPRBreach>

<sup>103</sup> <https://www.microsoft.com/en-us/corporate-responsibility/lerr>

portability of the data (see subchapter 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*) as well as the subsequent deletion of the data should be negotiated and recorded in the contract.

Microsoft grants at least 90 days of data access after termination of the subscription. Data will be deleted after 180 days at the latest. All storage devices on which customer data may be stored will be erased using a process that complies with NIST SP-800-88.<sup>104</sup>

## 4.12 NCD.2.3.01 Integrate ISMS

Azure as well as the cloud services used should be integrated into the ISMS of the institution. It should be noted that the requirements contained in the BSI Cloud Computing Compliance Criteria Catalogue (C5)<sup>99</sup>, which address the cloud customer, are implemented in the ISMS.

This is a customer-specific requirement. Information on the security concept can be found in subchapters 3.7 *OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage* and 3.12 *OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations*.

## 4.13 NCD.2.3.02 Verify Security Certifications

This requirement is customer-specific as it includes required certifications and audit reports based on the data categories according to the *BSI's minimum standards for the use of external cloud services*<sup>105</sup> and the customer's risk analysis. Furthermore, this requirement obliges the cloud customer to review regularly this evidence for compliance with security requirements.

Azure holds several global and regional certifications<sup>106</sup>. In addition, audit reports and other compliance information, such as penetration tests<sup>107,108</sup>, are regularly published on Microsoft's website. The responsibility for defining the required certifications and verifying that Azure holds these certifications lies with the customer.

Information can also be found in subchapter 3.13 *OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage*.

## 4.14 NCD.2.3.03 Check Performance

Before migrating to the cloud, the cloud user should make sure that the local infrastructure is adequate in terms of performance. In particular, the internet connection should meet the availability and

---

<sup>104</sup> <https://www.microsoft.com/en-us/trust-center/privacy/data-management>  
<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cancel-azure-subscription>  
<https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction>

<sup>105</sup> [https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe\\_Cloud-Dienste/Externe\\_Cloud-Dienste\\_node.html](https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html) (German only)

<sup>106</sup> <https://docs.microsoft.com/en-us/compliance/regulatory/offering-home>

<sup>107</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

<sup>108</sup> <https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3>

bandwidth requirements. This review should be repeated annually and should also assess the performance of the cloud service provider and the cloud service, as well as the network connection to the cloud service provider.

The current service status can be viewed online for Azure services.<sup>109</sup>

For more information and links on Azure migration and integration, see the following subchapters 3.5 *OPS.2.2.A5 Planning a Secure Migration to a Cloud Service* and 3.6 *OPS.2.2.A6 Planning the Secure Integration of Cloud Services*.

#### 4.15 NCD.2.3.04 Comply with Information Obligations

It is the institution's task to ensure that Microsoft, as a cloud service provider, complies with its contractual information obligations. Contractual information obligations exist, for example, when a sub-contractor is replaced or a relevant cyber-attack occurs.

Microsoft publishes information on various scenarios and incidents in order to fulfil its information obligations. Further information can be found in the following subchapters 3.4 *OPS.2.2.A4 Definition of Areas of Responsibilities and Interfaces* and 3.12 *OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations*.

#### 4.16 NCD.2.3.05 Enable Two-Factor Authentication

This requirement requires the use of multi-factor authentication (MFA) if available. At a minimum, multi-factor authentication (MFA) must be used for administrative accounts.

In Azure Active Directory, various options are offered to configure multi-factor authentication (MFA)<sup>110</sup>. Multi-factor authentication can be activated for all users, for individual users or with the help of conditional access for certain scenarios or events. Various multi-factor authentication (MFA) methods are supported, e.g. via mobile app, smart card or certain third-party MFA solutions.<sup>111</sup>

#### 4.17 NCD.2.4.01 Perform Data Return

All customer data must be returned by the cloud service provider in the agreed form at the end of cloud usage.

Further information on retrieving data from Azure can be found in subchapters 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship* and 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*.

---

<sup>109</sup> <https://status.azure.com/en-us/status>

<sup>110</sup> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing>

<sup>111</sup> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>



## 4.18 NCD.2.4.02 Conform Data Deletion

If data erasure is requested by the customer, the cloud service provider must contractually confirm the erasure of all data in accordance with *NCD.2.2.07 Ensure Data Return and Data Deletion at the Cloud Service Provider by Contract* (see subchapter 4.11). This includes data backups at the cloud service provider as well as data and data backups at possible subcontractors and other external third parties.

Customer must contact Microsoft for written proof of data deletion.

For information and links on terminating cloud usage, see subchapters 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* and 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*.

## 4.19 NCD.2.5.01 Shared Use of External Cloud Services

If a cloud service of another institution is used, various requirements must be complied with. The requirements listed below must also be implemented in whole or in part by the institution using a shared cloud service.

- *NCD.2.1.01 Strategy for Cloud Usage* (see subchapter 4)
- *NCD.2.2.01 Implementation of Security Requirements* (see subchapter 4.5)
- *NCD.2.2.04 Ensure Location by Contract* (see subchapter 4.8)

Furthermore, the contractual documents should be examined and compared with your own security requirements. The types of encryption used should also correspond to your own security requirements.

It should also be checked whether software installations for co-use of external cloud services on workstations or mobile devices are required. It should be checked whether the access and execution rights to be granted for this purpose are in line with the information security policy and security concept of the sharing institution and whether separate licenses may be required. In addition, the co-using institution can be guided by the *Minimum Standard for Mobile Device Management*<sup>112</sup>.

Microsoft publishes the generally applicable contract terms in the Licensing Portal<sup>113</sup>. Supplemental agreements should be provided by the contractor with whom the cloud is shared.

In Azure, communication data is encrypted using industry standards such as AES and TLS/SSL, and data-at-rest is also encrypted using various methods.<sup>114</sup> Further information and links can be found in subchapter 3.17 *OPS.2.2.A17 Use of Encryption When Using the Cloud*.

---

<sup>112</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard\\_Mobile-Device-Management.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf) (German only)

<sup>113</sup> <https://aka.ms/licensingdocs>

<sup>114</sup> <https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365>

With Intune, Microsoft provides Mobile Device Management (MDM) to secure mobile devices.<sup>115</sup> Together with conditional access, this can be used to restrict access to certain data or services in Azure.<sup>116</sup> Further information and links on aspects of mobile device management and conditional access can be found in subchapter 3.7 *OPS.2.2.A7 Drawing up a Security Concept for Cloud Usage*.

---

<sup>115</sup> <https://docs.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up>

<sup>116</sup> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

# 5

## Microsoft's Responsibilities as a Cloud Service Provider

Microsoft is responsible for the security of the cloud below the virtualization layer, with access to customer data. As the cloud customer should be able to evaluate the security of the cloud without the effort of a complete audit of the technical infrastructure but with similar adequate certainty, Microsoft has prepared a range of security related certifications and attestations for Azure.

The most important of these are:

- ISO 27001 (Information Security Management System)
- ISO 27017 (Code of practice for information security controls based on ISO 27002 for cloud services)
- ISO 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)
- Cloud Computing Compliance Controls Catalogue (C5)
- SOC 1 - SOC 2 - SOC 3 (SSAE16 / ISAE 3402)
- PCI-DSS (Payment Card Industry Data Security Standard)

Furthermore the feasibility of an "ISO 27001 certification based on IT-Grundschutz" for Azure is currently being analyzed. Such a certification will greatly ease the cloud customer's certification, but is not required.

# Appendix A

## Glossary of IT-Grundschutz-Terms

English term	German term	Description
BSI minimum standard for the use of external cloud services	Mindeststandards des BSI zur Nutzung externer Cloud-Dienste	This standard contains minimum-security requirements for the use of external cloud services in public administration.
Information Domain	Informationsverbund	This term refers to everything that falls under BSI IT-Grundschutz protection, i.e. all organizational and technical systems and processes to be modelled and matched with their appropriate requirements. This may refer to the entire organization or only a subset thereof, or even an individual process.
IT-Grundschutz Compendium	IT-Grundschutz Kompendium	Official body of standard threats and requirements in IT-Grundschutz methodology.
(IT) Security Concept	IT-Sicherheitskonzept	"IT Security Concept" describes the formal security concept according to IT-Grundschutz, the result of structure analysis, protection requirements, selection of safeguards, basic security checks and supplementary security analysis/risk analysis.
Modelling	Modellierung	Analyzing a system or process to specify the possible vulnerabilities and the belonging requirements.
Module	Baustein	Modules describe a specific item or process and draw together the relevant threats and requirements based on this.
Requirement	Anforderung	Requirements in BSI IT-Grundschutz are some kind of controls like there are used in the ISO 27001 Appendix A.

# Appendix B

## References to Further Information

Topic	Information Pointer
Legal information	<a href="https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx">https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx</a> <a href="https://www.microsoft.com/licensing/terms/welcome/welcomepage">https://www.microsoft.com/licensing/terms/welcome/welcomepage</a> <a href="https://www.microsoft.com/licensing/docs">https://www.microsoft.com/licensing/docs</a> <a href="https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services">https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services</a> <a href="https://aka.ms/DPA">https://aka.ms/DPA</a>
Due Diligence	<a href="https://azure.microsoft.com/en-us/overview/choosing-a-cloud-service-provider/">https://azure.microsoft.com/en-us/overview/choosing-a-cloud-service-provider/</a> <a href="https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist">https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist</a> <a href="https://www.microsoft.com/en-us/investor/default.aspx">https://www.microsoft.com/en-us/investor/default.aspx</a> <a href="https://www.microsoft.com/en-us/corporate-responsibility/lerr">https://www.microsoft.com/en-us/corporate-responsibility/lerr</a>
Compliance	<a href="https://servicetrust.microsoft.com/">https://servicetrust.microsoft.com/</a> <a href="https://www.microsoft.com/en-us/trust-center/">https://www.microsoft.com/en-us/trust-center/</a> <a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr</a> <a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics-windows">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics-windows</a> <a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-azure">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-azure</a>
Data Location	<a href="https://azuredatacentermap.azurewebsites.net">https://azuredatacentermap.azurewebsites.net</a>
Supplier and subcontractor management	<a href="https://www.microsoft.com/en-us/procurement/msp-overview.aspx">https://www.microsoft.com/en-us/procurement/msp-overview.aspx</a> <a href="https://go.microsoft.com/fwlink/?LinkId=2096306&amp;clid=0x407">https://go.microsoft.com/fwlink/?LinkId=2096306&amp;clid=0x407</a> (Microsoft Online Services Subprocessors List) <a href="https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426">https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426</a> (Microsoft Commercial Support Subcontractors)
Migration and portability	<a href="https://www.microsoft.com/en-us/legal/interoperability">https://www.microsoft.com/en-us/legal/interoperability</a> <a href="https://azure.microsoft.com/en-us/migration/">https://azure.microsoft.com/en-us/migration/</a>

Topic	Information Pointer
	<a href="https://azure.microsoft.com/en-us/migration/migration-partners/">https://azure.microsoft.com/en-us/migration/migration-partners/</a> <a href="https://azure.microsoft.com/en-us/resources/cloud-migration-simplified/">https://azure.microsoft.com/en-us/resources/cloud-migration-simplified/</a> <a href="https://azure.microsoft.com/mediahandler/files/resource-files/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20Onboarding%20Guide%20for%20IT%20Organizations.pdf">https://azure.microsoft.com/mediahandler/files/resource-files/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20Onboarding%20Guide%20for%20IT%20Organizations.pdf</a> <a href="https://azure.microsoft.com/mediahandler/files/resource-files/efc32c2a-5c32-407c-a67d-6116cb810546/Azure_Strategic_Implementation_Guide_for_IT_Organizations_New_to_Azure.pdf">https://azure.microsoft.com/mediahandler/files/resource-files/efc32c2a-5c32-407c-a67d-6116cb810546/Azure_Strategic_Implementation_Guide_for_IT_Organizations_New_to_Azure.pdf</a> <a href="https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service">https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service</a>
Availability, backup and resilience	<a href="https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview">https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview</a> <a href="https://azure.microsoft.com/en-us/resources/resilience-in-azure-whitepaper/">https://azure.microsoft.com/en-us/resources/resilience-in-azure-whitepaper/</a> <a href="https://azure.microsoft.com/en-us/features/resiliency/">https://azure.microsoft.com/en-us/features/resiliency/</a> <a href="https://azure.microsoft.com/en-us/services/backup">https://azure.microsoft.com/en-us/services/backup</a> <a href="https://docs.microsoft.com/en-us/azure/backup/backup-overview">https://docs.microsoft.com/en-us/azure/backup/backup-overview</a> <a href="https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/backup-and-recovery">https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/backup-and-recovery</a>
Logging and monitoring	<a href="https://docs.microsoft.com/en-us/azure/azure-monitor/overview">https://docs.microsoft.com/en-us/azure/azure-monitor/overview</a> <a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit">https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit</a> <a href="https://azure.microsoft.com/en-us/status/">https://azure.microsoft.com/en-us/status/</a> <a href="https://docs.microsoft.com/en-us/azure/sentinel/overview">https://docs.microsoft.com/en-us/azure/sentinel/overview</a> <a href="https://docs.microsoft.com/en-us/azure/service-health/">https://docs.microsoft.com/en-us/azure/service-health/</a>
Encryption	<a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview">https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview</a> <a href="https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption">https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption</a> <a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss">https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss</a> <a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview">https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview</a> <a href="https://docs.microsoft.com/en-us/azure/dedicated-hsm/overview">https://docs.microsoft.com/en-us/azure/dedicated-hsm/overview</a>
Further security aspects of Azure	<a href="https://info.microsoft.com/enterprise-cloud-strategy-ebook.html">https://info.microsoft.com/enterprise-cloud-strategy-ebook.html</a> <a href="https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview">https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview</a>

Topic	Information Pointer
	<p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview">https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview</a></p> <p><a href="https://azure.microsoft.com/en-us/solutions/confidential-compute/">https://azure.microsoft.com/en-us/solutions/confidential-compute/</a></p> <p><a href="https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security">https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security</a></p> <p><a href="https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune">https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/isolation-choices">https://docs.microsoft.com/en-us/azure/security/fundamentals/isolation-choices</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data">https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/anti-malware">https://docs.microsoft.com/en-us/azure/security/fundamentals/anti-malware</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/governance/blueprints/overview">https://docs.microsoft.com/en-us/azure/governance/blueprints/overview</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/governance/policy/overview">https://docs.microsoft.com/en-us/azure/governance/policy/overview</a></p> <p><a href="https://azure.microsoft.com/en-us/blog/azure-network-security/">https://azure.microsoft.com/en-us/blog/azure-network-security/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/pentesting">https://docs.microsoft.com/en-us/azure/security/fundamentals/pentesting</a></p>
Change Management	<p><a href="https://azure.microsoft.com/en-us/updates/">https://azure.microsoft.com/en-us/updates/</a></p>
BSI	<p><a href="https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.html">https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.html</a></p> <p><a href="https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html">https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html</a></p> <p><a href="https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html">https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html</a></p> <p><a href="https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf">https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf</a></p> <p><a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf</a> (German only)</p> <p><a href="https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html">https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html</a> (German only)</p> <p><a href="https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html">https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html</a></p>

Inés Atug, Manuel Atug, Marie-Luise Troschke, Andre Windsch

**HiSolutions AG**

Schloßstraße 1  
12163 Berlin

[info@hisolutions.com](mailto:info@hisolutions.com)

[www.hisolutions.com](http://www.hisolutions.com)

Fon +49 30 533 289-0

Fax +49 30 533 289-900

**HiSolutions AG**  
Niederlassung  
Frankfurt am Main  
Mainzer Landstraße 50  
60326 Frankfurt am Main

Fon: +49 30 533 289-0  
Fax: +49 30 533 289-900

**HiSolutions AG**  
Niederlassung  
Bonn  
Heinrich-Brüning-Straße 9  
53113 Bonn

Fon: +49 30 533 289-0  
Fax: +49 30 533 289-900

**HiSolutions AG**  
Niederlassung  
Nürnberg  
Zeltnerstraße. 3  
3. OG  
90443 Nürnberg

Fon: +49 911 8819 72 63  
Fax: +49 30 533 289-900

**HiSolutions AG**  
Niederlassung  
Düsseldorf  
Kaiserswerther Straße 135  
40474 Düsseldorf

Fon: +49 30 533 289-0  
Fax: +49 30 533 289-900