HISOLUTIONS

IT-Grundschutz Compliance on Azure

Version 19. September 2016

MICROSOFT DEUTSCHLAND GMBH

HiSolutions AG © 2016

Table of contents

1. Introduction ... 3
1.1 Executive Summary ... 3
1.2 Shared Responsibility Model ... 3
1.3 Basic IT-Grundschutz Implementation ... 4
2. Certification requirements ... 5
2.1 IT-Grundschutz Compliant Procedure ... 5
2.2 Integrating Microsoft Cloud Services into an Information Domain ... 5
2.2.1 Including the Cloud in the Structure Analysis ... 6
2.2.2 Determining the Protection Requirements for the Cloud Services ... 7
2.3 Modelling of Microsoft Cloud Basic Services ... 8
3. Implementation Module 1.17 Cloud Usage ... 9
3.1 S 2.40 (A) Timely Involvement of Staff/Factory Council ... 11
3.2 S 2.42 (A) Determination of Potential Communications Partners ... 11
3.3 S 2.534 (A) Determining a Cloud Usage Strategy ... 13
3.4 S 2.535 (A) Determining Security Policy for Cloud Usage ... 13
3.5 S 2.536 (A) Service Definition/Service Templates for Cloud Services ... 15
3.6 S 2.537 (A) Planning a Secure Migration to a Cloud Service ... 16
3.7 S 2.538 (A) Planning a Secure Integration of Cloud Services ... 17
3.8 S 2.539 (A) Creating a Security Concept for Cloud Services ... 17
3.9 S 4.459 (Z) Use of Encryption in Cloud Computing ... 19
3.10 S 4.461 (Z) Portability of Cloud Services ... 20
3.11 S 2.540 (A) Considered Selection of a Cloud Service Provider ... 22
3.12 S 2.541 (A) Contractual Agreements with Cloud Service Provider ... 23
3.13 S 2.542 (A) Secure Migration to a Cloud Service ... 27
3.14 S 2.543 (A) Maintaining Information Security in an Operational Cloud Service Environment ... 28
3.15 S 2.544 (C) Auditing Cloud Services ... 29
3.16 S 4.460 (Z) Use of Federated Services ... 30
3.17 S 2.307 (A) Well-Ordered Termination of an Outsourcing or Cloud Services Agreement ... 31
3.18 S 6.155 (A) Creation of a Disaster Recovery Plan for a Cloud Service ... 31
3.19 S 6.156 (Z) Implementing User-Side Data Backups ... 32
4. MICROSOFT's responsibilities as a Cloud Service Provider ... 33
Apendix A Glossary of IT-Grundschutz terms ... 34
Apendix B References to further information ... 35

1 Introduction

1.1 Executive Summary

Microsoft Azure is Microsoft's public cloud computing platform, offering a wide range of services from Infrastructure as a Service (IaaS) to Platform as a Service (PaaS) and Software as a Service (SaaS). Azure is especially suited for use in hybrid environments combining both on-premises and cloud infrastructure.

Microsoft Cloud Germany aims to offer all Azure services, but is physically based in Germany and offers additional protection from access by authorities from other jurisdictions violating domestic laws. This is also a requirement of German privacy law which strictly limits the transfer of personal data to other countries.

In Germany the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) provides the IT-Grundschutz methodology; consisting of an ISO 27001 compatible ISMS (BSI Standards 100-1, 100-2), a dedicated risk analysis method (BSI Standard 100-3), and the IT-Grundschutz Catalogues, a standard set of threats and safeguards for typical business environments.

The purpose of this workbook is to help customers of Microsoft Cloud Germany who wish to use Microsoft Cloud Germany Services implement the IT-Grundschutz methodology within the scope of their existing or planned ISO 27001 certification based on IT-Grundschutz.

This workbook describes how to model cloud services as part of the Information Domain[1], i.e. the certifiable scope of the ISMS, and how to apply the IT-Grundschutz methodology to applications within the cloud. An outline of how to implement the central IT-Grundschutz module M 1.17 Cloud Usage is given on a per-safeguard-basis.

1.2 Shared Responsibility Model

When implementing IT applications in a cloud service environment, the responsibility for implementing and maintaining security controls is, contrary to on-premises IT infrastructure, shared between customer and provider. Figure 1 shows a high level overview of how such partitioning may look. From the standpoint of the IT-Grundschutz methodology, final responsibility always lies with the customer (the data owner). A transfer of responsibilities can only occur when the provider includes the customers' applications in his own certification scope (i.e. a classical outsourcing scenario), including an aligned risk management.

[1] See Appendix A, Glossary of IT-Grundschutz Terms on page 15 for normative terms of IT-Grundschutz that have special meanings.

Recent versions of IT-Grundschutz allow a shared responsibility model that partitions responsibilities between customer and provider along virtualization boundaries, so that for each aspect there is only one party responsible (see Figure 1).

Figure 1: Shared Responsibilites for Security in Cloud Computing[2]

1.3 Basic IT-Grundschutz Implementation

This workbook is based on the 15th (2016) version of theIT-Grundschutz Catalogues. Since the 14th version the use of cloud services has been covered in its own module: M 1.17 Cloud Usage[3]. Together with the module M 5.23 Cloud Management it provides the basis for an orderly separation of responsibilities between cloud customer and cloud provider (See Figure 1).

The 14th and 15th revision of the IT-Grundschutz Catalogues by the BSI and the development of the module M 1.17 Cloud Usage created the opportunity to separate classic IT outsourcing from the usage of cloud services. Every requirement of the underlying service is implemented by the cloud customer as part of the module M 1.17 Cloud Usage.

[2] cf. Simorjay, Frank: Shared Responsibilities - For Cloud Computing. Ed. Microsoft, March 2016. (https://aka.ms/sharedresponsibility)

3 German: "B 1.17 Cloud-Nutzung"; no official translation available; see Appendix A (Glossary of IT-Grundschutz Terms) for a mapping of official German titles

2 Certification requirements

2.1 IT-Grundschutz Compliant Procedure

In order to remain IT-Grundschutz compliant whilst utilizing the Cloud Services of Microsoft Cloud Germany, the IT Security Concept must be updated to include the Cloud Services in accordance with BSI Standard 100-2. If necessary, the Information Domain must also be extended to include the cloud services.

The procedure for this is as follows:

1. All cloud services to be used and any directly impacted or additionally required target objects (e.g. web servers, networking equipment etc.) must be determined. During the structure analysis all target objects of the same type should be collated into target groups, in order to reduce complexity.
2. The protection requirements for each cloud service are determined by a responsible party from the service area.
3. The corresponding IT-Grundschutz modules and their respective safeguards are assigned to the appropriate target objects. In the case of IaaS further modules (dependent on the cloud service) are additionally applicable, as the customer enjoys an enhanced level of control over the target object along with correspondingly greater security responsibilities.
4. The current implementation is checked against safeguards of the modules in the basic security check.
5. The next step concerns target objects which have enhanced security requirements or for which no applicable IT-Grundschutz module is available. A supplementary security analysis is carried out for each of these target objects to determine if a further risk analysis is necessary.
6. For the selected target objects a risk analysis is conducted in which the threats and the resulting risksare identified and supplementary safeguards are defined.

2.2 Integrating Microsoft Cloud Services into an Information Domain

A useful approach for integrating cloud services into the Information Domain is to structure them as they would be structured if they were the equivalent private infrastructure the cloud services replace. Depending on the applicable service model, different layers (of the Grundschutz Model) fall under the responsibility of the cloud service provider.

Figure 2 shows this in practice. The servers and services operated by the cloud customer are referred to here as the “virtual customer environment”.

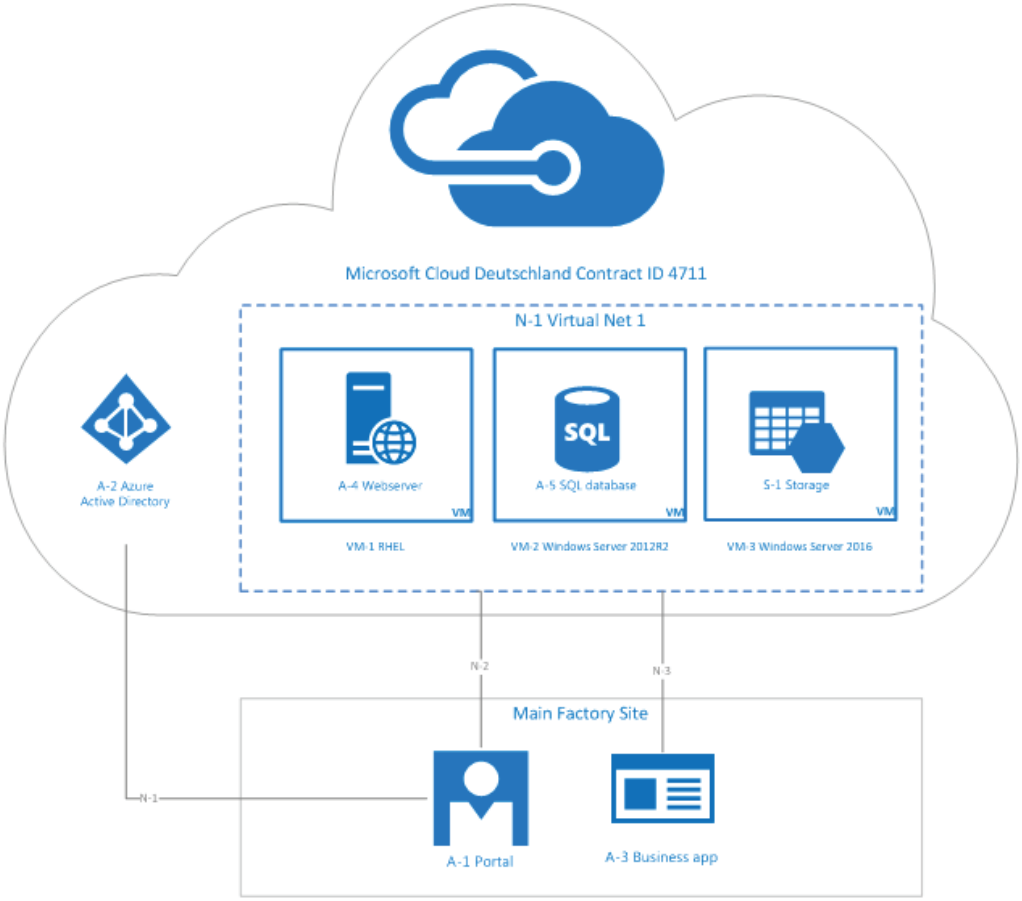

Figure 2: Network plan of IT-Grundschutz Information Domain with Azure SaaS and IaaS Services

2.2.1 Including the Cloud in the Structure Analysis

The IT-Grundschutz Catalogues use a layered approach for modelling safeguards, starting with layer 1 (Common aspects), 3 layers that cover the "physical platform" (layer 2 Infrastructure, layer 3 IT-Systems, and layer 4 Networks) and finally a layer for the applications (layer 5).

The cloud user need only take into account in the application layer (layer 5) when considering the use of cloud services (e.g. an Azure Active Directory subscription). The underlying layers 2 (infrastructure), 3 (platform and systems) and 4 (network) are all administered and controlled by Microsoft, and are not in the control of the cloud user.

The following objects must be considered in the structure analysis by the cloud user for each cloud service:

Layer	Cloud Infrastructure	Virtual Customer Environment IaaS	Virtual Customer Environment SaaS	Virtual Customer Environment PaaS
Layer 1: Common Aspects	Module M 1.17 Cloud Usage	Standard Modelling according to IT-Grundschutz Method	Standard Modelling according to IT-Grundschutz Method	Standard Modelling according to IT-Grundschutz Method
Layer 2: Infrastructure[4]	Not relevant for the Cloud User	Not relevant	Not relevant	Not relevant
Layer 3: IT-Systems	Not relevant for the Cloud User	Standard Modelling according to IT-Grundschutz Method	Not relevant	Not relevant
Layer 4: Networks	Not relevant for the Cloud User	Not relevant for the Cloud User	Not relevant	Not relevant
Layer 5: Applications	Not relevant for the Cloud User	Standard Modelling according to IT-Grundschutz Method	Standard Modelling according to IT-Grundschutz Method	Standard Modelling according to IT-Grundschutz Method

Table 1: Relevant IT-Grundschutz layers for a structure analysis by the cloud user

2.2.2 Determining the Protection Requirements for the Cloud Services

The IT-Grundschutz procedure for determining protection requirements is based on an inheritance model. In this model the protection requirements are first defined for the applications, classifying them regarding generally confidentiality, integrity and availability of the data they process and the business processes they support. The protection requirements will then be inherited by the IT systems the applications are running on and from there by the networks the IT systems are connected to and sites the IT systems are located (e. g. data centers).

For the virtual customer environment the determination of protection requirements is handled according to the standard IT-Grundschutz method. The protection requirements for each cloud service are determined in the same way as for standard infrastructure, whereby each service also inherits the protection requirements of the applications or IT systems running on it.

[4] Note: The layer „Infrastructure" refers to physical security aspects regarding particularly sites (e. g. data centers, office buildings), rooms (e. g. offices, server rooms) or cabelling (e. g. electric or IT cabelling).

2.3 Modelling of Microsoft Cloud Basic Services

The virtual environment within the cloud operated by the customer has to be modelled in the same way as a standard physical or virtual infrastructure would be modelled. This includes virtual servers, virtual networks and the applications. Note that the modelling process must take into account the individual scope, conditions and requirements of the cloud services and infrastructure.

Therefore this paper concentrates on the modelling of the cloud infrastructure as such by using module M 1.17 Cloud Usage of the IT-Grundschutz Catalogues.

The BSI standard requires that this module is to be used "per cloud service", without providing a definition for "cloud service". This can be read as "once per cloud provider", once per service model or even, very fine-grained, once per application. A reasonable solution or interpretation must be reached.

We suggest applying the module at most once per service model and provider, grouping individual Azure Services as they are used in the IT-Grundschutz Information Domain.

For grouping the Azure Services the grouping requirements of the IT-Grundschutz procedure (see BSI Standard 100-2) should be considered.[5] For instance if the same service model would be used for internal applications with greatly varying protection requirements, a more fine-grained approach probably has to be considered.

Microsoft Cloud Germany Basic Service	Service Model
Active Directory	SaaS/PaaS[6]
Azure KeyVault	SaaS/PaaS
Azure Portal	SaaS
Cloud Services	PaaS
Service Fabric	PaaS
SQL DB	SaaS/PaaS
Storage	PaaS
Virtual Machine Scale Sets (VMSS)	IaaS
Virtual Machines	IaaS
Virtual Networks	IaaS

Table 2: Modelling of Microsoft Cloud Germany Basic Services (Ring 0)

[5] Target objects can be assigned to the same group if all object are of the same type, are configured and integrated into a network in the same manner, are subject to the same basic administrative and infrastructural requirements, operate similar applications and have the same protection requirements.

[6] When considering the service models marked SaaS/PaaS, it is custom to consider the actual usage. While these services are highly customizable and can be used as a basis to develop further services, they are often used in the SaaS sense.

3 Implementation Module 1.17 Cloud Usage

The following section describes how all audit-relevant safeguards from Module M 1.17 Cloud Usage[7] can be implemented for Microsoft Cloud Germany. Every safeguard comes with review questions that are intended as a checklist for the safeguard; where applicable, pointers on possible answers are given at the end of each safeguard.

While some of the safeguards can only be fulfilled in an individual manner, many safeguards specify requirements which have common answers for all users of Microsoft Cloud Germany.

The following table gives an overview of the safeguards for which Microsoft can provide supporting information, both regarding implementation details and specific safeguard-related questions.

Safeguard	Supporting information available from Microsoft?	Description
S 2.40 (A) Timely Involvement of Staff/Factory Council	No	This safeguard is organization specific. Microsoft provides a detailed description of each cloud service in order to support the discussion regarding this safeguard.
S 2.42 (A) Determination of Potential Communications Partners	Yes	Microsoft provides supporting information regarding relevant contractual relationships (e.g. "ADV-Vereinbarung") as well as details of the data trustee role of T-Systems Deutschland GmbH.
S 2.534 (A) Determining a Cloud Usage Strategy	Yes	Microsoft has made available the workbook "Enterprise Cloud Strategy" to support users in formulating a cloud usage strategy.
S 2.535 (A) Determining Security Policy for Cloud Usage	Yes	In this chapter the security requirements and procedures of Microsoft Cloud Germany are set out.
S 2.536 (A) Service Definition/Service Templates for Cloud Services	Yes	This safeguard 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.

[7] The Grundschutz catalogue includes safeguards without audit relevance for explanatory purposes (marked as "W") – these are not included in the list.

Safeguard	Supporting information available from Microsoft?	Description
S 2.537 (A) Planning a Secure Migration to a Cloud Service	Yes	Microsoft has made available the workbook "Enterprise Cloud Strategy" to support users in their migration to cloud infrastructure.
S 2.538 (A) Planning a Secure Integration of Cloud Services	No	This safeguard is organization specific, as it covers internal planning for the secure integration of existing services.
S 2.539 (A) Creating a Security Concept for Cloud Services	Yes	While there is no generic template for each specific organization's requirements, Microsoft Cloud Germany addresses most of the technical threats and mitigations mentioned in the safeguard.
S 4.459 (Z) Use of Encryption in Cloud Computing	Yes	Microsoft Cloud Germany 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.
S 4.461 (Z) Portability of Cloud Services	Yes	For each service set out in chapter 2.3 Modelling of Microsoft Cloud Basic Services, the corresponding portability concerns are also addressed.
S 2.540 (A) Considered Selection of a Cloud Service Provider	Yes	See the Microsoft Online Subscription Agreement for a comparision of cloud service providers.
S 2.541 (A) Contractual Agreements with Cloud Service Provider	Yes	Detailed information concerning standard security requirements of Microsoft Cloud Germany is outlined in this safeguard.
S 2.542 (A) Secure Migration to a Cloud Service	Yes	This safeguard is organization specific, covering internal planning for the secure integration of existing services. Microsoft provides tools to assist with migrating current resources to Azure.
S 2.543 (A) Maintaining Information Security in an Operational Cloud Service Environment	Yes	Information is made available concerning the maintainance of a high level of information security, as well as methods by which the user may test the claims set out.
S 2.544 (C) Auditing Cloud Services	Yes	Information and guidance regarding current and past audits and security certifications are provided, including publically available reports and results, such that the customer is not required to carry out their own audit.
S 4.460 (Z) Use of Federated Services	Yes	Federated services are provided through the Microsoft Cloud Germany service Azure Active Directory, and have their own set of security requirements.

Safeguard	Supporting information available from Microsoft?	Description
S 2.307 (A) Well-Ordered Termination of an Outsourcing or Cloud Services Agreement	Yes	Information and guidance regarding termination of a Microsoft Cloud Germany subscription are provided, including cancellation and data deletion policies.
S 6.155 (A) Creation of a Disaster Recovery Plan for a Cloud Service	Yes	The disaster recovery plan must be individually developed for each cloud service. General guidelines are nonetheless provided.
S 6.156 (Z) Implementing User-Side Data Backups	No	This has to be initiated by your organization; either by yourself or by using another, independent service.

3.1 S 2.40 (A) Timely Involvement of Staff/Factory Council

This safeguard requires the consent of the worker's representatives/employee council to all safeguards enabling the monitoring of the behavior or performance of employees.

This safeguard is organization specific. Microsoft provides a detailed description of each cloud service in order to support the discussion regarding this safeguard.

3.2 S 2.42 (A) Determination of Potential Communications Partners

This safeguard aims to ensure complete transparency about all (external) parties that have access to the customers' data. It is required primarily for reasons of data protection, in particular due to the German Federal Data Protection Act (BDSG) and other applicable data privacy regulations (EU, federal states).

The extent of this safeguard depends largely on the kind of data stored in or accessible from the cloud. The customer must have already determined the protection requirements of the data, i.e.:

1. A confidentiality classification of said data.
2. An list of people allowed to receive the information.

Microsoft Cloud Germany offers special commitments for all data stored in Microsoft Cloud Germany through the "data trustee" construct:

- All access to the customer data (excluding access through or by the customer themselves) is controlled by the German data trustee that operates the physical data centers. The data trustee is T-Systems International GmbH (TSI), a Germany-based, world-leading service provider in IT and communication technologies and wholly-owned subsidiary of Deutsche Telekom AG.
- In the event of demands for data from foreign authorities or judicial orders, customer data is protected through the data trustee model. The data trustee (TSI) operates under German law and will

grant third-party access to customer data only after explicit consent from the customer or when otherwise required by German law.
- All access to customer data by Microsoft personnel or any third party is controlled by the data trustee and will only be granted in accordance with German law or as allowed by the customer.
- Allowed external access is limited to the minimum amount necessary to solve the problem at hand.

The authorative list of parties with access to the data can be acquired from the terms outlined in the "Supplement to the Online Services Terms for German Online Services, Amendment ID M370"[8], that is part of the contractual agreement with both Microsoft and the Data Trustee.

There are only two notable situations in which access by Microsoft personnel may occur:

1. When the data trustee grants Microsoft access to resolve immediate operational problems or in needs support to a customer service request to the data trustee. In this case, the access is monitored by the data trustee and limited to the least amount necessary to solve the problem at hand.
2. When customer sends data to Microsoft Customer Support directly (e.g. by email in a support question or by sharing your screen).

In this case, the potential list of entities with access to the data is documented in the Microsoft Services Supplier List.[9]

The above of course only applies to information stored with no external access offered by the customer themselves. When implementing services that allow other forms of access, this list must be extended to include the parties allowed access by the customer.

Review Question	Answer	Reference
Is clear what data may be handled by the various communications partners?	The commissioned data processing contract ("ADV-Vereinbarung"s) with the data trustee limits access to your data to the data trustee and personell as described above. Any further access by other parties has to be allowed by you – and documented accordingly.	Supplement to the Online Services: Terms for German Online Services, Amendment ID M370

[8] German: „Ergänzende Bestimmungen für Onlinedienste für Deutsche Onlinedienste, Zusatzvereinbarung ID M370"

[9] https://www.microsoft.com/en-us/download/details.aspx?id=50426

3.3 S 2.534 (A) Determining a Cloud Usage Strategy

This safeguard considers planning ahead of time how the cloud services are to be used and identifying in advance challenges for the security model.

It covers strategy, interfacing, networking, administration models and data management.

Microsoft has produced a workbook for general support in drawing up a cloud usage strategy, which answers important questions as well as providing experience-based recommendations in the areas of cloud strategy, cloud services models and security considerations.[10]

Note that the scope of planning necessarily depends on the specific requirements of the services ported to or created in the cloud.

When matching your requirements against Microsoft Cloud Germany offerings, see Appendix B and this section to get reference information.

3.4 S 2.535 (A) Determining Security Policy for Cloud Usage

This safeguard ensures the clear definition of security standards regarding cloud usage. It covers two areas: security requirements concerning your own organization, and security requirements concerning the cloud service provider. In order to cover all essential areas, organizational, technical and legal considerations must all be taken into account.

Security Requirements Concerning Your Own Organization
These are requirements that should be implemented by you to protect data and processes in the cloud; e.g. encrypting highly sensitive data before transferring it, creating local backups or creating offline caches for high-availability information. They should be documented in the security concept (see 3.8 S 2.539 (A) Creating a Security Concept for Cloud Services).

Security Requirements Concerning the Cloud Service Provider
These should document the requirements which are to be verified when choosing a cloud service provider. Issues to consider include geographic location, availability guarantees and SLA's, use of third-party personnel and whether other organizational security requirements or certifications are required.

Data Access and Data Protection Issues
Microsoft Cloud Germany offers the following commitments relevant to this safeguard:

- Storage location in Germany
- Access to customer data is controlled by the German Data Trustee operating under German law or by the customer itself.
  The restriction is specifically targeted at allowing access only in accordance with German and EU law (and through German courts) and includes access by Microsoft itself.

[10] https://info.microsoft.com/enterprise-cloud-strategy-ebook.html

- A contract with the German data trustee as a data processor on behalf of the customer (Auftragsdatenverarbeitung) that limits the use of the customer data to purposes necessary to provide the cloud services.

Availability

Availability requirements and service levels offered are dependent upon the service used, but in general Microsoft guarantees 99.5 or 99.9% availability per month with different service credits when they fail to reach that level.

If you should require further assurance, this should be achieved through the use of your own technical measures to provide fallback or replacement services.

Specific Assurances and Compliance

Microsoft Azure has a range of security related certifications for selected services, e.g.:

- ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)
- ISO/IEC 27001 (Information Security Management System)
- PCI-DSS (Payment Card Industry Data Security Standard)
- SOC 1 - SOC 2 - SOC 3 (SSAE16 / ISAE 3402)

Microsoft intends to replicate these certifications for Microsoft Cloud Germany after the date of general availability. Specific controls or requirements can be mapped to the mandatory controls of these standards. For further details see Chapter 4 of this document, Microsoft's Responsibilites as a Cloud Provider.

Other relevant assurances are available from:

- "Supplement to the Online Services: Terms for German Online Services, Amendment ID M370"[11] (terms of commissioned data processing / Vereinbarung zur Auftragsdatenverarbeitung)
- Consolidated Service Level Agreements:
- OnlineSvcsConsolidatedSLA(WW)(English)(June272016)[12]
- Service level agreements for Azure services:
- https://azure.microsoft.com/de-de/support/legal/sla/
- The list of certifications for Microsoft Azure is available at:
- https://www.microsoft.com/de-de/TrustCenter/Compliance?service=Azure#Icons

Review Question	Answer
Does the security policy include concrete, comprehensive security standards for the organization?	The security policy is organization specific (see above, "Security Requirements Concerning your own Organization").
There are any specific security requirements concerning the cloud service provider, and are they well documented?	These are your requirements, but see "Security Requirements Concerning the Cloud Service Provider" for specific assurances by Microsoft Cloud Germany.

[11] German: „Ergänzende Bestimmungen für Onlinedienste für Deutsche Onlinedienste, Zusatzvereinbarung ID M370"

[12] http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37

Review Question	Answer
Are the protection requirements of the cloud services regarding Confidentiality, Integrity and Availability well documented?	These are the requirements of your organisation, but see "Security Requirements Concerning the Cloud Service Provider" for specific assurances from Microsoft Cloud Germany
Are any country-specific requirements relevant to the cloud services (e.g. legal jurisdiction for the service) known and documented?	This explicitly references competing legal frameworks for international providers; this is not an issue here due to the construct of the German data trustee (see section 3.2 "S 2.42 (A) Determination of Potential Communications Partners" for a detailed explanation).

3.5 S 2.536 (A) Service Definition/Service Templates for Cloud Services

This safeguard requires your organization (as the cloud service customer) to define the desired cloud services in terms of business impact and suggests using a standardized ITIL style service template for this purpose.

This safeguard is organization specific, since its purpose is to document internal requirements and necessary protections in a format that allows a comparison of cloud providers.

Still, this safeguard mentions additional practical requirements for which information is available:

Compliance Requirement	Implementation on Microsoft Cloud Germany	Reference
Secure authentication methods, 2-factor authentication for administration	Role-based access control is available for controlling cloud services via the Azure Portal. For a secure, wide-ranging identity- and access management system, Microsoft offers different Active Directory Service options, depending on requirement (Azure Active Directory, Azure Active Directory B2C). A subscription to Microsoft cloud service Multi-Factor Authentication allows the use of multi-factor authentication.	https://azure.microsoft.com/de-de/features/azure-portal/ https://azure.microsoft.com/de-de/services/multi-factor-authentication/ https://azure.microsoft.com/de-de/services/active-directory/ https://azure.microsoft.com/de-de/services/active-directory-b2c/

Compliance Requirement	Implementation on Microsoft Cloud Germany	Reference
Encryption requirements	Microsoft Cloud Germany offers encryption in conjunction with a variety of cloud services. The Cloud Service Virtual Network allows the construction of a secure, isolated environment with a dedicated DNS server. A secure connection can be established using either an IPSec VPN or the ExpressRoute cloud service.	(M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx[13] https://www.microsoft.com/de-de/TrustCenter/Security/Encryption https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/ https://blogs.msdn.microsoft.com/azuresecurity/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/ https://azure.microsoft.com/de-de/services/virtual-network/ https://azure.microsoft.com/de-de/services/expressroute/
Client software interoperability	Developer Tools and SDKs are available for a variety of programming languages and platforms, simplifying integration and development and the administration of Microsoft Cloud Germany service subscriptions.	https://azure.microsoft.com/de-de/tools/

3.6 S 2.537 (A) Planning a Secure Migration to a Cloud Service

The transition to using cloud services requires careful conception and planning, which must been seen as part of the overall security concept.

The organizational rules, responsibilities and processes surrounding the migration and suitable test and handover procedures are to be determined as part of this safeguard, along with an assessment of the implementation of any prior agreements. Both the remaining on-premise IT infrastructure and current working processes must be reviewed to see if alterations are necessary for adapting to the use of cloud services.

Microsoft offers a comprehensive workbook[14] to support you in migration planning. The workbook combines answers to important questions and experience based recommendations concerning a migration to

[13] German: „Ergänzende Bestimmungen für Onlinedienste für Deutsche Onlinedienste, Zusatzvereinbarung ID M370"

[14] https://info.microsoft.com/enterprise-cloud-strategy-ebook.html

the cloud. An additional workbook covering the migration of SQL Server databases is also available.[15]

3.7 S 2.538 (A) Planning a Secure Integration of Cloud Services

This safeguard aims to ensure that any changes necessary for the adoption of cloud services are identified ahead of time and planned accordingly.

- Interface Systems (load balancers, proxies, routers, secure gateways etc.):
  - Existing systems must provide suitable interoperability, efficiency, performance and throughput as well as an acceptable level of redundancy for the use of the cloud service. Alternatively, new systems may be procured.
  - If an API is used to connect, further security safeguards (M 5.24 Web-Service) may be applicable.
- Network Connection:
  The network connection for using the cloud service must provide sufficient bandwidth to fulfil the requirements of the service. Redundant connections or other additional measures may be appropriate or even required, dependent on the protection requirements of the system.
- Administration:
  For the administration and usage of the cloud service, a role-based permissions model must be applied or newly created.
- Data Management:
  An appropriate backup and data retention strategy must be developed for the data stored in the cloud.

This safeguard is organization specific, as it covers internal planning for the secure integration of existing services.

3.8 S 2.539 (A) Creating a Security Concept for Cloud Services

This safeguard involves creating a security concept for each specific cloud service, including all the security safeguards required for its use. These safeguards are developed from the requirements of the security policy for the cloud service. Additionally, the security concept lays out the particular configuration (cloud user, cloud service provider, internet service provider, etc.) and threat model, which the concrete safeguards are developed in response to.

While there is no generic template for your organizations requirements, Microsoft Cloud Germany addresses most of the technical threats and mitigations mentioned in the safeguard:

[15] https://blogs.msdn.microsoft.com/microsoft_press/2016/05/11/free-ebook-microsoft-azure-essentials-migrating-sql-server-databases-to-azure/

Threat	Mitigation available	Reference
Lack of portability Use of proprietary data formats	Many services on Azure have an equivalent on-premises Setup; most of them use standard formats. E.g.: - Azure Virtual Machines are portable back to Hyper-V - Azure SQL services can be migrated back to a Microsoft SQL-Server	https://blogs.technet.microsoft.com/cbernier/2014/01/27/move-vms-between-hyper-v-and-windows-azure/ https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/
Difficult to determine where data is physically stored	Microsoft Cloud Germany Data is only stored in German data centers	See 3.2 S 2.42 (A) Determination of Potential Communications Partners
Unauthorized access by third parties	Data Trustee model	See 3.4 S 2.535 (A) Determining Security Policy for Cloud Usage
Supervision of service delivery	SLA monitoring through „Service health" module in the portal application	https://azure.microsoft.com/de-de/documentation/articles/insights-how-to-customize-monitoring/ https://azure.microsoft.com/de-de/features/azure-portal/ https://azure.microsoft.com/de-de/status/
Unauthorized access by third parties	Data-at-rest-encryption is available as an option	See 3.9 S 4.459 (Z) Use of Encryption in Cloud Computing
Unauthorized access by third parties	Data-in-transit-encryption	See 3.9 S 4.459 (Z) Use of Encryption in Cloud Computing
Isolation	The environment of each cloud user is isolated from the others. The corresponding technologies and processes (e.g. Hypervisor isolation, root OS, guest VMs and network isolation) depend on the individual cloud service.	https://azure.microsoft.com/de-de/blog/new-windows-azure-security-overview-white-paper-now-available/ https://azure.microsoft.com/de-de/blog/microsoft-azure-network-security-whitepaper-version-3-is-now-available/

Review Question	Answer
Has the network provider produced a security concept in accordance with the appropriate guidelines and standards?	Microsoft Cloud Germany's security concept fulfills a variety of security standards. Further information is given in Section 3.1.4 S 2.535 (A), Determining Security Policy for Cloud Usage.

Review Question	Answer
Is the existence and implementation of the security concept checked by either the cloud service provider or an independent third party?	Microsoft Azure and Microsoft Cloud Germany are continually audited, due to the requirements of multiple compliance standards and certifications. Information and guidance regarding current and past audits and security certifications are provided, including publically available reports and results.

3.9 S 4.459 (Z) Use of Encryption in Cloud Computing

This additional safeguard for enhanced protection requirements strives to ensure that, where required, suitable encryption is used to secure data, both in transit and at rest. Dependent on the method of encryption, the responsibility may lie either with the customer or with the cloud service provider. If the cloud service provider is responsible for the encryption, then the encryption service provided should be checked against the standards set out in the service definition.

Microsoft Cloud Germany already employs encryption as standard in a number of different areas. The cloud user has the option to enable encryption, dependent on the chosen cloud service, using standard or individual encryption technologies.[16]

Review Question	Answer	Reference
If encryption is carried out by the cloud provider, do contractual terms exist mandating the use of secure ciphers with appropiately long keys?	Microsoft offers encryption in conjunction with a number of cloud services. For example, Azure Storage includes the Azure Storage Service Encrytion (SSE) feature, which encrypts data as they are saved to the cloud storage device. Using the Key Vault, it is also possible to encrypt the virtual hard drives of cloud-based Windows and Linux virtual machines.	https://www.microsoft.com/de-de/TrustCenter/Security/Encryption https://azure.microsoft.com/de-de/services/key-vault/ https://azure.microsoft.com/de-de/documentation/articles/storage-security-guide/ https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/ https://blogs.msdn.microsoft.com/azuresecurity/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/ https://azure.microsoft.com/de-de/services/key-vault/ https://azure.microsoft.com/de-de/documentation/articles/expressroute-introduction/ https://azure.microsoft.com/de-de/services/virtual-machines/security/

[16] https://www.microsoft.com/de-de/TrustCenter/Security/Encryption

Review Question	Answer	Reference
If managing your own encryption, is there a suitable key management system in place?	This requirement is the responsibility of the cloud user. Microsoft Azure offers secure key management and storage for other cloud services with the Key Vault cloud service.	https://azure.microsoft.com/de-de/services/key-vault/
Are the particular characteristics of the cloud service model taken into account when employing encryption?	This requirement is the responsibility of the cloud user. The employed encryption should be helpful against the assumed attack scenarios – e.g. encrypting data-at-rest for a database does not help against online attacks using SQL injection.	

3.10 S 4.461 (Z) Portability of Cloud Services

This additional safeguard aims to ensure a high degree of flexibility when changing cloud service provider 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 interopability and portability . The Cloud Service API Management and the cloud services make use of standard formats and offer a number of different connection methods.

Further portability considerations are listed in the table below.

Cloud service	Portability	Reference
Azure Active Directory	Using Azure Active Directory enables the use of Single-Sign-On across thousands of cloud SaaS applications. With Azure AD Connect, local profiles can be integrated into Azure Active Directory and synchronized across the cloud.	https://azure.microsoft.com/de-de/services/active-directory/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-whatis/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-aadconnect/
Azure KeyVault	Key Vault is a cloud service for secure secrets management on Microsoft Cloud Germany. Portability is not provided for.	https://azure.microsoft.com/de-de/services/key-vault/

Cloud service	Portability	Reference
Azure Portal	Azure Portal is a web application provided by Microsoft. There are no portability considerations.	https://azure.microsoft.com/de-de/features/azure-portal/
Cloud Services	Cloud Services is a platform for developing and deploying your own cloud services and applications. There are no portability considerations.	https://azure.microsoft.com/de-de/services/cloud-services/
Service Fabric	Service Fabric is a platform for developing and deploying microservice-based applications and managing their life cycles. There are no portability considerations.	https://azure.microsoft.com/de-de/services/service-fabric/
SQL DB	The Azure SQL Databases can be copied and simply deployed in other environments.	https://azure.microsoft.com/de-de/services/sql-database/ https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/
Storage	Azure Storage allows the customer to import and export data.	https://azure.microsoft.com/de-de/services/storage/ https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/#wann-sollte-der-importexport-dienst-von-azure-verwendet-werden
Virtual Machine Scale Sets (VMSS)	VMSS is a cloud service for scaling virtual machines in Microsoft Cloud Germany. Portability is not provided for.	https://azure.microsoft.com/de-de/services/virtual-machine-scale-sets/
Virtual Machines	Microsoft offers the readiness assessment tool, which checks physical or virtual environments and prepares a comprehensive report with the required steps for a migration to Microsoft Cloud Germany. Additionally, Microsoft offers the Virtual Machine Optimization Assessment Tool, for optimizing the performance of VMs (e.g. after migration to the cloud)	https://azure.microsoft.com/de-de/services/virtual-machines/ https://azure.microsoft.com/de-de/downloads/vm-readiness-assessment/ https://azure.microsoft.com/de-de/downloads/vm-optimization-assessment/
Virtual Networks	Azure Virtual Network offers an isolated, secure environment for virtual machines and applications. There are no portability considerations.	https://azure.microsoft.com/de-de/services/virtual-network/

Review Question	Answer	Reference
Were all important requirements for a move to another provider or back to on-premises well defined?	This requirement is the responsibility of the cloud user.	
Is it possible to carry out portability tests?	This requirement is the responsibility of the cloud user. Microsoft offers the readiness assessment tool, which checks physical or virtual environments and prepares a comprehensive report with the required steps for a migration to Microsoft Cloud Germany.	https://azure.microsoft.com/de-de/downloads/vm-readiness-assessment/
Are portability guidelines or standards included in the contractual arrangement with the cloud service provider?	Portability is not set out contractually, however Microsoft has made a number of provisions. For example, Storage Data can be imported and exported and SQL databases can be copied and imported into other environments. Furthermore, APIs can be used, which may be managed using Azure Powershell or the cloud service API Management.	https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/#wann-sollte-der-importexport-dienst-von-azure-verwendet-werden https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/ https://azure.microsoft.com/de-de/documentation/articles/powershell-install-configure/ https://azure.microsoft.com/de-de/services/api-management/

3.11 S 2.540 (A) Considered Selection of a Cloud Service Provider

The aim of this safeguard is to ensure the selection of a suitable cloud service provider.For a detailed and thorough comparison, a detailed requirements document should be drawn up. This document must precisely outline what is expected and required from the cloud service, including a description of the security concept and security policies. A requirements analysis carried out beforehand may be useful in drawing up the document.

Starting from the defined requirements, a service catalog or a requirement specification can be created. This catalogcan then be used to compare the competing cloud service providers and rate them using a points matrix. Finally, a cost-benefit analysis should be carried out to compare the remaining offers and to provide a realistic assessment of the potential cost savings from moving to a cloud service model.

The basic aspects listed in the table below must be investigated and appropriate answers obtained before the offers are evaluated. If the results are not satisfactory, a cloud provider may be removed from further consideration.[18]

Review Question	Answer	Reference
Was a detailed requirements profile (corresponding to the service definition) developed for the cloud service provider?	This requirement is the responsibility of the cloud user.	
Does a service description or a product specification exist, allowing comparing and constrasting of the offers from a variety of cloud service providers?	This requirement is the responsibility of the cloud user.	
Do additional or external sources (e.g. Market analyses, contractual rules or choice of location) influence the standing of each prospective service provider?	This requirement is the responsibility of the cloud user.	
Have the available service descriptions (SLAs and/or general terms of business) been checked in detail, and any clarifications requested?	This requirement is the responsibility of the cloud user. The relevant agreements are the Microsoft Online Subscription Agreement as well as the SLAs of each cloud service.	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/

3.12 S 2.541 (A) Contractual Agreements with Cloud Service Provider

This safeguard ensures that contractual agreements are appropriate in type, scope and level of detail for the protection requirements of the data and the applications.

The previously defined requirements must be considered, and at least the following points require an answer with respect to Microsoft Cloud Germany.

[18] Further aspects and assistance in choosing a cloud service provider is available from Microsoft at https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/

Contract documents	Microsoft Cloud Germany	Reference
Physical location of the services and Cloud Service Provider	The cloud services are run from data centres located in Germany. All processing of customer data by the data trustee takes place inside of Germany.	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx (M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx
Subcontractors and third parties involved with service delivery	Microsoft employs subcontractors for specific, limited support tasks. A german data trustee is entrusted with controlling all acces to customer data.	https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426
Rules governing the infrastructure of the Cloud Service Provider	The data centres used for Microsoft Cloud Germany are located (for redundancy) in Frankfurt am Main and Magdeburg. They are connected over a private network over which data is continuously exchanged. The implementation of a multiclient infrastructure follows compliance standards fulfilled by in Europe by Microsoft Azure.	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx
Rules concerning the personnel of the Cloud Service Provider	The personnel (both internal and external) employed by Microsoft Cloud Germany have all required competencies and are cleared in accordance with internal policies.	Internal Paper: HR Policy Microsoft Azure Standard Operating Procedure: Personnel Screening (SOP ID: 21)
Rules concerning processes, working procedures and responsibilities	A comprehensive set of rules, including information security policies (e.g. re asset management, malware protection) underlies Microsoft Cloud Germany.	Several Microsoft Azure Standard Operating Procedures
Provisions for ending the contractual agreement	Every cloud service is offered on a subscription basis, with cancellation possible at any time. (Additional options for term commitments at discounted pricing are available, but optional.)	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/
Ensuring secure deletion of data by the Cloud Service Provider	Customer data is deleted within 180 days of cancelling the service. Physical storage media will be securely destructed on-site at the end of their service life. The customer is additionally able to ensure the secure deletion of their data by encrypting data stored in the cloud using the encryption offered by Microsoft Cloud Germany.	(M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx https://www.microsoft.com/de-de/TrustCenter/Security/Encryption Internal Paper: On-Site Data Bearing Device Destruction Procedure

Contract documents	Microsoft Cloud Germany	Reference
Rules concerning access rights	Access to customer data is primarily reserved for the customer themselves. Only for support and maintenance purposes, with continuous monitoring by the data trustee, are Microsoft support personnel permitted to access stored customer data. The personnel (both internal and external) employed by Microsoft Cloud Germany have all required competencies and are cleared in accordance with internal policies.	(M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx Microsoft Sovereign Cloud - Compliance in the cloud for German business organizations Internal Paper: HR Policy; Microsoft Azure Standard Operating Procedure: Personnel Screening (SOP ID: 21)
Provisions for critical or emergency scenarios	Microsoft Cloud Germany has set out rules for continuation of services to the level set out by the SLA. Corresponding measures include the geographical separation of the data centres and the continuous replication of data between them. The customer may also choose to meet any further requirements through the use of Microsoft Cloud Germany services such as Backup or Site Recovery.	Internal Paper: Business Continuity and Disaster Recovery (SOP ID: 20) https://www.microsoft.com/de-de/cloud/deutschland/default.aspx https://azure.microsoft.com/de-de/services/backup/ https://azure.microsoft.com/de-de/services/site-recovery/
Provisions regarding legal requirements	Microsoft complies with all laws and rules concerning its provision of the cloud services. The data trustee also complies with all laws relating to its role in the provision of the cloud services. Further rules and guidelines are set out in the internal policy document "Legal and Regulatory Compliance".	MicrosoftOnlineServicesTerms(English)(July2016) Microsoft Azure Standard Operating Procedure: Legal and Regulatory Compliance (SOP ID: 11)
Definition of change management and test processes.	Change management and test policies are defined in an internal policy document.	Microsoft Azure Standard Operating Procedure: Hardware Change and Release Management (SOP ID: 24) Microsoft Azure Standard Operating Procedure: Secure Development Lifecycle (SDL) (SOP ID: 15)

Contract documents	Microsoft Cloud Germany	Reference
Rules governing checks and audits.	Microsoft Cloud Germany offers customers the ability to monitor SLA compliance with the "Service Health" module in the Azure Portal. Cloud users have the ability to carry out penetration tests against their cloud services, given prior agreement. The monitoring of Microsoft Cloud Germany is governed by a number of internal rules. Successful and unsuccessful attempts to access customer data as well as changes to data are logged and the logs stored for a year. System logs are deleted after 90 days. Microsoft Azure and Microsoft Cloud Germany are also continually audited, due to the requirements of multiple compliance standards and certificationsInformation and guidance regarding current and past audits and security certifications are provided, including publically available reports and results.	https://security-forms.azure.com/penetration-testing/terms Microsoft Azure Standard Operating Procedure: Logging and Monitoring (SOP ID: 12) Microsoft Azure Standard Operating Procedure: Penetration Testing (SOP ID: 23) https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx https://trustportal.office.com/
Consideration of special requirements	In Microsoft Cloud Germany the cloud user has the option of making backups through a cloud service such as Azure Backup. Data can also be imported and exported. This is in addition to the portability provisions of each cloud service.	https://azure.microsoft.com/de-de/services/backup/ https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/ 3.10 S 4.461 (Z) Portability of Cloud Services

Review Question	Answer	Reference
Are the contractual agreements appropriate in type, scope and level of detail for the protection requirements of the data and the applications connected with the cloud service usage?	A process exists for Microsoft Cloud Germany allowing all customer data which may be stored in the cloud to be classified according to sensitivity and have the appropriate protective measures applied to it. The procedure also ensures that Microsoft service personnel may not access customer data without prior customer permission and authorization and monitoring by the data trustee.	Internal Paper: Asset Management (SOP ID: 03); Asset Classification and Protection Matrix (Azure) (M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx

Review Question	Answer	Reference
What, if any, rules govern the physical location of the cloud service provision?	The cloud services are run from data centres located in Germany. All processing of customer data by the data trustee takes place inside of Germany.	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx (M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx
Have clear responsibilities, escalation stages and communication paths been set out between the contracting institution and the cloud service provider?	Microsoft Cloud Germany users have access to account management and billing support, as well as support and guidance offered in the Azure Portal. Technical support can be requested via the Azure Portal on the purchase of a corresponding support package.	https://azure.microsoft.com/de-de/support/options/ https://azure.microsoft.com/de-de/support/faq/ https://azure.microsoft.com/de-de/support/plans/
Do agreements covering the secure deletion of data by the cloud service provider exist?	Customer data is deleted within 180 days of cancelling the service. The customer is able to ensure the secure deletion of their data by encrypting data stored in the cloud using the encryption offered by Microsoft Cloud Germany.	(M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx https://www.microsoft.com/de-de/TrustCenter/Security/Encryption https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/ https://blogs.msdn.microsoft.com/azuresecurity/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/
Do written rules exist regarding cancellation and service termination?	Every cloud service is offered on a subscription basis, with cancellation possible at any time. (Additional options for term commitments at discounted pricing are available, but optional)	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/

3.13 S 2.542 (A) Secure Migration to a Cloud Service

This safeguard looks at the actual migration to the cloud service according to the considerations given in the migration security concept 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.

This safeguard is organization specific, as it covers internal planning for the secure integration of existing services. Microsoft provides tools to assist with migrating current resources to Azure.[19]

3.14 S 2.543 (A) Maintaining Information Security in an Operational Cloud Service Environment

The aim of this safeguard is to maintain a comparable or enhanced level of information security after a migration to a cloud service. Accordingly, guidelines and documentation should be kept up to date and conformance with standards should be regularly checked, both on the side of the cloud user as well as the cloud service provider.

Review Question	Answer	Reference
Are the policy documents and service documentation regularly updated?	This requirement is the responsibility of the cloud user.	
Is the provision of the service regularly checked or audited?	This requirement is the responsibility of the cloud user. Microsoft Cloud Germany includes an integrated SLA Monitoring system ("Service Health"), over which the compliance of the services can be checked.	https://azure.microsoft.com/de-de/documentation/articles/insights-how-to-customize-monitoring/ https://azure.microsoft.com/de-de/features/azure-portal/ https://azure.microsoft.com/de-de/status/
Were security verifications or checks carried out by the service provider?	This requirement is the responsibility of the cloud user. Microsoft Cloud Germany offers in this respect a variety of publications and verifications as well as applicable certifications. This can be verified by a user of Microsoft Cloud Germany on the public website as well as in the form of an audit which can be viewed in the Service Trust Portal.	https://www.microsoft.com/de-de/TrustCenter/STP/default.aspx https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx https://trustportal.office.com/
Has the contracting institution been in regular contact with the cloud service provider?	Microsoft Cloud Germany offers a variety of support options. Cloud users will be contacted in the event of significant service disruption.	

[19] https://azure.microsoft.com/de-de/downloads/

Review Question	Answer	Reference
Are exercises and tests carried out to practice responding to system failures?	This requirement is the responsibility of the cloud user. Microsoft Cloud Germany has set out rules for continuation of services to the level set out by the SLA.	Internal Paper: Business Continuity and Disaster Recovery (SOP ID: 20)

3.15 S 2.544 (C) Auditing Cloud Services

This safeguard looks to ensure both that the cloud user satisfies her auditing requirements and also that agreements are being upheld on both sides. This may be achieved through, for instance, on-site audits or specific questionnaires, independent of the cloud service model.

Microsoft Azure and Microsoft Cloud Germany are continually audited, due to the requirements of multiple compliance standards and certifications. The list of compliance standards for Microsoft Azure includes ISO/IEC 27018, ISO/IEC 27001, PCI-DSS, and SOC 1/2/3 (see section 4 for more details). These audits are conducted accredited audit firms. Additonal internal audits are conducted by Microsoft.Information about these audits is available online through the Microsoft Trust Center. In addition, contracted enterprise and government customers can opt in to the Service Trust Portal (STP), which provides direct access to many of the compliance reports and attestations.

Microsoft intends to cover all audit requirements arising from IT-Grundschutz with independent third party-audits.
Penetration testing directly by the cloud customer is possible given advance notice and adherence to band-with limits.

Review Question	Answer	Reference
Has the institution contractually ensured the right to carry out audits?	Microsoft Azure and Microsoft Cloud Germany are continually audited, due to the requirements of multiple compliance standards and certifications.	https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx https://trustportal.office.com/
Is the implementation of security measures inspected by audits or by answering questionnaires? Are the particulars of the IaaS, PaaS and SaaS models taken into account during audits?	Information and guidance regarding current and past audits and security certifications are provided, including publically available reports and results, such that the customer is not required to carry out their own audit.Enterprise customers can get direct access to most compliance reports throught the Service Trust Portal (STP).	https://www.microsoft.com/de-de/TrustCenter/STP/default.aspx https://security-forms.azure.com/penetration-testing/terms

3.16 S 4.460 (Z) Use of Federated Services

This additional safeguard for enhanced protection requirements considers the security requirements of federated cloud services. 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 security measure is to ensure that only the minimum necessary information is sent in the SAML[20] ticket to the cloud service provider. Additionally, user rights and roles must be regularly checked to ensure that only authorized users have access.

Microsoft Cloud Germany offers federated services through Azure Active Directory.

Review Question	Answer	Reference
Is only the required information sent in the SAML Ticket to the cloud service provider?	This requirement is the responsibility of the cloud user. Microsoft offers federated services with Azure Active Directory, which supports the SAML 2.0 protocol as well as WS-Federation and OpenID Connect. The information contained in the SAML tickets can be configured according to your requirements or the requirements of each application.	https://azure.microsoft.com/de-de/services/active-directory/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-single-sign-on-protocol-reference/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-saas-custom-apps/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-saml-claims-customization/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-token-and-claims/
Are user rights regularly checked and can it be ensured, that a SAML ticket can only be granted to authorized users?	This requirement is the responsibility of the cloud user.	

[20] SAML (Security Assertion Markup Language) is a standard authentication and authorization protocol

3.17 S 2.307 (A) Well-Ordered Termination of an Outsourcing or Cloud Services Agreement

This safeguard aims to make clear that a move to either another cloud service provider or back to a classic 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.
Microsoft Cloud Germany, in order to protect customer data, has contracted T-Systems International GmbH to act as a data trustee. Customer data will be deleted at most 180 days after the end of the agreed usage period or the cancellation of the user agreement[21].

Review Question	Answer	Reference
Does the contract with the cloud service provider set out comprehensive terms regarding termination of the service provision?	Every cloud service is offered on a subscription basis, with cancellation possible at any time. (Additional options for term commitments at discounted pricing are available, but optional.)	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/
Can it be ensured that a termination of the cloud service agreement does not unduly damage the contracting party?	This requirement is the responsibility of the cloud user.	

3.18 S 6.155 (A) Creation of a Disaster Recovery Plan for a Cloud Service

This safeguard looks to secure cloud usage through the creation of a disaster recovery plan. This must include all technical and organizational aspects for Business Continuity Management.

The disaster recovery plan must be individually developed for each cloud service. Disaster recovery must be addressed during the development process for Microsoft Cloud Germany applications.[22] To aid with the process Microsoft Cloud Germany offers data recovery within the cloud via the Site Recovery cloud service.[23] If futher protection is required, the Hybrid Cloud Platform product Microsoft Azure Stack can be used to assist with data recovery.[24]

[21] (M370)EnrAmend(Supplement to German Online Service)ENG)(May2016)(CR).docx

[22] https://azure.microsoft.com/de-de/documentation/articles/resiliency-disaster-recovery-high-availability-azure-applications/

[23] https://azure.microsoft.com/de-de/services/site-recovery/

[24] https://azure.microsoft.com/de-de/overview/azure-stack/

3.19 S 6.156 (Z) Implementing User-Side Data Backups

This additional safeguard for higher protection requirements aims to ensure data availability when access to the cloud services is lost or the cloud services themselves are unavailable.

This has to be initiated by your organization; either by yourself or by using another, independent service. If an external provider is decided upon, the customer must ensure that all the requirements for backup and data security are fulfilled.

4 MICROSOFT's responsibilities as a Cloud Service Provider

Microsoft is responsible for the security of the cloud below the virtualization layer, with acces to customer data controlled by the Data Trustee T-Systems. 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 for Azure.

The most important of these are:

- ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)
- ISO/IEC 27001 (Information Security Management System)
- PCI-DSS (Payment Card Industry Data Security Standard)
- SOC 1 - SOC 2 - SOC 3 (SSAE16 / ISAE 3402)

These certifications will be replicated for Microsoft Cloud Germany after the date of general availability. Specific assurances can be mapped to the mandatory controls of these standards.

Furthermore the feasibility of an "ISO 27001 certification based on IT-Grundschutz" for Microsoft Cloud Germany is currently being analysed.[25] Such a certification will greatly ease the cloud customer's certification, but is not required.

Cloud Service Provider security can also be checked against the Cloud Computing Compliance Controls Catalogue (C5) from the BSI. This sets out the requirements a cloud service provider must fufil, or at least the minimum standards to be required of a service provider.[26] In addition to the C5 Requirements Catalog, requirements and recommendations from the standards ISO/IEC 27001:2013, CSA Cloud Controls Matrix 3.01, AICPA - Trust Services Principles Criteria 2014, ANSSI Référentiel Secure Cloud 2.0 (Draft), IDW ERS FAIT 5 04.11.2014, BSI IT-Grundschutz 14. EL 2014 and BSI SaaS Sicherheitsprofile 2014 are also referred to. A feasibility study regarding certification according to these standards is currently being carried out.

To aid in security audits, a second part of this paper will outline how the existing security controls and certifications of Microsoft Cloud Germany can be mapped to IT-Grundschutz.

[25] https://www.microsoft.com/de-de/cloud/deutschland/default.aspx

[26] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

Glossary of IT-Grundschutz terms

Apendix A

English term	German term	Description
Safeguard	Maßnahme	Standard security safeguard in IT-Grundschutz. A literal translation would be "measure"; often used synonymously with "control".
Information Domain	Informationsverbund	This term refers to the everything that falls under the IT-Grundschutz protection, i.e. all organisational and technical systems and processes to be modelled and matched with their appropriate safeguards. This may refer to the entire organization or only a subset thereof, or even an individual process.
Modelling	Modellierung	Analyzing a system or process to determine the possible vulnerabilities and the required protective safeguards.
Module	Baustein	Modules describe a specific item or process and draw together the relevant threats and applicable safeguards.
M 1.17 Cloud Usage	B 1.17 Cloud-Nutzung	Translations for the module 1.17 Cloud Services are inofficial; the module has been added only after the last available official English translation; most of the safeguards are also new and have no official translation.
IT-Grundschutz catalogues	IT-Grundschutz-Kataloge	Official body of standard threats and security safeguards in IT-Grundschutz methodology.
(IT) Security Concept	Sicherheitskonzeption	"IT Security Concept" always 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.

References to further information

Apendix B

Topic	Information Pointer
Legal information	https://azure.microsoft.com/de-de/support/legal/
	http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37
	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/
Azure Services, tools and further information	https://info.microsoft.com/enterprise-cloud-strategy-ebook.html
	https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/
	https://azure.microsoft.com/de-de/services/
	https://azure.microsoft.com/de-de/features/azure-portal/
	https://azure.microsoft.com/de-de/services/active-directory/
	https://azure.microsoft.com/de-de/services/active-directory-b2c/
	https://azure.microsoft.com/de-de/services/virtual-network/
	https://azure.microsoft.com/de-de/services/expressroute/
	https://azure.microsoft.com/de-de/services/virtual-machine-scale-sets/
	https://azure.microsoft.com/de-de/services/virtual-machines/
	https://azure.microsoft.com/de-de/services/api-management/
	https://azure.microsoft.com/de-de/services/backup/
	https://azure.microsoft.com/de-de/services/site-recovery/
	https://azure.microsoft.com/de-de/services/cloud-services/
	https://azure.microsoft.com/de-de/services/service-fabric/
	https://azure.microsoft.com/de-de/services/sql-database/
	https://azure.microsoft.com/de-de/services/storage/
	https://azure.microsoft.com/de-de/services/key-vault/
	https://azure.microsoft.com/de-de/tools/
	https://blogs.technet.microsoft.com/cbernier/2014/01/27/move-vms-between-hyper-v-and-windows-azure/

Topic	Information Pointer
	https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/
	https://azure.microsoft.com/de-de/documentation/articles/insights-how-to-customize-monitoring/
	https://azure.microsoft.com/de-de/status/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-whatis/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-aadconnect/
	https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/#wann-sollte-der-importexport-dienst-von-azure-verwendet-werden
	https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/
	https://azure.microsoft.com/de-de/downloads/vm-readiness-assessment/
	https://azure.microsoft.com/de-de/downloads/vm-optimization-assessment/
	https://azure.microsoft.com/de-de/documentation/articles/powershell-install-configure/
	https://azure.microsoft.com/de-de/support/options/
	https://azure.microsoft.com/de-de/support/faq/
	https://azure.microsoft.com/de-de/support/plans/
	https://azure.microsoft.com/de-de/overview/azure-stack/
Security Aspects Microsoft Cloud Germany	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx
Security Aspects Azure	https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx
	https://www.microsoft.com/de-de/TrustCenter/Security/AzureSecurity
	https://trustportal.office.com/
	https://security-forms.azure.com/penetration-testing/terms
	https://www.microsoft.com/de-de/TrustCenter/STP/default.aspx
	https://azure.microsoft.com/de-de/services/multi-factor-authentication/
	https://www.microsoft.com/de-de/TrustCenter/Security/Encryption
	https://azure.microsoft.com/de-de/documentation/articles/storage-security-guide/
	https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/

Topic	Information Pointer
	https://blogs.msdn.microsoft.com/azuresecurity/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/
	https://azure.microsoft.com/de-de/blog/new-windows-azure-security-overview-white-paper-now-available/
	https://azure.microsoft.com/de-de/blog/microsoft-azure-network-security-whitepaper-version-3-is-now-available/
	https://azure.microsoft.com/de-de/services/virtual-machines/security/
	https://gallery.technet.microsoft.com/Azure-Responses-to-CSA-46034a11
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-single-sign-on-protocol-reference/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-saas-custom-apps/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-saml-claims-customization/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-token-and-claims/
	https://azure.microsoft.com/de-de/documentation/articles/resiliency-disaster-recovery-high-availability-azure-applications/
Microsoft Services Supplier List	https://www.microsoft.com/en-us/download/details.aspx?id=50426
BSI	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html;jsessionid=F6BE71C1337EB6140D7D0952EA479087.2_cid368
	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html;jsessionid=F6BE71C1337EB6140D7D0952EA479087.2_cid368
	https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

Enno Ewers, Matthias Pohl
Phone +49 30 533289-0
ewers@hisolutions.com
pohl@hisolutions.com

HiSolutions AG
Bouchéstraße 12
12435 Berlin

info@hisolutions.com
www.hisolutions.com
Fon +49 30 533 289-0
Fax + 49 30 533 289-900

HiSolutions AG
Branch Office
Frankfurt am Main
Mainzer Landstraße 50
60325 Frankfurt am Main

Phone +49 30 533 289-0
Fax + 49 30 533 289-900

HiSolutions AG
Branch Office
Köln
Theodor-Heuss-Ring 23
50688 Köln

Phone +49 221 77 109-550
Fax + 49 30 533 289-900

HiSolutions AG
Branch Office
München
Landsberger Str. 302
80687 München

Phone +49 89 904 05-160
Fax + 49 30 533 289-900