

# IT-Grundschutz Compliance on Office 365

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 Office 365 ..... 8
- 3 Implementation of Module OPS.2.2 Cloud Usage ..... 10
  - 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 ..... 22
  - 3.5 OPS.2.2.A5 Planning the Secure Migration to a Cloud Service ..... 23
  - 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 ..... 24
  - 3.8 OPS.2.2.A8 Careful Selection of a Cloud Service Provider ..... 26
  - 3.9 OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider ..... 29
  - 3.10 OPS.2.2.A10 Secure Migration to a Cloud Service ..... 34
  - 3.11 OPS.2.2.A11 Drawing Up a Contingency Concept for 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 In-House Backups ..... 39
  - 3.17 OPS.2.2.A17 Use of Encryption When Using the Cloud ..... 40
  - 3.18 OPS.2.2.A18 Use of Federation Services ..... 42
  - 3.19 OPS.2.2.A19 Security Vetting of Employees ..... 43
- 4 Implementation of Minimum Standard for the Use of External Cloud Services ..... 45
  - 4.1 NCD.2.1.01 Strategy for Cloud Usage ..... 48

|      |  |    |
|------|--|----|
| 4.2  | NCD.2.1.02 Security Policy for External Cloud Usage.....   | 48 |
| 4.3  | NCD.2.1.03 Security Concept for External Cloud Services.....   | 49 |
| 4.4  | NCD.2.1.04 Emergency and Continuity Management.....  | 50 |
| 4.5  | NCD.2.2.01 Implementation of Security Requirements .....   | 50 |
| 4.6  | NCD.2.2.02 Contractually Ensure Dealings with Subcontractors and Other External Third Parties51          |    |
| 4.7  | NCD.2.2.03 Ensure Jurisdiction by Contract.....  | 51 |
| 4.8  | NCD.2.2.04 Ensure Location by Contract.....  | 52 |
| 4.9  | NCD.2.2.05 Ensure that Disclosure Obligations and Investigative Powers are Contractually Guaranteed..... | 52 |
| 4.10 | NCD.2.2.06 Regulating the Termination of the Contractual Relationship.....                               | 52 |
| 4.11 | NCD.2.2.07 Ensure Data Return and Data Deletion at the Cloud Service Provider by Contract 53             |    |
| 4.12 | NCD.2.3.01 Integrate ISMS .....  | 53 |
| 4.13 | NCD.2.3.02 Verify Security Certifications.....   | 53 |
| 4.14 | NCD.2.3.03 Check Performance.....  | 54 |
| 4.15 | NCD.2.3.04 Comply with Information Obligations .....   | 54 |
| 4.16 | NCD.2.3.05 Enable Two-Factor Authentication .....  | 54 |
| 4.17 | NCD.2.4.01 Perform Data Return.....  | 54 |
| 4.18 | NCD.2.4.02 Conform Data Deletion.....  | 55 |
| 4.19 | NCD.2.5.01 Shared Use of External Cloud Services .....   | 55 |
| 5    | Microsoft’s Responsibilities as a Cloud Service Provider.....  | 57 |
|      | Appendix A Glossary of IT-Grundschutz-Terms .....  | 58 |
|      | Appendix B References to Further Information.....  | 59 |

# 1

## Executive Summary

Office 365 is Microsoft's enterprise productivity, communication and collaboration suite in the cloud. It provides multi-platform office applications and services including business email, team chat, video conferencing, shared calendars and cloud storage. Office 365 is provided from regions depending on the first activated subscription of the customer and can be verified any time from within the admin portal in Office 365.

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 information security management system (ISMS) described in 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 Office 365 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>1</sup> as part of the Information Domain<sup>2</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 Use of External Cloud Services"<sup>3</sup> which addresses German federal authorities. Chapter 5 discusses Microsoft's responsibilities as a cloud service provider.

---

<sup>1</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>2</sup> See Appendix A Glossary of BSI IT-Grundschutz-Terms for normative terms that have special meanings.

<sup>3</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 Office 365 workbook is based on the revised version of the BSI IT Grundschutz Compendium<sup>4</sup> from the year 2021. This version includes the module *OPS.2.2 Cloud Usage*<sup>5</sup>. It distinguishes between the use of cloud services such as Office 365 and classic IT outsourcing.

### 2.1 Shared Responsibility Model

In contrast to on-premises IT infrastructure, in a cloud service environment, the responsibility for implementing and maintaining security controls for IT applications is shared between customer and the cloud service provider. A full transfer of responsibilities can only occur when the cloud service provider includes the customers' applications in his 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 his cloud service provider along application boundaries, ensuring only one party is responsible for any particular aspect.







Table 1 shows a high level overview of how such a partitioning may look like for Software-as-a-Service (SaaS). 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>4</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>5</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 (SaaS model)<sup>6</sup>

| Aspect/Responsibility   |   | Description  |
|---|---|--|
|  |   |  |
| Security Concept  |    | <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 Office 365.</p>   |
| Data classification & accountability  |    | <p>The value of data can only be determined by the customer, who should therefore identify, classify and label their data.</p> <p>Office 365 supports customers in protecting their data through solutions such as Microsoft Information Protection<sup>7</sup>.</p>   |
| Client & end-point protection   |   | <p>Customers should clearly define the devices and clients that are permitted to access the cloud.</p>   |
| Identity and access management  |  | <p>Office 365 provides multiple options for identity and access management ranging from completely cloud-based (cloud-only identity<sup>8</sup>) to federation with the local Active Directory<sup>9</sup>. Together 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 even for the cloud-only identity option, responsibility still lies partially with the customer.</p> <p>Access to customer data by Microsoft employees can be controlled via Customer Lockbox<sup>11</sup>.</p> |
| Audits  |  | <p>Office 365 is continually audited by independent third parties due to the requirements of multiple compliance standards and certifications.</p>   |

<sup>6</sup> <https://aka.ms/sharedresponsibility>

<sup>7</sup> <https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection>

<sup>8</sup> <https://docs.microsoft.com/en-us/office365/enterprise/about-office-365-identity>

<sup>9</sup> <https://docs.microsoft.com/en-us/office365/enterprise/plan-for-directory-synchronization>

<sup>10</sup> <https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication>

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

## Aspect/Responsibility

-  Cloud Customer
-  Cloud Service Provider

## Description

The list of compliance standards for Office 365 includes BSI C5, ISO 27001, ISO 27017 and ISO 27018.<sup>12</sup>

### Portability



Customer data stored with Office 365 can be exported and downloaded using Microsoft's tools or third party tools.

### Disaster recovery



Office 365 has designed its services with the necessary precaution. The services keep multiple live copies of customer data in multiple datacenters in the chosen regions to ensure the contractual availability<sup>13</sup>.

Customers should develop a disaster recovery plan, which should include backing up data.

### Application level controls



For Office 365 customers the general application level controls (e.g., antimalware and patch management) are provided by Microsoft.

### Network controls



For Office 365 customers the network is managed, configured and secured by Microsoft.

### Host infrastructure



The host infrastructure is provided and managed by Microsoft. The management of host infrastructure includes, for instance, the procurement of servers and their secure configuration.

### Physical security



Physical security ensures 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, a breakdown at another physical location.

<sup>12</sup> <https://docs.microsoft.com/en-us/compliance/regulatory/offering-home>

<sup>13</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-resiliency-and-continuity>

## 2.2 Modelling Office 365

In order to remain IT-Grundschutz-compliant whilst utilizing Office 365 services the IT Security Concept needs to be updated to include Office 365 in accordance with BSI Standard 200-2<sup>14</sup>.

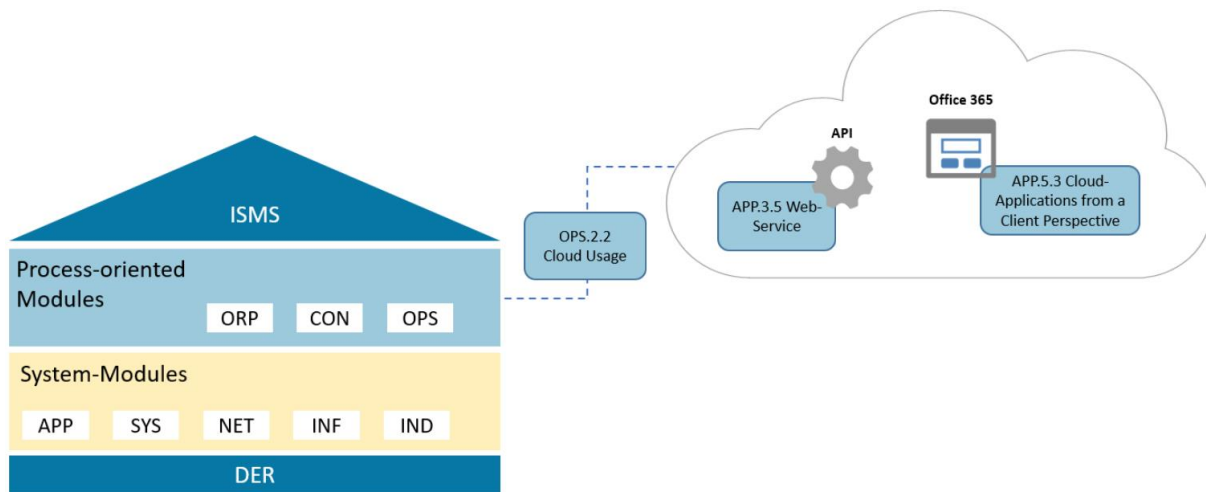


Figure 1 Multi-Layer model of IT-Grundschutz Compendium with Cloud Usage as SaaS

The IT-Grundschutz Compendium takes a layered approach for modelling the information domain. This model consists of four layers: the information security management system module (ISMS), process modules (ORP, CON, OPS), system modules (APP, SYS, NET, INF, IND) and detection and reaction modules (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. Since Office 365 is covered by the Software-as-a-Service (SaaS) deployment model, this workbook only discusses the shared responsibilities regarding SaaS. According to the IT-Grundschutz approach, Microsoft, as the cloud service provider, is responsible for the entire cloud computing stack, from data centers to servers and networks up to the SaaS application. On the customer side, the module *OPS.2.2 Cloud Usage*<sup>15</sup> defines the responsibilities of the customer across the entire cloud stack. The module *OPS.2.2 Cloud Usage* covers applications provided as a cloud service as well as their administration, which encompasses Office 365. The IT-Grundschutz Compendium<sup>16</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 Office 365 from the customer perspective will be included in the new modules *APP.5.3 Cloud-Applications from a Client Perspective* and *APP.3.5 Web-Services*, which

<sup>14</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)

<sup>15</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>16</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)

are not yet published. As long as the modules are not published, a risk analysis must be carried out according to the IT-Grundschutz risk analysis method<sup>17</sup>. Figure 1 shows that module OPS.2.2 Cloud Usage acts as interface between the customer's on premise environment and the customer's cloud environment.

Figure 2 presents the general structure of Office 365 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 combination of network components and Internet service provider.

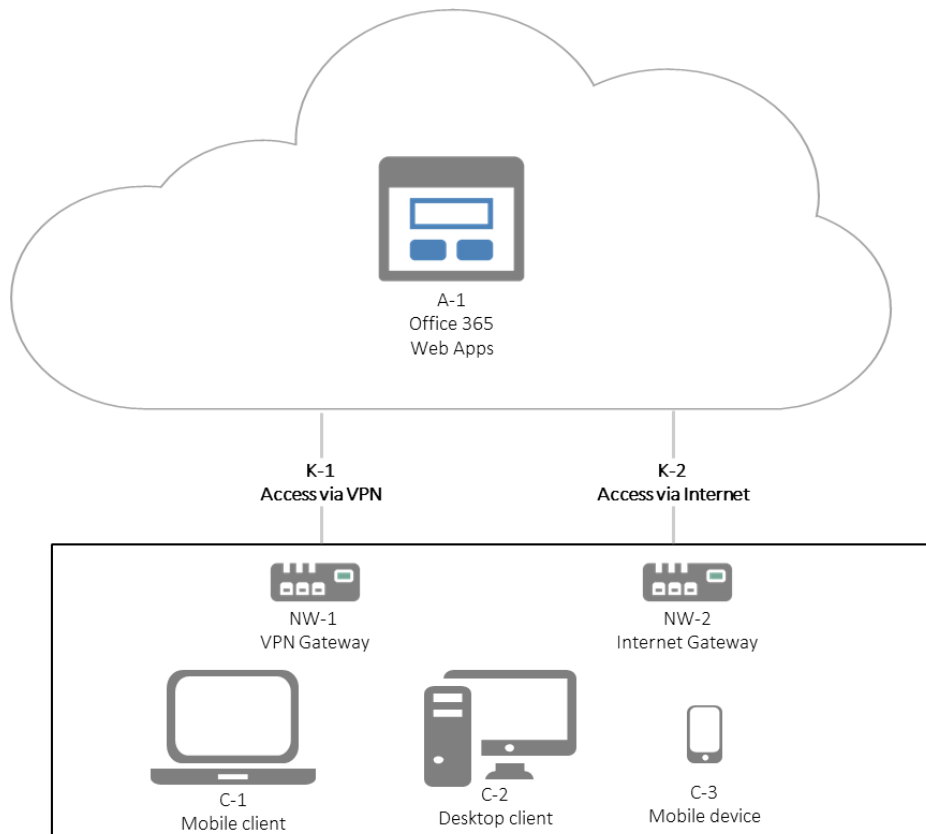


Figure 2 Modelling Office 365 in an IT-Grundschutz network plan (example)

The requirements described in the following chapter provide additional information referenced by the module *OPS.2.2 Cloud Usage*<sup>18</sup> and the applicable implementation notes or helpful online resources provided by Microsoft.

<sup>17</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)

<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)

# 3

## Implementation of Module OPS.2.2 Cloud Usage

The following chapter describes how all requirements from Module *OPS.2.2 Cloud usage*<sup>19</sup> can be implemented for Office 365. In the revised IT-Grundschutz, the requirements were separated from implementation instructions. Implementation instructions for *OPS.2.2 Cloud usage*<sup>20</sup> contains concrete safeguards with which the requirements can be implemented.

While some requirements can only be fulfilled individually, 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 2: 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>21</sup> to support users in formulating a cloud usage strategy.   |
| OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage | Yes  | The security requirements and procedures for the use of Office 365 within an organization need to be defined. Organization is provided with details to aid the definition of security requirements with respect to the confidentiality, integrity and availability of information processed by Office 365. |
| OPS.2.2.A3 Service Definition for Cloud                 | Yes  | This requirement considers additional practical requirements for Office 365 regarding secure authentication, encryption and client interoperability. Microsoft provides  |

<sup>19</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>20</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>21</sup> <https://info.microsoft.com/enterprise-cloud-strategy-ebook.html>

| Requirement   | Supporting information available from Microsoft? | Description  |
|---|--|--|
| Services by the Customer  |  | information on features, which may be used by the customer in securing data.   |
| 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 documentation. <sup>22</sup> Microsoft offers several methods of connecting to and managing Office 365.        |
| OPS.2.2.A5 Planning the Secure Migration to a Cloud Service         | Yes  | Microsoft provides detailed information on security aspects to consider when migrating to Office 365 online services <sup>23</sup> .   |
| OPS.2.2.A6 Planning the Secure Integration of Cloud Services        | Yes  | This requirement aids secure integration of Office 365 into customer's environment. <sup>24</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, Office 365 addresses most of the technical threats and mitigations mentioned in the requirement to support organization in creating a security concept for Office 365.         |
| OPS.2.2.A8 Careful Selection of a Cloud Service Provider            | Yes  | Microsoft offers guidance for the evaluation of Office 365.  |
| OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider | Yes  | Detailed information concerning the contractual arrangements between customer and Microsoft is outlined in this requirement.<br><br>Detailed information concerning the contractual arrangements between customer and Microsoft is outlined in this requirement. |

<sup>22</sup> <https://aka.ms/sharedresponsibility>

<sup>23</sup> <https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices>

<sup>24</sup> <https://docs.microsoft.com/en-us/office365/enterprise/office-365-integration>



| Requirement   | Supporting information available from Microsoft? | Description   |
|---|--|---|
| OPS.2.2.A10 Secure Migration to a Cloud Service                           | Yes  | This requirement covers the execution of the previously planned migration. Microsoft provides tools to assist with migrating current resources to Office 365.   |
| OPS.2.2.A11 Drawing Up a Contingency Concept for Cloud                    | Yes  | The disaster recovery is developed individually for Office 365. General guidelines and information are provided.  |
| OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations | Yes  | Information is made available concerning maintenance of a high level of information security, as well as methods by which user may test the claims set out, especially adherence to the Office 365 SLA. |
| OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage   | Yes  | Microsoft provides information regarding certifications, the corresponding audit reports and other security relevant information, such as penetration testing reports.                                  |
| OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship           | Yes  | Information and guidance on exporting data stored in Office 365 upon termination of an Office 365 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 Office 365.   |
| OPS.2.2.A16 Implementing In-House Backups                                 | Yes  | This must be initiated by the organization; either directly or using a third-party service. Office 365 offers integrated functions for data backup and recovery.  |
| OPS.2.2.A17 Use of Encryption When Using the Cloud                        | Yes  | Microsoft has published information about how Office 365 employs encryption for data in transit and data at rest to meet enhanced protection requirements where necessary.                              |
| OPS.2.2.A18 Use of Federation Services                                    | Yes  | Federated services are provided through the Microsoft Azure service Azure Active Directory, which can be used for the management of users and groups in Office 365.                                     |

| Requirement                               | Supporting information available from Microsoft? | Description   |
|---|--|---|
| OPS.2.2.A19 Security Vetting of Employees | Yes  | Background checks of employees of the cloud provider and its 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 Office 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 characteristics of the services. For example, Azure Active Directory can be used for identity and access management for Office 365, Dynamics 365 and Azure.

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

In a cloud use strategy, the objectives, opportunities and risks of cloud use 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.

Microsoft has produced a general support workbook for creating a cloud use strategy, which answers important questions as well as providing experience-based recommendations concerning cloud strategy, cloud services models and security considerations.<sup>25</sup> The workbook also covers different migration scenarios for Office 365.

The customer must decide which services are to be migrated onto Office 365. This may include partial integration of services (e.g., using Office 365 online but the Outlook/Exchange service on-premises) or the integration of on-premises operational services (e.g., integration of Active Directory on-premises).

Depending on the chosen Microsoft 365 or Office 365 plan<sup>26</sup>, there are multiple solutions with differing levels of integration and connection between cloud services, on-premises services and client applications. The most suitable strategy will likely vary between customers. The following table describes two possible variants with different complexity; the optimum solution for any given customer may lie anywhere on a sliding scale between these two endpoints.

<sup>25</sup> <https://info.microsoft.com/enterprise-cloud-strategy-ebook.html>

<sup>26</sup> <https://technet.microsoft.com/en-us/library/office-365-plan-options.aspx>

Table 3: Different complexities of Office 365 integration

| Low complexity and integration  | High complexity and integration  |
|---|--|
| Cloud only services, fewer administration and control features  | Cloud services connected with on-premises services (e.g., Exchange, SharePoint and Active Directory)   |
| Two-factor authentication via Microsoft features only   | Alternate two-factor authentication available (e.g., via smartcards)   |
| No connection and synchronization between cloud services and on-premises services, higher administrative requirements (e.g., user management) | High integration and synchronization between cloud services and on-premises services, lower administrative requirements, fine grained user access management, automated application and license deployment available |
| High dependency and availability requirements for the Internet connection   | Online and offline processing of business information with synchronization   |
| Web based Office 365 applications   | Web based and local installation of Office 365 applications  |

When matching your requirements against Office 365 offerings, see Appendix B to get reference information.

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

The security policy for cloud use 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 and defined level of protection of the cloud service for the cloud service. The identified 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.

Microsoft provides Office 365 specific information to assist organizations in establishing their security policy regarding data privacy, compliance, transparency and other individualized customer controls.<sup>27</sup> Content of a policy for cloud use depends on the approved development models and cloud services. The table below lists information about security or compliance requirements, which might be fulfilled by the chosen cloud service provider.

<sup>27</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/>  
<https://docs.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide>

Table 4: Useful information on compliance requirements for a security policy for cloud use

| Compliance Requirement                  | Implementation in Office 365   | References  |
|---|--|---|
| <p>Identity &amp; Access Management</p> | <p>Office 365 uses Azure Active Directory to manage identities and authentication. Office 365 supports cloud-only and hybrid identity. Hybrid identities are managed locally and synchronized (with or without password hash) to Azure Active Directory.</p> <p>Azure Active Directory provides different ways to use hybrid identities for Office 365:</p> <ul style="list-style-type: none"> <li>• Password hash synchronization (PHS) synchronizes local accounts including a hash of the password hash into Azure Active Directory</li> <li>• Pass-through authentication (PTA) allows a user to login to Azure using their local 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 a local Active Directory. The users are authenticated against the on-premises Active Directory.</li> </ul> <p>Office 365 supports role based access control (RBAC) and provides several built-in roles. Besides internal accounts of an institution or company, Office 365 allows to add and manage guest accounts and external partners (Business-to-Business, B2B).</p> <p>Office 365 supports several multi factor authentication (MFA) methods, e.g. via mobile app, smart card or certain third party MFA solutions.</p> <p>Privileged Identity Management (PIM) allows managing and monitoring administrative access to Office 365. For example, with PIM privileged access can be limited in time.</p> <p>The conditional access feature of Azure Active Directory can also be used for Office 365. With this feature, Office 365 customer can add automated access</p> | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity">https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity</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> <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/active-directory/external-identities/o365-external-user">https://docs.microsoft.com/en-us/azure/active-directory/external-identities/o365-external-user</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles">https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing">https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure">https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure</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> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up">https://docs.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up</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> |

| Compliance Requirement | Implementation in Office 365  | References   |
|------------------------|---|--|
|                        | <p>control decisions for accessing data and apps in Office 365 that are condition based. Further information and links on encryption and cryptographic functions can be found in Table 10 in subchapter 3.17 <i>OPS.2.2.A17 Use of Encryption When Using the Cloud</i>.</p> <p>Mobile device management (MDM) or Intune can be used to secure and configure mobile devices that are allowed to access Office 365.</p>   | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption</a></p>   |
| Asset Management       | <p>Resources, users and groups can be managed using the admin center of Office 365.</p> <p>Office 365 allows to label data according to sensitivity and to enforce automatically protection settings based on the label.</p> <p>Microsoft Information Protection (MIP) can help to classify data and can be used to apply labels and to apply optionally protection safeguards. Labels can be applied automatically based on rules / conditions or manually.</p>  | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/admin/admin-overview/about-the-admin-center">https://docs.microsoft.com/en-us/microsoft-365/admin/admin-overview/about-the-admin-center</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels">https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection">https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection</a></p>   |
| Protection of Data     | <p>Customer isolation within Office 365 is implemented by several technical means. This includes logical isolation using role based access control, encryption and storage level isolation for SharePoint.</p> <p>Data at-rest and in-transit can be encrypted using state of the art cryptographic methods and protocols, like AES, IPSec or TLS/SSL. For example, email and attachments stored in Office 365 mailbox or the communication of devices with Office 365.</p> <p>Microsoft continuously tests and monitors the security of Office 365 and takes actions accordingly. Corresponding reports, e.g. for penetration tests or audits, can be accessed using the trust center.</p> | <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls">https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-monitoring-and-testing">https://docs.microsoft.com/en-us/compliance/assurance/assurance-monitoring-and-testing</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/microsoft-365/enterprise/view-service-health">https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health</a></p> |

| Compliance Requirement | Implementation in Office 365  | References   |
|------------------------|---|--|
|                        | <p>The service health of Office 365 can be viewed on the Office 365 Service health page in the Office 365 admin center.</p> <p>Office 365 has detailed logging functionality implemented. The logs are accessible in a unified and searchable audit log that allows viewing user and administrator activity in Office 365.</p> <p>Data can be automatically protected based on assigned labels, e.g. by automated encryption or with data loss prevention (DLP) safeguards.</p> | <p><a href="https://status.office365.com/">https://status.office365.com/</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance">https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels">https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels">https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/security-roadmap">https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/security-roadmap</a></p> |

## Compliance and Audit

Microsoft invested in the processes to meet the requirements of the Model Clauses for the transfer of personal data processors.

Office 365 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

Additionally, Microsoft provides guidance how General Data Protection Regulation (GDPR) requirements can be realized in Office 365 by the customer. This includes an accountability readiness checklist, a data protection impact assessment template and how to suitably answer data subject requests.

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.

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-EU-Model-Clauses>

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365>

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365>

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-Office365>

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-arc-Office365>

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-ISO-27018>

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

<https://docs.microsoft.com/en-us/compliance/assurance/assurance-auditing-and-reporting-overview>

| Compliance Requirement | Implementation in Office 365   | References   |
|------------------------|--|--|
|                        | <p>Office 365 provides several auditing and reporting features including a unified audit log with search features. The unified audit log can also be used to track user or administrator activity.</p> <p>Microsoft provides detailed guidelines how to achieve security and compliance with legal or regulatory standards with Office 365.</p> <p>Office 365 allows the definition of data retention policies to manage effectively data in compliance with policies, regulations and legal requirements. The policies can ensure content cannot be permanently deleted before the end of the retention period. Additionally, the policies can be used to delete permanently content after end of the retention period.</p> <p>Microsoft provides an overview about its data storage locations for Office 365.</p> <p>Compliance Manager is a workflow-based risk assessment tool to track, assign and verify compliance activities related to Office 365. It provides a centralized dashboard for standards, regulations and implementation including results for service assessments.</p> <p>Electronic discovery (eDiscovery) is the process of identifying and delivering electronic information that can be used as evidence in legal cases. The eDiscovery service allows to search, identify, hold and export content in Office 365. Use of the Advanced eDiscovery solution allows, for example, further analysis of the content found by eDiscovery.</p> | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance">https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/">https://docs.microsoft.com/en-us/microsoft-365/</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/retention">https://docs.microsoft.com/en-us/microsoft-365/compliance/retention</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations">https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager">https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery">https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/overview-ediscovery-20">https://docs.microsoft.com/en-us/microsoft-365/compliance/overview-ediscovery-20</a></p> |
| Backup and archiving   | <p>Office 365 preserves permanent files of all data collected in a non-rewriteable, non-erasable format using retention and preservation policies including a preservation lock.</p> <p>Data resiliency and recoverability are built-in for Office 365, to maximize reliability and minimize negative effects on</p>   | <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-immutability">https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-immutability</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-resiliency-overview">https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-resiliency-overview</a></p>  |



| Compliance Requirement | Implementation in Office 365   | References  |
|------------------------|--|---|
|                        | <p>customers. This is achieved through a combination of physical infrastructure and software solutions, e.g. by saving copies of customer data within different fault zones or as many fault domains as possible.</p> <p>Exchange Online backup and archiving can be realized by the customer using Exchange Online Archiving to store mailbox data within different data center. Additionally, third party solutions can be used to realize backups and archives for different Office 365 services.</p>   | <p><a href="https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data">https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data</a></p> <p><a href="https://docs.microsoft.com/en-us/exchange/back-up-email">https://docs.microsoft.com/en-us/exchange/back-up-email</a></p>   |
| Threat protection      | <p>Microsoft realizes its defense against distributed denial of service (DDoS) attacks following the three core principles Absorption, Detection and Mitigation. Due to the size and amount of cloud services of Microsoft, it has the capacity to absorb DDoS attacks until detection and mitigation step in and thus is able to provide strong network protection to its cloud customers.</p> <p>Additionally, third party DDoS protection solutions can be used to protect Office 365 against DDoS attacks.</p> <p>Office 365 has a strong malware protection in place. This includes automatic scans of the environment, at least weekly scans of the file system, real-time scans of files as they are downloaded, opened or executed, automatic daily signature updates as well as altering, cleaning and mitigating detected malware.</p> | <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-dos-defense-strategy">https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-dos-defense-strategy</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection">https://docs.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection</a></p> |
| Change Management      | <p>Microsoft provides a guideline how to stay up to date with the fast development within Office 365 and how to get latest update information. Thereby, Microsoft provides a roadmap of ongoing and planned updates.</p>   | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/admin/manage/stay-on-top-of-updates">https://docs.microsoft.com/en-us/microsoft-365/admin/manage/stay-on-top-of-updates</a></p> <p><a href="https://www.microsoft.com/en-us/microsoft-365/roadmap">https://www.microsoft.com/en-us/microsoft-365/roadmap</a></p>   |

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

For every planned and ordered cloud service a definition 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 detailed descriptions of the services and features available with Office 365<sup>28</sup>. Each service has its own service description containing relevant information for this service, for instance, a service overview, prerequisites, system requirements, features contained within the different subscriptions and the corresponding pricing.

As part of the service definition for cloud services, the institution should also address the following aspects in more detail: Selection of secure authentication methods, definition of Operational Level Agreements (OLAs) and Service Level Agreements (SLAs) and further security aspects as described in the table below.

Table 5: Selection of further information that needs to be considered for the service definitions

| Compliance Requirement                  | Implementation in Office 365  | References  |
|---|---|---|
| Choice of secure authentication methods | Office 365 offers basic Azure Active Directory features including a subset of Azure Multi-Factor Authentication (MFA).                                  | <a href="https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication">https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication</a> |
|   | Role-based access control is available for controlling cloud services via the Microsoft Office 365 Portal.  | <a href="https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing">https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing</a>                                       |
|   | Depending on the Microsoft 365 or Office 365 plan further multi-factor authentication features can be used.   | <a href="https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles">https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles</a>   |
|   | Azure Active Directory enables customers to provision role-based access rights within the cloud or as hybrid solution with your local active directory. | <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>   |
|   | The conditional access feature allows to restrict the access to services based on customer definable conditions like source IP,                         | <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>   |

<sup>28</sup> <https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-service-descriptions-technet-library>

| Compliance Requirement                            | Implementation in Office 365   | References   |
|---|--|--|
|   | <p>device user or the authentication method.</p> <p>Intune can be used to secure and configure mobile devices that are allowed to access Office 365.</p>   |  |
| <p>Further considerations of security aspects</p> | <p>Office 365 offers encryption for data at rest and in transit (see also the <i>Confidentiality</i> section in the table within subchapter 3.17 OPS.2.2.A17 <i>Use of Encryption When Using the Cloud</i>).</p> <p>Customer lockbox allows the customer to approve or deny Microsoft's support to access customer data in support cases.</p> <p>Isolation between customers (multi-tenancy) is realized on compute, storage, database and network level to ensure that no access to other customer's data is possible, even when running on the same hardware.</p> <p>Data resiliency and recoverability are built-in for Office 365, to maximize reliability and minimize negative effects on customers. This is achieved through a combination of physical infrastructure and software solutions, e.g. by saving copies of customer data within different fault zones or as many fault domains as possible.</p> <p>For Exchange Online backup and archiving can be realized by the customer using Exchange Online Archiving to store mailbox data within different data centers. Additionally, third party solutions can be used to realize backups and archives for different Office 365 services.</p> | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo">https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo</a></p> <p><a href="https://docs.microsoft.com/en-us/office365/servicedescriptions/skype-for-business-online-service-description/skype-for-business-online-features">https://docs.microsoft.com/en-us/office365/servicedescriptions/skype-for-business-online-service-description/skype-for-business-online-features</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-service-encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-service-encryption</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests">https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests</a></p> <p><a href="https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-tenant-isolation-overview">https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-tenant-isolation-overview</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls">https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-resiliency-overview">https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-resiliency-overview</a></p> |

| Compliance Requirement           | Implementation in Office 365   | References   |
|----------------------------------|--|--|
|                                  |  | <a href="https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data">https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data</a><br><br><a href="https://docs.microsoft.com/en-us/exchange/back-up-email">https://docs.microsoft.com/en-us/exchange/back-up-email</a> |
| Client software interoperability | Office 365 offers a variety of functionalities via Office 365 APIs. All of the Office 365 Management APIs are consistent in design and implementation with the current suite of Office 365 REST APIs, using common industry-standard approaches, including OAuth v2, OData v4, and JSON. | <a href="https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-apis-overview">https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-apis-overview</a>  |

### 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>29</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.

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.

---

<sup>29</sup> <https://aka.ms/sharedresponsibility>  
<https://azure.microsoft.com/mediahandler/files/resourcefiles/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20nboard-ing%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/>

### 3.5 OPS.2.2.A5 Planning the 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 further course 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 Office 365 must be appropriately planned.

Microsoft offers a workbook<sup>30</sup> to support customers in migration planning. The workbook combines answers to important questions with experience-based recommendations concerning a migration to the cloud. When planning the migration, the customer should consider security aspects across the various phases.

The migration to Office 365 includes data types, such as files (e.g., fileservers)<sup>31</sup> and mailboxes (e.g., Microsoft Exchange)<sup>32</sup>. Microsoft provides support for migrating multiple email accounts to Office 365<sup>33</sup> and for migrating to SharePoint Online<sup>34</sup>. Additionally, Microsoft offers FastTrack for valid subscriptions aiding the migration process<sup>35</sup>.

### 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 the Secure Migration to a Cloud Service*), the integration of Office 365 is essential for secure and continuous IT operations. This requirement considers aspects beyond planning the migration.

There are various methods to prepare the integration of cloud based Office 365 features. The organization shall establish and document a security concept that considers security requirements affecting the following aspects:

- Required adaptations of the existing IT landscape
- Suitability of existing interfaces (e.g., proxy) for Office 365 use

---

<sup>30</sup> <https://info.microsoft.com/enterprise-cloud-strategy-ebook.html>

<sup>31</sup> <https://docs.microsoft.com/en-us/sharepointmigration/migrate-to-sharepoint-online>  
<https://docs.microsoft.com/en-us/sharepointmigration/sharepoint-online-and-onedrive-migration-speed>

<sup>32</sup> <https://docs.microsoft.com/en-us/microsoft-365/compliance/use-network-upload-to-import-pst-files>

<sup>33</sup> <https://docs.microsoft.com/en-us/Exchange/mailbox-migration/mailbox-migration>

<sup>34</sup> <https://docs.microsoft.com/en-us/sharepointmigration/migrate-to-sharepoint-online>

<sup>35</sup> <https://docs.microsoft.com/en-us/fasttrack/introduction>

- Definition of the administration model for the cloud based Office 365 features, e.g., use 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

The Office 365 integration<sup>36</sup> options include:

- Hybrid use (cloud services and on-premises) with synchronization, including the option of migration to cloud based services and deactivation of on-premises components in a downstream step
- Use of Microsoft's data portability features<sup>37</sup> for Exchange, SharePoint and user defined domains within the Microsoft Cloud
- Use of third-party tools for Office 365 and SharePoint integration

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>38</sup>

Microsoft Information Protection (MIP)<sup>39</sup> can be used to classify local data as well as data stored in the cloud. Based on the classification, security measures can then be implemented, such as a document may only be read by a limited group of people. Within the framework of this requirement, it should be decided to what extent the functionalities are integrated into the local network.<sup>40</sup>

Additionally, a learning platform is offered, where many specific supporting contents can be found for training.<sup>41</sup>

With the Evergreen approach, Microsoft aims to keep all Office 365 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.

### 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 Office 365 as cloud service should be developed. Threats arise from contractual deficiency, dependencies or responsibilities. They cause loss of control and inefficient performance. Several parties are involved, particularly in regards to the cloud services. At the very least, the following parties should be taken into account: cloud service customer, Microsoft as cloud service provider and network provider.

<sup>36</sup> <https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity>  
<https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration>

<sup>37</sup> [https://docs.microsoft.com/en-us/openspecs/data\\_portability/ms-dataportlp/a2bc1311-e0e7-4808-970a-4dc0a100f708](https://docs.microsoft.com/en-us/openspecs/data_portability/ms-dataportlp/a2bc1311-e0e7-4808-970a-4dc0a100f708)  
<https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/interoperability-connectivity-and-compatibility>

<sup>38</sup> <https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security>

<sup>39</sup> <https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection>

<sup>40</sup> <https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

<sup>41</sup> <https://docs.microsoft.com/en-us/learn/azure/>

While there is no generic template for your organization's requirements, Microsoft Office 365 addresses many of the threats and mitigations mentioned in the official implementation recommendations of IT-Grundschutz as follows.

Table 6: Threats to be addressed in the security concept for cloud use

| Cloud-specific threats  | Conditions on Office 365   | References  |
|---|--|---|
| Pre-emptive or compulsorily contract ending   | Contract ending is addressed in detail within a dedicated requirement.   | Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i>  |
| Lack of portability, e.g. because of proprietary data formats (possibly resulting in Vendor lock in)  | Portability as addressed in detail within a dedicated requirement.   | Subchapter 3.15 <i>OPS.2.2.A15 Ensuring the Portability of Cloud Services</i>   |
| Missing knowledge about physical data storage location  | Office 365 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.<br><br>All datacenters from Microsoft are physical protected against unauthorized access and several other threats.   | <a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations">https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations</a><br><br><a href="https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure">https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure</a>  |
| 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 that are allowed to access Office 365.<br><br>Together with conditional access, this can be used to restrict access to certain data or services within Office 365, 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. | <a href="https://docs.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up">https://docs.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up</a><br><br><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><br><br><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> |
| Unauthorized access (e.g. by cloud provider admins or other cloud customers)  | By default Microsoft personnel has no access to customer data. By using lock-box customer can approve or deny Microsoft access to their data. Access to customer data by Microsoft personnel is secured by strong secure safeguards such as multi factor authentication  | <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><br><br><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>  |



| Cloud-specific threats | Conditions on Office 365   | References  |
|------------------------|--|---|
|                        | <p>(MFA) and detailed logging and monitoring.</p> <p>Even when running on same hardware, the isolation between customers (multi-tenancy) is realized on compute, storage, database and network level to ensure that no access to other customer's data is possible</p> <p>To prevent unauthorized access to customer data, it is encrypted at rest and during transfer, including transfer between Office 365 data centers, using state of the art protocols and cryptography such as AES.</p> | <p><a href="https://go.microsoft.com/fwlink/p/?LinkID=2162834">https://go.microsoft.com/fwlink/p/?LinkID=2162834</a> (Whitepaper: How does Microsoft handle your data in the cloud?)</p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests">https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests</a></p> <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls">https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-service-encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-service-encryption</a></p> |

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

Subsequent to the planning and conception process, a detailed requirement profile of Microsoft as cloud service provider should be developed. These requirements should be defined according to 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.<sup>42</sup> If the results are not satisfactory, a cloud service provider may be removed from further consideration. Microsoft supports due diligence evaluations with a checklist that is based on international standard ISO/IEC 19086-1, the Cloud Computing Service Level.<sup>43</sup>

The following table lists information, which should be gathered and assessed ahead of migrating to the cloud.

Microsoft provides information for a thorough evaluation of Office 365.<sup>44</sup>

Table 7: Consideration before migration to Office 365

| Consideration to be made   | Conditions on Office 365   | References  |
|--|--|---|
| Publicly available information about the provider (reputation, ratings and rankings, core business, performance, cloud experience) | <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>Office 365 is constantly extended and updated. Microsoft publishes roadmaps and further information about planned updates for Office 365 on their webpage.</p> <p>Exchange with other customer is possible in the Microsoft Technet community to receive further information about Office 365.</p> <p>Microsoft provides customer stories on their usage of Office 365.</p> <p>Microsoft provides the Service Health feature within Office 365 admin center, which shows the status of services, like Office 365. The dashboard can be customized and provides users with the ability to track relevant events or configure event alarms.</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://www.microsoft.com/en-us/microsoft-365/roadmap">https://www.microsoft.com/en-us/microsoft-365/roadmap</a></p> <p><a href="https://techcommunity.microsoft.com/t5/Office-365/bd-p/Office365General">https://techcommunity.microsoft.com/t5/Office-365/bd-p/Office365General</a></p> <p><a href="https://products.office.com/en-us/business/customer-stories">https://products.office.com/en-us/business/customer-stories</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health">https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health</a></p> <p><a href="https://admin.microsoft.com/">https://admin.microsoft.com/</a></p> <p><a href="https://status.office365.com/">https://status.office365.com/</a></p> <p><a href="https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity">https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity</a></p> |
| Due-Diligence  | <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>  |

<sup>42</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>43</sup> <https://www.microsoft.com/en/trust-center/compliance/due-diligence-checklist>

<sup>44</sup> <https://www.microsoft.com/en-us/trust-center>

Consideration to be made

Conditions on Office 365

References

Access through cloud provider or third parties

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.

The access can be denied or approved by the customer using the customer lock-box features.

The customer isolation implemented in Office 365 ensures that different customers cannot access the data of others, even if they are computed or stored on the same hardware.

Data at rest and in transit is encrypted in Office 365, so unauthorized parties cannot access the information contained.

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

<https://www.microsoft.com/en-us/trust-center/privacy/data-access>

<https://go.microsoft.com/fwlink/p/?LinkId=2162834&clcid=0x407> (Whitepaper: How does Microsoft handle your data in the cloud?)

<https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests>

<https://docs.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls>

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

Installation of additional software

Office 365 can be used with the browser or with local installations of appropriate office applications. Access to the later varies across subscription types.

<https://www.microsoft.com/en-us/microsoft-365/microsoft-365-and-office-resources>

Locations of the cloud provider

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 purpose, customer data is replicated to other datacenters within the same geolocation.

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations>

Subcontractors of the cloud provider

Microsoft publishes and regularly updates 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.

<https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407> (Microsoft Online Services Subprocessors List)

| Consideration to be made                                  | Conditions on Office 365   | References  |
|---|--|---|
|   | <p>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 EU Model Clauses.</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/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/p/?LinkID=2162834&amp;clid=0x407">https://go.microsoft.com/fwlink/p/?LinkID=2162834&amp;clid=0x407</a> (Whitepaper: How does Microsoft handle your data in the cloud?)</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> |
| <p>Consideration of contractual basis and regulations</p> | <p>The Service Level Agreements and Microsoft's Online Services Terms are the standard stipulations governing the use of Office 365 services. They are published on the webpage and accessible without Microsoft subscription or Office 365 account.</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>Evaluation of services including warranties</p>        | <p>Services descriptions, documentation and pricing information are published on the webpage of each service.</p>  | <p><a href="https://docs.microsoft.com/en-us/office365/service-descriptions/office-365-service-descriptions-technet-library">https://docs.microsoft.com/en-us/office365/service-descriptions/office-365-service-descriptions-technet-library</a></p> <p><a href="https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans">https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans</a></p>   |

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

Following the selection of one or more suitable cloud service provider, the relevant aspects should be defined in contractual service level agreements. 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 in Office 365. The previously defined requirements must be considered, and at least the following points must be answered with respect to Office 365.

Table 8: Content to be considered for drafting of contract

| Contract documents   | Conditions on Office 365   | References  |
|--|--|---|
| <p>Physical location of the services and cloud service provider</p>    | <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 Office 365, among others, will take place exclusively within Europe.</p> <p>All datacentres 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://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations">https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations</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/compliance/assurance/assurance-datacenter-security">https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security</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> |
| <p>Supervision of service delivery</p>                                 | <p>Microsoft provides the Service Health feature within the Office 365 admin center, which shows the status of services, such as Office 365. Customers can check the service status page for known issues preventing customers from logging into their tenant.</p>   | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health">https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health</a></p> <p><a href="https://admin.microsoft.com/">https://admin.microsoft.com/</a></p> <p><a href="https://status.office365.com/">https://status.office365.com/</a></p> <p><a href="https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity">https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity</a></p>   |
| <p>Subcontractors and third parties involved with service delivery</p> | <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><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>   |

| Contract documents   | Conditions on Office 365  | References  |
|--|---|---|
| <p>Rules concerning the personnel of the cloud service provider</p>        | <p>The personnel (both internal and external) employed by Microsoft have all required competencies and are cleared according to internal policies.</p>  | <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/office365/securitycompliance/office-365-personnel-controls">https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-personnel-controls</a></p>   |
| <p>Rules concerning communication channels and contact persons</p>         | <p>The account manager is the primary contact point for customer.</p> <p>The main communication channel online for Office 365 is the support menu within the administrative interface. Additional means of contacting Microsoft is the support webpage.</p>   | <p><a href="https://support.office.com/en-us/home/contact">https://support.office.com/en-us/home/contact</a></p>  |
| <p>Rules concerning processes, working procedures and responsibilities</p> | <p>Office 365 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 Office 365.</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/en-us/licensing/product-licensing/products">https://www.microsoft.com/en-us/licensing/product-licensing/products</a></p> <p><a href="http://status.office365.com/">http://status.office365.com/</a></p> <p>Subchapter 2.1 <i>Shared Responsibility Model</i></p> <p><a href="https://www.microsoft.com/en-us/microsoft-365/roadmap">https://www.microsoft.com/en-us/microsoft-365/roadmap</a></p> |
| <p>Provisions for ending the contractual agreement</p>                     | <p>Office 365 is offered on an annual subscription basis. Early termination may be possible.</p>  | <p><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></p> <p><a href="https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans">https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans</a></p>   |

| Contract documents   | Conditions on Office 365  | References  |
|--|---|---|
|  |   | <p>Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i></p>   |
| <p>Secure deletion of data by the cloud service provider</p> | <p>When a paid subscription is terminated or ends, the Office 365 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><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview">https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview</a></p> <p><a href="https://www.microsoft.com/en-us/trust-center/privacy/data-management">https://www.microsoft.com/en-us/trust-center/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/compliance/assurance/assurance-data-bearing-device-destruction">https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction</a></p> |
| <p>Emergency preparedness</p>                                | <p>Office 365 has defined rules for continuation of services to the level set out by the SLA.</p> <p>Corresponding safeguards include the geographical separation of the data centers and the continuous replication of data between them.</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/compliance/assurance/assurance-data-resiliency-overview">https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-resiliency-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>Rules governing checks and audits</p>                     | <p>Office 365 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>Cloud users have the ability to carry out penetration tests against their</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/msrc/pentest-rules-of-engagement">https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement</a></p>   |



| Contract documents | Conditions on Office 365   | References |
|--------------------|--|------------|
|                    | <p>cloud services without notifying Microsoft, whether the corresponding rules of engagement are adhered. The main restriction is that no Denial of Service (DoS) tests are allowed. In addition, other Office 365 customers must not be disturbed by penetration tests.</p> |            |

## Data Protection

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.

Microsoft offers customers the EU Standard Contractual Clauses (SCC) (also known as EU Model Clauses), 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.

As a result of the European Court of Justice (ECJ) ruling in July 2020 that invalidated the EU-US Privacy Shield Agreement, the *Microsoft Products and Services Data Protection Addendum* was supplemented by the *Appendix C Additional Safeguard Addendum*. This appendix specifies additional security measures with regard to the processing of personal data.

Microsoft provides information about how the GDPR requirements are handled and 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.

<https://aka.ms/DPA>

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses>

<https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview>

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr>

<https://eu-coc.cloud/en/home.html>

### 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 the Secure Migration to a Cloud Service*) 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 provides a variety of tools to assist with migrating current resources to Office 365.<sup>45</sup>

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

A business continuity concept should be developed as a preventive security safeguard for Office 365. Particularly, 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 contractually covered by the service levels agreements<sup>46</sup>. Instead, this requirement covers the individual plan for an organization in the event of loss of the cloud service itself or access to it. It also addresses situations where the applicable service levels do not cover the requirements.

Should the online services be unavailable, the disaster recovery plan may include carrying out data backups (see subchapter 3.16 *OPS.2.2.A16 Implementing In-House Backups*) and use of the desktop version of Office 365. In this case, a Microsoft 365 or Office 365 plan including desktop software needs to be chosen. Alternatively, the use of Office 365 as a hybrid solution could also be considered to reduce the impact of unavailability of online services.

When using hybrid or online-only solutions of Office 365, one should also consider the increased dependency on the availability of the Internet connection compared to on-premises solutions. Therefore, the disaster recovery plan should also include an agreement with the Internet service provider or provision for a redundant connection.

Furthermore, business continuity plans concerning the relevant business processes, which depend on Office 365, should be considered specifically and in detail the loss of availability. This should be planned independently of the reason for the availability loss (e.g., outage of Internet access in the local network, outage at the Internet service provider).

---

<sup>45</sup> <https://www.microsoft.com/en-us/fasttrack/>

<sup>46</sup> <https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx> (Service Level Agreements)

## 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 compliant with standards should be checked regularly, by both the customer as well as the cloud service provider.

Table 9: Requirements to preserve information security

| Requirements   | Details on Office 365  | 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>Office 365 includes an integrated SLA Monitoring system ("Service Health") which enables checking the compliance of the services. This includes receiving service notification on a mobile device.</p> <p>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.</p> | <p><a href="http://status.office365.com/">http://status.office365.com/</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health">https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health</a></p> <p><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></p> <p><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></p> |
| Security certificates should be supplied by the cloud service provider.  | <p>Office 365 offers, in this case, a variety of publications and verifications as well as applicable certifications. This can be verified by a user of Office 365 on the public website as well as in the audit results that can be viewed in the Service Trust Portal (STP).</p>   | <p><a href="https://servicetrust.microsoft.com/">https://servicetrust.microsoft.com/</a></p> <p><a href="https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview">https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview</a></p> <p><a href="https://servicetrust.microsoft.com/Documents/ComplianceReports">https://servicetrust.microsoft.com/Documents/ComplianceReports</a></p>  |
| Coordination talks should be held regularly between the cloud ser-   | <p>Office 365 offers a variety of options for support and gathering of status</p>  | <p><a href="http://status.office365.com">http://status.office365.com</a></p> <p><a href="https://support.microsoft.com/en-us/office">https://support.microsoft.com/en-us/office</a></p>   |

| Requirements  | Details on Office 365  | References   |
|---|--|--|
| <p>vice provider and the organization using the cloud.</p>  | <p>information. Customers will be contacted in the event of significant service disruption.</p>  |  |
| <p>Exercises and tests to simulate the response to system failures should be planned and performed.</p> | <p>Office 365 has defined rules for the continuation of services to the level set out by the SLA.</p>  | <p><a href="https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity">https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity</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>Ensure proper administration of cloud services</p>   | <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 security policies and a secure score functionality to inform about configurations that might be considered as insecure.</p> | <p><a href="https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reference-policies-practices-and-guidelines">https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reference-policies-practices-and-guidelines</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score">https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score</a></p>  |
| <p>Ensuring interoperability of cloud services</p>  | <p>When using multiple cloud services, interoperability tests should be performed for each service to ensure proper collaboration between the different cloud services.</p>  | <p><a href="https://www.microsoft.com/en-us/legal/interoperability">https://www.microsoft.com/en-us/legal/interoperability</a></p> <p><a href="https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/interoperability-connectivity-and-compatibility">https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/interoperability-connectivity-and-compatibility</a></p> <p>Subchapter 3.15 <i>OPS.2.2.A15 Ensuring the Portability of Cloud Services</i></p> |
| <p>Proper execution of data backups</p>   | <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 a hybrid environment or a backup services provided by an external provider or backup system of the customer. If an external provider is de-</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 <i>OPS.2.2.A16 Implementing In-House Backups</i></p>   |

| Requirements   | Details on Office 365  | References   |
|--|--|--|
|  | <p>ecided upon, the customer must ensure that all the requirements for backup and data security are fulfilled.</p>   |  |
| <p>Control of technical safeguards to prevent the use of unauthorized services</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>Microsoft Information Protection (MIP) can be used to classify local data as well as data stored in the cloud. Based on the classification, security measures can then be implemented, such as a document may only be read by a limited group of people.</p> | <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task">https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/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> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection">https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection</a></p> |
| <p>Performing audits, security checks, penetration tests or vulnerability analyses</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><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 the customer satisfies auditing requirements and also 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 Cloud and Office 365 are continually audited, due to the requirements of multiple international and national compliance standards and certifications. The list of compliance standards for Office 365 includes BSI C5, ISO 27001, ISO 27017 and ISO 27018 (see chapter 5 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>47</sup>, which provides direct access to many of the compliance reports and attestations.

<sup>47</sup> <https://servicetrust.microsoft.com/>

Nevertheless, the responsibility reading and assessing the reports lies with the cloud customer. The assessment should only be done by qualified personnel from the customer.

### 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 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>48</sup> to its customers.

Office 365 provides different ways to export customer data. Document data can be easily exported to existing Microsoft formats such as Excel or Word and Exchange mailboxes can be exported using the .pst file format. In general, Office 365 application data can be easily imported into its on-premises counterpart.

With the hybrid solution of Office 365, data can be synchronized to the on-premises IT system.<sup>49</sup> Otherwise, if a bulk export needs to be performed, third-party solutions are available.

By default, Office 365 data can be exported for 90 days upon contract termination. Customer data will be deleted within 180 days<sup>50</sup> after the end of the agreed use period or the cancellation of the user agreement.<sup>51</sup>

When terminating the Office 365 contract as an online service, 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.

---

<sup>48</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

<sup>49</sup> <https://docs.microsoft.com/en-us/office/office-365-management-api/>

<sup>50</sup> <https://docs.microsoft.com/en-us/microsoft-365/commerce/subscriptions/cancel-your-subscription>

<https://www.microsoft.com/en-us/trust-center/privacy/data-management>

<https://www.microsoft.com/en-us/trust-center/privacy/data-management>

<https://aka.ms/DPA>

<sup>51</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview>

## 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 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.

Office 365 supports various methods of data migration:

1. Using Office 365 APIs, allowing access to customer data.<sup>52</sup>
2. Using portability options provided by the single cloud services. For instance, downloading documents from SharePoint Online or exporting Exchange Online data using Import and Export wizard.<sup>53,54</sup>
3. Synchronization of data to on-premises components when using the hybrid cloud solution.<sup>55</sup>
4. Use of third-party tools for Office 365 to import/export data.

The data will be exported in common formats, e.g., Microsoft Office (Word, Excel, PowerPoint etc.) or .pst files (Exchange). The specifications of the relevant Office Open XML or .pst file formats are freely available.<sup>56</sup> The Azure File storage can be used to store the files. As Azure File storage supports the SMB protocol the files can then be transferred via SMB to a Windows share.<sup>57</sup>

The move to another cloud service provider or to on-premises environments should be adequately planned and tested. The following questions should be considered:

- Does the target environment offer the same features as Office 365 (functionality, security, performance, scalability etc.)?
- Is the new platform able to process the exported data of Office 365?
- Are there any Microsoft or third-party tools for converting the data or file formats into the target formats?

## 3.16 OPS.2.2.A16 Implementing In-House Backups

This requirement aims to ensure data availability when access to Office 365 data is lost, cloud services themselves are unavailable or data is lost due to user action (e.g., inadvertent deletion of data).

Office 365 offers several integrated functions and options for data recovery, for instance “Recycle Bin”, online data backup or archiving functions as well as third-party applications.

---

<sup>52</sup> <https://docs.microsoft.com/en-us/previous-versions/office/office-365-api/>

<sup>53</sup> <https://support.office.com/en-us/article/export-to-excel-from-sharepoint-bfb2ea48-6118-4fa9-abb6-cced9424e5d9>

<sup>54</sup> <https://support.office.com/en-us/article/download-files-and-folders-from-onedrive-or-sharepoint-5c7397b7-19c7-4893-84fe-d02e8fa5df05>

<sup>55</sup> <https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models>

<sup>56</sup> DOCX-Files: [https://docs.microsoft.com/en-us/openspecs/office\\_standards/ms-docx/b839fe1f-e1ca-4fa6-8c26-5954d0abbccd](https://docs.microsoft.com/en-us/openspecs/office_standards/ms-docx/b839fe1f-e1ca-4fa6-8c26-5954d0abbccd)  
XLSX-Files: [https://docs.microsoft.com/en-us/openspecs/office\\_standards/ms-xlsx/2c5dee00-ef2-4b22-92b6-0738acd4475e](https://docs.microsoft.com/en-us/openspecs/office_standards/ms-xlsx/2c5dee00-ef2-4b22-92b6-0738acd4475e)  
PST-Files: [https://docs.microsoft.com/en-us/openspecs/office\\_file\\_formats/ms-pst/141923d5-15ab-4ef1-a524-6dce75aae546](https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-pst/141923d5-15ab-4ef1-a524-6dce75aae546)

<sup>57</sup> <https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

Customers should decide, whether the data recovery functions and options in Office 365 meet their needs, e.g., legal, contractual or protection requirements, or if an additional export to local or another cloud backup storage should be implemented. This should be considered in the organization's data backup policy, which is described in the IT-Grundschrift module *CON.3 Data backup policy* as a part of the IT-Grundschrift Compendium. Especially the content of requirement *CON.3.A6 Development of a data backup policy*, *CON.3.A8 Function tests and verification of recovery*, *CON.3.A1 Determining the factors influencing data backup* and *CON.3.A3 Identification of legal factors influencing data backups* should be considered for the decision making.

In Office 365, several functions and interfaces for exporting data are implemented. A range of commercial solutions exist which also offer backup to the cloud itself or to local storage.

Upon deciding and carrying out data backups, your organization should consider the following aspects:

- What data or files are required to be exported and individually backed up?
- Which export functions are available?
- Do the export functions conform to legal, contractual, protection and other requirements?
- Is the backup storage medium (local or cloud) compliant with legal, contractual, protection and any other further requirements?
- Can the backed up data and files be recovered?

### 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 appropriate safeguards such as algorithms, protocols or key length, as insufficiently protected data can be viewed by unauthorized third parties. Office 365 offers different encryption options using encryption in a number of areas. Customers have the option of activating encryption with standard or individual encryption technologies, depending on the selected service.<sup>58</sup> The different encryption options are dependent on the service and must be evaluated by the customer on a case-by-case basis using the documentation and guidelines provided by Microsoft for Office 365.<sup>59</sup>

The following table illustrates the functionality provided by Office 365 to encrypt data at-rest, in-transit, and to securely manage secrets.

Table 10: Offerings regarding encryption and cryptography in Office 365

| Category                   | Details  | References  |
|----------------------------|--|---|
| Encryption of data-at-rest | Office 365 servers encrypt storing messaging data and other content using disk encryption (BitLocker using AES 256). | <a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption">https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption</a> |

<sup>58</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption>

<sup>59</sup> <https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption>



| Category | Details   | References   |
|----------|---|--|
|          | <p>BitLocker is also used, for example, for encrypting the mailbox data in Exchange Online. Microsoft provides information about the BitLocker configuration. Service level encryption encrypts all mailbox data at the mailbox level.</p> <p>All customer files in Microsoft SharePoint Online and OneDrive for Business are protected by unique, per-file keys. Files are only stored encrypted in the connected Azure Storage.</p> <p>Teams uses SharePoint Online for storing data that is encrypted with AES 256-bit keys.</p> <p>With Skype for Business Microsoft provides encryption as well using AES 256-bit keys for customer data on the web conferencing server.</p> | <p><a href="https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption-for-microsoft-365-services">https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption-for-microsoft-365-services</a></p> |

Encryption of data-in-transit

Office 365 encrypts connections using industry-standards such as AES and TLS/SSL.

<https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption-in-transit>

For email encryption, Office 365 provides various options: Office Message Encryption (OME), Secure/Multipurpose Internet Mail Extensions (S/MIME) and Information Rights Management (IRM). Office Message Encryption and Information Rights Management are based on Azure Rights Management (RMS). Encryption is used in Office 365 by default.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/exchange-online-uses-tls-to-secure-email-connections>

In Skype for Business data is shared via HTTPS during conferences.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption>

Azure Rights Management (Azure RMS) is part of Microsoft Information Protection (MIP). It includes encryption, identity, and authorization policies.

<https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption-for-microsoft-365-services>

The corresponding encryption is transparent for users.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ome>

<https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work>

| Category                                     | Details   | References   |
|--|---|--|
| Key management and own encryption mechanisms | <p>As a SaaS application, it is not possible to implement your own encryption mechanism.</p> <p>Microsoft provides a suitable key management for its online applications by its own trust center infrastructure. In that context, Microsoft Azure offers secure key management and storage for other cloud services with the Key Vault cloud service. As part of Azure Rights Management the customer can manage the encryption keys (the “bring your own key”, BYOK scenario).</p> <p>In addition, Office 365 supports customer key, which is based on service encryption and Double Key Encryption for full customer key control (but with the loss of some functionality).</p> | <p><a href="https://azure.microsoft.com/en-us/services/key-vault/">https://azure.microsoft.com/en-us/services/key-vault/</a></p> <p><a href="https://docs.microsoft.com/en-us/information-protection/deploy-use/operations-customer-managed-tenant-key">https://docs.microsoft.com/en-us/information-protection/deploy-use/operations-customer-managed-tenant-key</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/activate-rms-in-microsoft-365">https://docs.microsoft.com/en-us/microsoft-365/enterprise/activate-rms-in-microsoft-365</a></p> <p><a href="https://docs.microsoft.com/en-us/office365/securitycompliance/controlling-your-data-using-customer-key">https://docs.microsoft.com/en-us/office365/securitycompliance/controlling-your-data-using-customer-key</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption</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>60</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 Office 365 through Azure Active Directory for the management of users and groups in Office 365.<sup>61</sup> There are three general ways to realized hybrid accounts with different advantages and disadvantages.<sup>62</sup>

<sup>60</sup> SAML (Security Assertion Markup Language) is a standard authentication and authorization protocol

<sup>61</sup> <https://docs.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings>

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

- **Password hash synchronization (PHS):**<sup>63</sup> For PHS Azure Active Directory Connect synchronizes a hash of user password hashes from a customer on-premises Active Directory to Azure Active Directory, allowing Azure Active Directory to directly validate user passwords.
- **Pass-through authentication (PTA):**<sup>64</sup> PTA allows users to sign in on-premises and to cloud-based applications 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 to enforce on-premises Active Directory security and password policies.
- **Active Directory Federation Services (ADFS):**<sup>65</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>66</sup> as well as WS-Federation and OpenID Connect.<sup>67</sup> The information contained in the SAML<sup>68</sup> tickets can be configured according to organizational requirements or the requirements of each application.<sup>68</sup>

The user rights should be regularly checked and it should be ensured, that a SAML<sup>69</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>69</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>70</sup>

Furthermore, checking the correct ticket issuing process of SAML<sup>69</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.

<sup>63</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-pha>

<sup>64</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

<sup>65</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

<sup>66</sup> <https://docs.microsoft.com/en-us/azure/active-directory/develop/single-sign-on-saml-protocol>

<sup>67</sup> <https://docs.microsoft.com/en-us/azure/active-directory/develop/id-tokens>

<sup>68</sup> <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-saml-claims-customization>

<sup>69</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/02\\_ORP\\_Organisation\\_und\\_Personal/ORP\\_4\\_Identitaets\\_und\\_Berechtigungsmanagement\\_Editon\\_2021.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.html)  
[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bau-steine/ORP/ORP\\_4\\_Identit%C3%A4ts- und\\_Berechtigungsmanagement.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bau-steine/ORP/ORP_4_Identit%C3%A4ts- und_Berechtigungsmanagement.html)(German only)

<sup>70</sup> <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

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 Microsoft, including the requirements and expectations of Microsoft and its customers.<sup>71</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>72</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>73</sup> Microsoft also offers the SCoC Training Program to provide training to supplier employees.<sup>74</sup>

---

<sup>71</sup> <https://www.microsoft.com/en-us/procurement/msp-overview.aspx?activetab=pivot1:primaryr4>

<sup>72</sup> <https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr7>

<sup>73</sup> <https://www.microsoft.com/en-us/procurement/msp-overview.aspx?activetab=pivot1:primaryr4>

<sup>74</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>75</sup> which applies to federal authorities and that set 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 Office 365, 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>75</sup> can be implemented for Office 365. 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* 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 11: 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> |

<sup>75</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.2.1.03 Security Concept for External Cloud Services   | Subchapter 3.7 <i>OPS.2.2.A7 Drawing Up a Security Concept for Cloud Usage</i>  |
| NCD.2.1.04 Emergency and Continuity Management  | Subchapter 3.11 <i>OPS.2.2.A11 Drawing Up a Contingency Concept for Cloud Service</i><br>Subchapter 3.15 <i>OPS.2.2.A15 Ensuring the Portability of Cloud Services</i><br>Subchapter 3.16 <i>OPS.2.2.A16 Implementing In-House Back-ups</i> |
| NCD.2.2.01 Implementation of Security Requirements  | Subchapter 3.2 <i>OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage</i>   |
| NCD.2.2.02 Contractually Ensure Dealings with Subcontractors and Other External Third Parties       | Subchapter 3.8 <i>OPS.2.2.A8 Careful Selection of a Cloud Service Provider</i><br>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i>   |
| NCD.2.2.03 Ensure Jurisdiction by Contract  | Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i>   |
| NCD.2.2.04 Ensure Location by Contract  | Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i>   |
| NCD.2.2.05 Ensure that Disclosure Obligations and Investigative Powers are Contractually Guaranteed | Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i>   |
| NCD.2.2.06 Regulating the Termination of the Contractual Relationship                               | Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i><br>Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i>   |
| NCD.2.2.07 Ensure Data Return and Data Deletion at the Cloud Service Provider by Contract           | Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i><br>Subchapter 3.14 <i>OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship</i>   |

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

| Requirement | Links   |
|-------------|---|
|             | <p>Subchapter 3.9 <i>OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider</i></p> <p>Subchapter 3.17 <i>OPS.2.2.A17 Use of Encryption When Using the Cloud</i></p> |

## 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 Office 365 meets the requirements. The use of Office 365 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>76</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>77</sup> and security measures per cloud service used, which can be carried out by the cloud customer.<sup>78</sup> For example, the Microsoft Defender for Office 365<sup>79</sup> service complements the built-in virus protection<sup>80</sup> in Office 365 with functionalities such as safe attachments<sup>81</sup> and anomaly-based malware detection<sup>82</sup>.

## 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 Office 365 must create a security policy by the responsible persons. The *BSI's minimum standards for the use of external cloud services*<sup>83</sup> stipulate that the implementation of and compliance with the basic criteria according to the BSI's

<sup>76</sup> <https://info.microsoft.com/enterprise-cloud-strategy-ebook.html>

<sup>77</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide>

<sup>78</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/>

<sup>79</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/>

<sup>80</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-online-protection-overview>

<sup>81</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/turn-on-mdo-for-spo-odb-and-teams>  
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments>

<sup>82</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365>

<sup>83</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)



Cloud Computing Compliance Criteria Catalogue (C5)<sup>84</sup> must be specified as special security requirements for the cloud service provider in the security policy.

External auditors have determined compliance with the basic criteria according to the BSI's Cloud Computing Compliance Criteria Catalogue (C5)<sup>84</sup> for Office 365. The SOC 2 report on the audit can be viewed in the Service Trust Portal (STP)<sup>85</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>86</sup> and security measures per cloud service used, which can be carried out by the cloud customer.<sup>87</sup> For example, the Microsoft Defender for Office 365<sup>88</sup> service complements the built-in virus protection<sup>89</sup> in Office 365 with functionalities such as safe attachments<sup>90</sup> and anomaly-based malware detection<sup>91</sup>.

Microsoft Information Protection (MIP) can help to classify data and can be used to apply labels and to apply optionally protection safeguards. Labels can be applied automatically based on rules / conditions or manually.<sup>92</sup>

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*.

---

<sup>84</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)

<sup>85</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

<sup>86</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide>

<sup>87</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/>

<sup>88</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/>

<sup>89</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-online-protection-overview>

<sup>90</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/turn-on-mdo-for-spo-odb-and-teams>  
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments>

<sup>91</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365>

<sup>92</sup> <https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection>

## 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>93</sup> also requires an assessment by the institution of how a failure of Office 365 would affect the institution. In addition, it should be checked together with the responsible emergency officer whether the use of Office 365 affects the previous disaster management and thus the previous preventive / reactive measures can be adapted.

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.<sup>94</sup>

The preparation of a contingency concept is described in more detail in subchapter 3.11 *OPS.2.2.A11 Drawing Up a Contingency Concept for 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 In-House Backups*.

## 4.5 NCD.2.2.01 Implementation of Security Requirements

Before concluding a contract, it must be assessed whether Office 365 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*). Further, as part of the use of Office 365, 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>95</sup> and security measures per cloud service used, which can be carried out by the cloud customer.<sup>96</sup> For example, the Microsoft Defender for Office 365<sup>97</sup> service complements the built-in virus protection<sup>98</sup> in Office 365 with functionalities such as safe attachments<sup>99</sup> and anomaly-based malware detection<sup>100</sup>.

Microsoft permits audits by customers under terms and conditions set forth in the Microsoft Online Services Data Protection Addendum (DPA)<sup>101</sup>. If customer's audit requirements under the Standard

---

<sup>93</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>94</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-business-continuity-disaster-recovery>

<sup>95</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide>

<sup>96</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/>

<sup>97</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/>

<sup>98</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-online-protection-overview>

<sup>99</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/turn-on-mdo-for-spo-odb-and-teams>  
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments>

<sup>100</sup> <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365>

<sup>101</sup> <https://aka.ms/DPA>

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. Microsoft has published corresponding certifications, proofs or audit reports in the Service Trust Portal (STP)<sup>102</sup>. The current SOC 2 report on the audit of the Cloud Computing Compliance Criteria Catalogue (C5)<sup>104</sup> can also be accessed there.

#### 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>103</sup> External auditors have determined compliance with the basic criteria according to the BSI Cloud Computing Compliance Criteria Catalogue (C5)<sup>104</sup> for Office 365. The SOC 2 report on the audit can be viewed in the Service Trust Portal (STP)<sup>104</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>105</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*.

---

<sup>102</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

<sup>103</sup> <https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx>  
<https://www.microsoft.com/licensing/docs>

<sup>104</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>

<sup>105</sup> <https://aka.ms/DPA>

## 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 Office 365 services are operated.<sup>106</sup> In addition, Microsoft publishes statistics on law enforcement requests from around the world twice a year.<sup>107</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>108</sup> also requires the agreement of contractual penalties in the event of non-fulfilment.

Microsoft has an internal policy<sup>109</sup> on notifying affected parties during an information security incident. Information about obligations to inform subjects under the GDPR are published as well<sup>110</sup>. In addition, Microsoft publishes statistics on law enforcement requests from around the world twice a year.<sup>111</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*.

---

<sup>106</sup> <https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations>  
<https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations>

<sup>107</sup> <https://www.microsoft.com/en-us/corporate-responsibility/lerr>

<sup>108</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>109</sup> <https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification>

<sup>110</sup> <https://servicetrust.microsoft.com/ViewPage/GDPRBreach>

<sup>111</sup> <https://www.microsoft.com/en-us/corporate-responsibility/lerr>

## 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 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>112</sup>

## 4.12 NCD.2.3.01 Integrate ISMS

Office 365 as cloud service 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>114</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>113</sup> and the customer's risk analysis. Furthermore, this requirement obliges the cloud customer to review regularly this evidence for compliance with security requirements.

Office 365 holds several global and regional certifications<sup>114</sup>. In addition, audit reports and other compliance information, such as penetration tests<sup>115</sup>, are regularly published on Microsoft's website. The responsibility for defining the required certifications and verifying that Office 365 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*.

---

<sup>112</sup> <https://www.microsoft.com/en-us/trust-center/privacy/data-management>  
<https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction>

<sup>113</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>114</sup> <https://docs.microsoft.com/en-us/compliance/regulatory/offering-home>

<sup>115</sup> <https://servicetrust.microsoft.com/Documents/ComplianceReports>  
<https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3>

## 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 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.

For more information and links on Office 365 migration and integration, see the following subchapters 3.5 *OPS.2.2.A5 Planning the 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 subcontractor is replaced or a relevant cyber-attack occurs.

The current service status can be accessed online for Office 365 services.<sup>116</sup>

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>117</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>118</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.

---

<sup>116</sup> <https://status.office365.com/>

<sup>117</sup> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing>

<sup>118</sup> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

Further information on retrieving data from Office 365 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*.

## 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 subchapter 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 4.1)
- *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>119</sup>.

Microsoft publishes the generally applicable contract terms in the Licensing Portal<sup>120</sup>. Supplemental agreements should be provided by the contractor with whom the cloud is shared.

---

<sup>119</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>120</sup> <https://aka.ms/licensingdocs>

In Office 365, communication data is encrypted using industry standards such as AES and TLS/SSL, and data-at-rest is also encrypted using various methods.<sup>121</sup> Further information and links can be found in subchapter 3.17 *OPS.2.2.A17 Use of Encryption When Using the Cloud*.

With Intune, Microsoft provides Mobile Device Management (MDM) to secure mobile devices.<sup>122</sup> Together with conditional access, this can be used to restrict access to certain data or services in Office 365.<sup>123</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>121</sup> <https://docs.microsoft.com/en-us/compliance/assurance/assurance-encryption>

<sup>122</sup> <https://docs.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up>

<sup>123</sup> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>



# 5

## Microsoft's Responsibilities as a Cloud Service Provider

Microsoft shares responsibility with the customer for the security of Office 365 (see subchapter 2.1 *Shared Responsibility Model*). 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 Office 365.

The most important of these are:

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

Furthermore the feasibility of an "ISO 27001 certification based on IT-Grundschutz" for Office 365 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 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 security requirements 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 requirements, basic security checks and supplementary security analysis/risk analysis.  |
| Modelling   | Modellierung  | Analyzing a system or process to determine the possible vulnerabilities and the required protective requirements.   |
| Module  | Baustein  | Modules describe a specific item or process and draw together the relevant threats and applicable requirements.   |
| Requirement   | Anforderung   | Standard security requirement in IT-Grundschutz; Often used synonymously with “control”.  |

# 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><br><a href="https://www.microsoft.com/licensing/terms/welcome/welcomepage">https://www.microsoft.com/licensing/terms/welcome/welcomepage</a><br><a href="https://www.microsoft.com/licensing/docs">https://www.microsoft.com/licensing/docs</a><br><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><br><a href="https://aka.ms/DPA">https://aka.ms/DPA</a>       |
| Due Dilligence                                     | <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><br><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><br><a href="https://www.microsoft.com/en-us/investor/default.aspx">https://www.microsoft.com/en-us/investor/default.aspx</a><br><a href="https://www.microsoft.com/en-us/corporate-responsibility/lerr">https://www.microsoft.com/en-us/corporate-responsibility/lerr</a>  |
| Compliance Information                             | <a href="https://servicetrust.microsoft.com/">https://servicetrust.microsoft.com/</a><br><a href="https://www.microsoft.com/en-us/TrustCenter/Compliance">https://www.microsoft.com/en-us/TrustCenter/Compliance</a><br><a href="https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan">https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan</a><br><a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-home">https://docs.microsoft.com/en-us/compliance/regulatory/offering-home</a><br><a href="https://www.microsoft.com/en-us/corporate-responsibility/lerr">https://www.microsoft.com/en-us/corporate-responsibility/lerr</a> |
| Office 365 services, tools and further information | <a href="https://info.microsoft.com/enterprise-cloud-strategy-ebook.html">https://info.microsoft.com/enterprise-cloud-strategy-ebook.html</a><br><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><br><a href="http://status.office365.com/">http://status.office365.com/</a><br><a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health">https://docs.microsoft.com/en-us/microsoft-365/enterprise/view-service-health</a><br><a href="https://fasttrack.microsoft.com/">https://fasttrack.microsoft.com/</a>                         |
| Security Aspects Office 365                        | <a href="https://servicetrust.microsoft.com/">https://servicetrust.microsoft.com/</a><br><a href="https://docs.microsoft.com/en-us/microsoft-365/security/defender/overview-security-center">https://docs.microsoft.com/en-us/microsoft-365/security/defender/overview-security-center</a>  |

| Topic                            | Information Pointer  |
|----------------------------------|--|
|                                  | <p><a href="https://docs.microsoft.com/en-us/azure/active-directory/">https://docs.microsoft.com/en-us/azure/active-directory/</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models">https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models</a></p> <p><a href="https://docs.microsoft.com/en-us/office/office-365-management-api/">https://docs.microsoft.com/en-us/office/office-365-management-api/</a></p> <p><a href="https://docs.microsoft.com/en-us/azure/information-protection/activate-office365">https://docs.microsoft.com/en-us/azure/information-protection/activate-office365</a></p> <p><a href="https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption">https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption</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><a href="https://go.microsoft.com/fwlink/p/?LinkID=2162834&amp;clcid=0x407">https://go.microsoft.com/fwlink/p/?LinkID=2162834&amp;clcid=0x407</a><br/>(Whitepaper: How does Microsoft handle your data in the cloud?)</p>   |
| Microsoft Services Supplier List | <p><a href="https://go.microsoft.com/fwlink/?LinkID=2096306&amp;clcid=0x407">https://go.microsoft.com/fwlink/?LinkID=2096306&amp;clcid=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>   |
| 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