IT-Grundschutz Compliance on Dynamics 365

February 17, 2023

MICROSOFT DEUTSCHLAND GMBH

Table of contents

1 Executive Summary

Microsoft Dynamics 365 is a suite of intelligent business applications. Dynamics 365 unifies customer relationship management (CRM) and enterprise resource planning (ERP) capabilities by delivering new applications to help manage specific business functions. With Dynamics 365[1] Microsoft offers cloud services for managing customer relationships, keeping track of sales, marketing, analyzing and reporting business data.

Customers can select one or more regions from which Dynamics 365 is provided. In Germany, the two former regions (Germany Northeast and Germany Central) are deprecated and replaced by the new regions as part of the Azure global infrastructure, Germany West Central and Germany North[2]. Depending on customer preference, data can be stored in one or more regions, e.g. for availability reasons.

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has published (and continues to refine) the IT-Grundschutz methodology. This consists of an ISO 27001 compatible 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 standard (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 Dynamics 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*[3] as part of the Information Domain[4] is given on a per-requirement-basis in chapter 3. Chapter 4 gives information about implementing the BSI minimum standard "Minimum Standard on the Usage of External Cloud Services"[5] which addresses German federal authorities. Chapter 5 discusses Microsoft's responsibilities as a cloud service provider.

[1] https://www.microsoft.com/en-us/dynamics365/what-is-crm

[2] https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/

[3] 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)

[4] See Appendix A
Glossary of IT-Grundschutz-Terms for normative terms that have special meanings.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.html (German only)

2 Compliance Requirements

This Dynamics 365 workbook is based on the revised edition of the BSI IT-Grundschutz Compendium[6] from the year 2021. This edition includes the module *OPS.2.2 Cloud Usage*[7]. It distinguishes between the use of cloud services such as Dynamics 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 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 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.

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html (German only)

[7] 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)[8]

Aspect/Responsibility 🟧 Cloud Customer 🟨 Cloud Service Provider		Description
Security Concept	🟧	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. This document helps to establish a security concept for Dynamics 365.
Data classification & accountability	🟧	The value of data can only be determined by the customer, who should therefore identify, classify, and label their data. In Dynamics 365, the fields that hold personal or sensitive data can be classified.[9]
Client & end-point protection	🟧	Customers should clearly define the devices and clients that are permitted to access the cloud.
Identity and access management	🟨🟧	Dynamics 365 provides multiple options for identity and access management ranging from completely cloud-based (cloud-only identity)[10] to a hybrid approach[11] where user data is managed locally. With Azure Active Directory, the customer is able to configure password guidelines and multi-factor authentication[12] according to their specific guidelines. Note that Microsoft is responsible for providing a functional and secure identity and access management, but even for the cloud-only identity option, responsibility for the identity and access management still lies with the cloud user. Access to customer data by Microsoft employees can be controlled via Customer Lockbox[13].
Audits	🟨🟧	Dynamics 365 is continually audited by independent third parties due to the requirements of multiple compliance standards and certifications. The list of compliance standards for Dynamics 365 includes for example BSI C5, ISO 27001, ISO 27017and ISO 27018.[14]

[8] https://aka.ms/sharedresponsibility

[9] https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/developer/devenv-classifying-data-sensitivity and https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/developer/devenv-classifying-data

[10] https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview

[11] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/resilience-in-hybrid

[12] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

[13] Fehler! Linkreferenz ungültig. https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

[14] https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

Aspect/Responsibility 🟧 Cloud Customer 🟨 Cloud Service Provider		Description
Portability	🟨🟧	Customer data stored with Dynamics 365 can be exported and downloaded using Microsoft's tools or third party tools.
Disaster recovery	🟨🟧	Dynamics 365 has designed its services with the necessary precaution. The services keeps multiple live copies of customer data in multiple datacenters in the chosen region to ensure the contractual availability[15]. Customers should develop a disaster recovery plan, which should include backing up data.
Application level controls	🟨	For Dynamics 365 customers the general application level controls (e.g., antimalware and patch management) are provided by Microsoft.
Network controls	🟨	For Dynamics 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.

2.2 Modelling Dynamics 365

In order to remain IT-Grundschutz-compliant while utilizing Dynamics 365 services, the IT Security Concept needs to be updated to include Dynamics 365 in accordance with BSI Standard 200-2[16].

[15] https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/datacenter/new-datacenter-regions

[16] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html

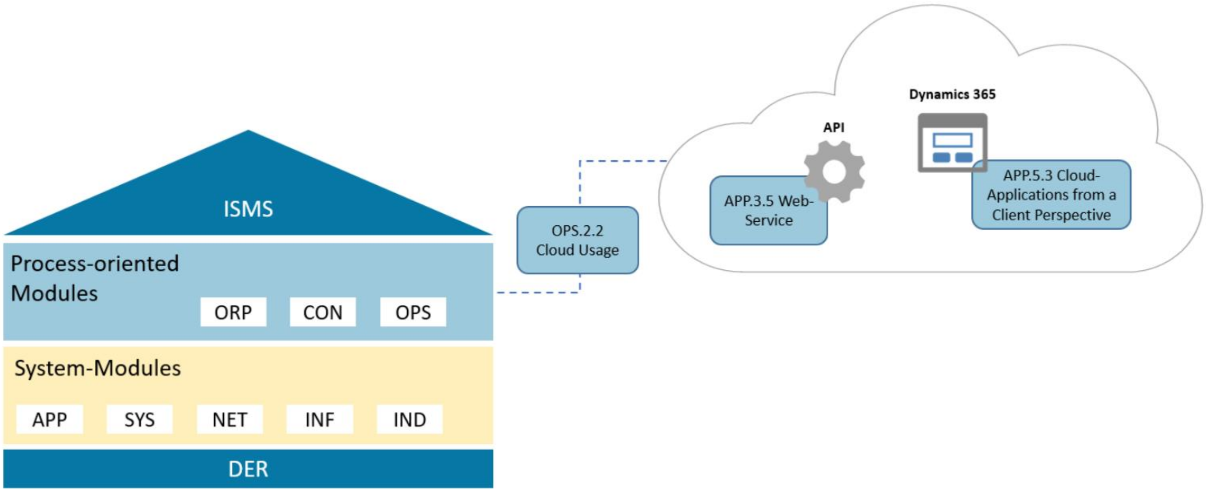

Figure 1 Multi-Layer model of IT-Grundschutz Compendium with Cloud Usage as SaaS

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 Dynamics 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*[17] defines the responsibilities of the customer across the entire cloud stack.

The module *OPS.2.2 Cloud Usage*[17] covers applications provided as a cloud service as well as their administration, which encompasses Office 365. The IT-Grundschutz Compendium[18] 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 Dynamics 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 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[19]. Figure 1 shows that module *OPS.2.2 Cloud Usage*[17] acts as interface between the customer's on premise environment and the customer's cloud environment.

Figure 1 presents the general structure of Dynamics 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.,

[17] 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)

[18] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html (German only)

[19] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html

your Internet and/or VPN connection) as part of the system with the appropriate modules for combination of network components and Internet service provider.

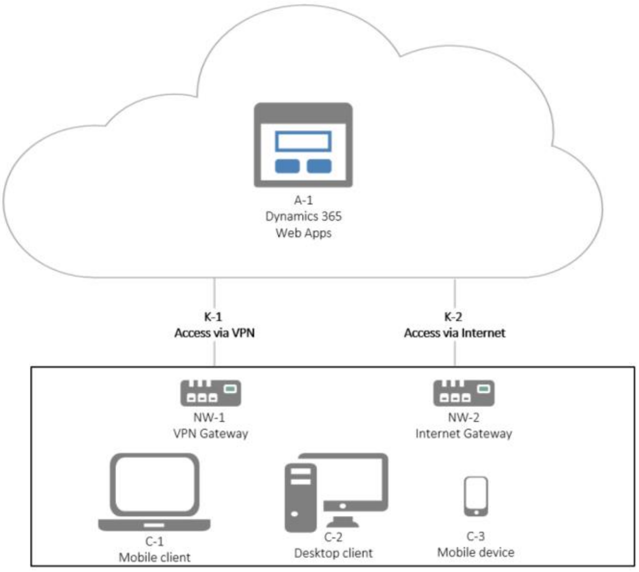

Figure 2 Modelling Dynamics 365 in an IT-Grundschutz network plan (example)

The requirements described in the following chapter provide additional information referencing the module *OPS.2.2 Cloud Usage*[17] and the applicable implementation notes or helpful online resources provided by Microsoft.

3 Implementation of Module OPS.2.2 Cloud Usage

The following chapter describes how all requirements from Module *OPS.2.2 Cloud usage*[20] can be implemented for Dynamics 365. In the revised IT-Grundschutz, the requirements were separated from implementation instructions. Implementation instructions for *OPS.2.2 Cloud usage*[21] contain 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 "Enterprise Cloud Strategy"[22] guide to help users define 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 Dynamics 365 within an organization need to be defined. Organizations are provided with details to aid the definition of security requirements with respect to the confidentiality, integrity and availability of information processed by Dynamics 365.
OPS.2.2.A3 Service Definition	Yes	This requirement considers additional practical requirements for Dynamics 365 regarding secure authentication,

[20] 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)

[21] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.html (German only)

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

Requirement	Supporting information available from Microsoft?	Description
for Cloud Services by the Customer		encryption and Dynamics 365 interoperability. Microsoft provides information on features, which may be used by the customer in securing data.
OPS.2.2.A4 Definition of Areas of Responsibility and Interfaces	Yes	All responsibilities and points of interaction must be documented. The responsibilities of each party are recorded in the Shared Responsibilities document.[23] Microsoft offers several methods of connecting to and managing Microsoft Dynamics 365.
OPS.2.2.A5 Planning a Secure Migration to a Cloud Service	Yes	Microsoft provides detailed information on security aspects to consider when migrating to Dynamics 365 online services with the workbook "Cloud Migration Simplified"[24].
OPS.2.2.A6 Planning the Secure Integration of Cloud Services	Yes	This requirement contributes to the secure integration of Dynamics 365 into customer's environment. Microsoft offers different methods to integrate Dynamics 365 with local environments.
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, Dynamics 365 addresses most of the technical threats and mitigations mentioned in the requirement to support organization in creating a security concept for Dynamics 365.
OPS.2.2.A8 Careful Selection of a Cloud Service Provider	Yes	Microsoft offers guidance for the evaluation of Dynamics 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.
OPS.2.2.A10 Secure Migration to a Cloud Service	Yes	This requirement covers execution of the previously planned migration. Microsoft provides tools to assist with migrating current resources to Dynamics 365.
OPS.2.2.A11 Drawing Up a Contingency Concept for a Cloud Service	Yes	The disaster recovery is developed individually for Dynamics 365. General guidelines and information are provided.

[23] https://aka.ms/sharedresponsibility

[24] https://azure.microsoft.com/en-us/resources/cloud-migration-simplified/

Requirement	Supporting information available from Microsoft?	Description
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 Dynamics 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 Dynamics 365 upon termination of a Microsoft Dynamics 365 subscription are provided, including cancellation and data deletion policies.
OPS.2.2.A15 Ensuring the Portability of Cloud Services	Yes	Portability aspects are addressed for Dynamics 365 using examples.
OPS.2.2.A16 Implementing In-House Backups	Yes	This must be initiated by the organization; either directly or using a third-party service. Dynamics 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 Dynamics 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 Azure Active Directory, which can be used for the management of users and groups in Dynamics 365.
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 a total of three compliance workbooks, handling compliance for IT-Grundschutz on cloud services. They are available for Microsoft Dynamics 365, Microsoft 365 and Azure. As typical for cloud, Microsoft has implemented these services by leveraging synergies between online services, improving resource utilization on both sides. These synergies and common themes are also reflected in the great similarities within the three workbooks. In this way, customers using IT-Grundschutz for more than one of these services can benefit greatly from the similarities and synergies of these services by addressing certain topics in general and only adding certain specificities of the services. For example, Azure Active Directory can be used for identity and access management for Azure, Dynamics 365 and Microsoft 365.

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

In a cloud 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.[25] The workbook also covers different migration scenarios for Dynamics 365.

The customer must decide which applications or services are to be migrated onto Dynamics 365. This may include partial integration of services (e.g., using Dynamics 365 online but the Exchange service on-premises[26]) or the integration of on-premises operational services (e.g., integration of Active Directory on-premises).

Depending on the chosen Dynamics 365 plan[27], 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.

Table 3: Different complexities of Dynamics 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 and Active Directory)
Two-factor authentication via Microsoft features only	Alternate two-factor authentication with Azure Active Directory 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

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

[26] https://docs.microsoft.com/en-us/power-platform/admin/connect-exchange-server-on-premises

[27] https://dynamics.microsoft.com/en-us/pricing/

Low complexity and integration	High complexity and integration
High dependency and availability requirements for the Internet connection	Online and offline processing of business information with synchronization
Web based Dynamics 365 applications	Web based and local installation of Dynamics 365 applications

When matching your requirements against Dynamics 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 usage is defined based on the strategy (see subchapter 3.1 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage*). The security policy covers all security requirements, which need to be established in the organization. This includes all security requirements for the provider and the defined level of protection of the cloud service regarding confidentiality, integrity and availability. 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 Dynamics 365 specific information per cloud service to assist organizations in establishing their security policy regarding data privacy, compliance, transparency and other individualized customer controls.[28] 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.

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

Compliance Requirement	Implementation in Dynamics 365	References
Identity & Access Management	Dynamics 365 is deployed on Microsoft's Azure platform and uses Azure Active Directory to manage identities and authentication. Dynamics 365 supports cloud-only and hybrid identity. Hybrid identities are managed on-premises and synchronized (with or without password hash) to Azure Active Directory. Azure Active Directory provides different ways to use hybrid identities for Dynamics 365:	https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis https://docs.microsoft.com/en-us/azure/active-directory/hybrid/ https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs

[28] For example: https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/security-concepts https://docs.microsoft.com/en-us/dynamics365/fraud-protection/data-processing-protection

Compliance Requirement	Implementation in Dynamics 365	References
	• Password hash synchronization (PHS) synchronizes on-premises accounts including a hash of the password hash into Azure Active Directory. • Pass-through authentication (PTA) allows a user to login to Dynamics 365 using their on-premises credentials and Dynamics 365 then validates the password against the on-premises Active Directory. • Active Directory Federation Service is a trust between Azure Active Directory and an on-premise Active Directory. The users are authenticated against the on-premises Active Directory. Dynamics 365 supports role based access control and provides several built-in roles. Besides internal accounts of an institution or company Dynamics 365 allows to add and manage guest accounts and external partners (Business-to-Business, B2B). Dynamics 365 supports several Multi Factor Authentication (MFA) methods, e.g. via mobile app, smart card or certain third party MFA solutions. Privileged Identity Management (PIM) allows to manage and monitor administrative access to Dynamics 365. For example, with PIM privileged access can be limited in time. Administrators can set a timeout for inactivity, which causes an automatically log out, for each of their Dynamics 365 for Customer Engagement instances. The application logs the user off when the inactivity session expires. The conditional access feature of Azure Active Directory can also be used for Dynamics 365. With this feature, Dynamics 365 customer can add automated access control decisions for accessing data and apps in Dynamics 365 that are condition based.	https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/security-roles-privileges https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/invite-users-azure-active-directory-b2b-collaboration https://docs.microsoft.com/en-us/dynamics365/business-central/ui-define-granular-permissions https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/multifactor-authentication https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/user-session-management https://docs.microsoft.com/en-us/power-platform/admin/user-session-management https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Compliance Requirement	Implementation in Dynamics 365	References
	Mobile device management (MDM) or Intune can be used to secure and configure mobile devices that are allowed to access Dynamics 365.	https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules https://docs.microsoft.com/en-us/intune/what-is-intune
Asset Management	Customers of Dynamics 365 can classify their data by tagging. For example, this classification can be applied on business data that is stored in table fields of the database.	https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/developer/devenv-classifying-data
Protection of Data	Customer isolation within Dynamics 365 is implemented by several technical means. This includes logical isolation using role based access control. In Dynamics 365, access can be restricted down to the fields using the so-called field-level security. 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 data-at-rest in customer engagement apps (Dynamics 365 Sales, Dynamics 365 Customer Service, Dynamics 365 Field Service, Dynamics 365 Marketing, and Dynamics 365 Project Service Automation) cell level encryption is used for a set of default tables that contain sensitive information, such as user names. This encryption cannot be deactivated. Microsoft continuously tests and monitors the security of Dynamics 365 and takes actions accordingly. Corresponding reports, e.g. for penetration tests or audits, can be accessed using the trust center. The service health of Dynamics 365 can be viewed on the Dynamics 365 Service health page in the Microsoft 365 admin center. Dynamics 365 has detailed logging and monitoring functionality implemented. The logs are accessible in a unified and searchable audit log that allows to view	https://docs.microsoft.com/en-us/power-platform/admin/multiple-online-environments-tenants https://docs.microsoft.com/en-us/power-platform/admin/field-level-security https://docs.microsoft.com/en-us/power-platform/admin/data-encryption https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-encryption-in-microsoft-dynamics-365 https://docs.microsoft.com/en-us/compliance/regulatory/offering-home https://docs.microsoft.com/en-us/power-platform/admin/notifications-explained#service-health-dashboard https://docs.microsoft.com/en-us/power-platform/admin/enable-use-comprehensive-auditing https://docs.microsoft.com/en-us/power-platform/admin/audit-data-user-activity

Compliance Requirement	Implementation in Dynamics 365	References
	user and administrator activity in Dynamics 365.	
Compliance and Audit	Microsoft invested in the processes to meet the requirements of the Model Clauses for the transfer of personal data processors. Dynamics 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 Dynamics 365 by the customer. This includes an accountability readiness checklist, a data protection impact assessment 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. Dynamics 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. Microsoft provides detailed guidelines how to achieve security and compliance with legal or regulatory standards with Dynamics 365. With Dynamics 365 Fraud Protection personal data can be identified, deleted or exported. Microsoft provides an overview about its data storage locations for Dynamics 365.	https://docs.microsoft.com/en-us/compliance/regulatory/offering-EU-Model-Clauses https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-dynamics https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Dynamics365 https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics-windows https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-arc-azure-dynamics-windows 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/powerapps/developer/data-platform/auditing-overview https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance https://docs.microsoft.com/en-us/power-platform/admin/audit-data-user-activity https://docs.microsoft.com/en-us/dynamics365/fraud-protection/security-compliance https://www.microsoft.com/en-us/trust-center/privacy/data-location https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-

Compliance Requirement	Implementation in Dynamics 365	References
	Compliance Manager is a workflow-based risk assessment tool to track, assign and verify compliance activities related to Dynamics 365. It provides a centralized dashboard for standards, regulations and implementation including results for service assessments.	and-regulatory-reqs-using-microsoft-cloud
Backup and Archiving	Manual or automated backups of data stored in customer engagement apps (Dynamics 365 Sales, Dynamics 365 Customer Service, Dynamics 365 Field Service, Dynamics 365 Marketing, and Dynamics 365 Project Service Automation) can be performed. Backups are possible for Azure SQL databases, where Dynamics 365 data is stored. Data resiliency and recoverability can be used from the built-in features of the Azure platform, where Dynamics 365 runs, to maximize reliability and minimize negative effects on customers. This is achieved through a combination of physical infrastructure and software solutions. Additional backup possibilities for Dynamics 365 are planned for following releases (e.g. download of data backups in Dynamics 365). In the Microsoft Dynamics 365 (online) data center, a duplicate and synchronized (alternative) copy of the stored data is managed on another server. In the event of an incident in the data center that no longer allows access to the data, it is possible to switch to alternative location, minimizing the severity of business interruption. Once the problem is resolved, service access to the primary location can be restored. Otherwise third-party solutions for backups are also available.	https://docs.microsoft.com/en-us/power-platform/admin/backup-restore-environments https://docs.microsoft.com/en-us/azure/sql-database/sql-database-automated-backups https://azure.microsoft.com/en-us/features/resiliency/ https://azure.microsoft.com/en-us/resources/resilience-in-azure-whitepaper/

Compliance Requirement	Implementation in Dynamics 365	References
Threat Protection	Dynamics 365 runs on Azure, which has a basic level of Distributed Denial of Service (DDoS) protection in place automatically and for free, which is sufficient for common network level attacks. A subscription for the standard DDoS protection provides protection against more sophisticated attacks and provides support of DDoS experts for customization and during DDoS attacks. Azure provides a free real-time malware protection to identify and remove several kind of malware like viruses or spyware, which Dynamics 365 customer can use in their Azure subscription.	https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware
Change Management	Microsoft provides a guideline how to stay up to date with the fast development within Dynamics 365 and how to get latest update information. Thereby, Microsoft provides a roadmap of ongoing and planned updates. Finance and Operations offers an internal change tracking feature in Microsoft Dynamics 365.	https://dynamics.microsoft.com/en-us/roadmap/overview/ https://docs.microsoft.com/en-us/dynamics365-release-plan/2021wave2/ https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/data-entities/entity-change-track

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 added value 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 Dynamics 365[29]. 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.

[29] https://docs.microsoft.com/en-us/dynamics365/

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 Dynamics 365	References
Choice of secure authentication methods	Dynamics 365 offers Azure Active Directory features including a subset of Azure Multi-Factor-Authentication (MFA). Role-based access control is available for controlling cloud services via the Microsoft Azure Portal. Azure Active Directory enables customers to provision role-based access rights within the cloud or as hybrid solution with your local active directory. The conditional access feature allows to restrict the access to services based on customer definable conditions like source IP, device user or the authentication method. Intune can be used to secure and configure mobile devices that are allowed to access Dynamics 365.	https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/set-up-multi-factor-authentication https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing https://docs.microsoft.com/en-us/dynamics365/unified-operations/dev-itpro/sysadmin/role-based-security https://docs.microsoft.com/en-us/power-platform/admin/security-roles-privileges https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/dynamics365/mobile-app/secure-manage-phones-tablets
Further considerations of security aspects	Dynamics 365 offers encryption for data at rest and in transit (see also the *Confidentiality* section in the table within subchapter 3.17 *OPS.2.2.A17 Use of Encryption When Using the Cloud*). 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. Data resiliency and recoverability can be used from the built-in	https://docs.microsoft.com/en-us/power-platform/admin/data-encryption https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365 https://docs.microsoft.com/en-us/azure/security/fundamentals/isolation-choices https://azure.microsoft.com/en-us/features/resiliency/

Compliance Requirement	Implementation in Dynamics 365	References
	features of the Azure platform, where Dynamics 365 runs, to maximize reliability and minimize negative effects on customers. This is achieved through a combination of physical infrastructure and software solutions. Also, regular backups are performed (see subchapter 3.16 OPS.2.2.A16 Implementing In-House Backups) Additionally access can be restricted with IP address rules in Dynamics 365.	https://azure.microsoft.com/en-us/resources/resilience-in-azure-whitepaper/ https://docs.microsoft.com/en-us/dynamics365/admin/backup-restore-instances https://docs.microsoft.com/en-us/power-platform/admin/backup-restore-environments https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules
Client software interoperability	Dynamics 365 offers a variety of functionalities via Dynamics 365 APIs. All of the Dynamics 365 Management APIs are consistent in design and implementation with the current suite of Dynamics 365 REST APIs, using common industry-standard approaches, including OAuth v2, OData v4, and JSON.	https://docs.microsoft.com/en-us/rest/dynamics365/

3.4 OPS.2.2.A4 Definition of Areas of Responsibility 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.[30] For further information on the shared responsibility model refer to 2.1 Shared Responsibility Model at the beginning of this document.

After the responsibilities are identified it is important to clearly define 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.

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

The development of a migration concept forms an important foundation for a secure and sustainable migration to the cloud. Above all, organizational regulations and task assignments must be taken into account. Including responsibilities, test and transfer procedures, which are of particular importance to ensure resilient and secure business operation. In the 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 Dynamics 365 must be appropriately planned.

Microsoft offers a workbook[31] to support customer 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.

Microsoft provides support for migrating from online tenant to online tenant[32] or from on-premises solutions to Dynamics 365 online services.[33] Additionally, Microsoft offers FastTrack for valid subscriptions aiding the migration process[34].

[30] https://aka.ms/sharedresponsibility
https://azure.microsoft.com/mediahandler/files/resourcefiles/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20Onboarding%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/

[31] https://azure.microsoft.com/en-us/resources/cloud-migration-simplified/

[32] https://docs.microsoft.com/en-us/power-platform/admin/move-environment-tenant

[33] https://dynamics.microsoft.com/en-us/cloud-migration/

[34] https://docs.microsoft.com/en-us/dynamics365/get-started/fasttrack/customer-engagement/microsoft-fasttrack-dynamics-365

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

In addition to planning a secure migration (see subchapter 3.5 *OPS.2.2.A5 Planning a Secure Migration to a Cloud Service*), the secure integration of Dynamics 365 is essential for secure, continuous IT operations. This requirement considers aspects beyond planning the migration.

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

- Required adaptions of the existing IT landscape
- Suitability of existing interfaces (e.g., proxy) for Dynamics 365 use
- Definition of the administration model for the cloud based Dynamics 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 Dynamics 365 integration 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[35]
- Use of third-party tools for Dynamics 365

To secure the connection between cloud services and on-premises a Cloud Access Security Broker (CASB) like Microsoft's Cloud App Security[36] 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 cloud services in use.

Additionally, a learning platform is offered, where many specific supporting contents can be found for training.[37]

With the Evergreen approach, Microsoft aims to keep all Dynamics 365 services and the entire Azure 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.[38]

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 Dynamics 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.

[35] https://docs.microsoft.com/en-us/dynamics365/customer-engagement/developer/data-export-service

[36] https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

[37] https://docs.microsoft.com/en-us/learn/azure/

[38] https://dynamics.microsoft.com/en-us/business-applications/product-updates/
https://dynamics.microsoft.com/en-us/roadmap/overview/

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

While there is no generic template for your organization's requirements, Microsoft Dynamics 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 Dynamics 365	References
Pre-emptive or compulsorily contract ending	Contract ending is addressed in detail within a dedicated requirement.	Subchapter 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*
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 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*
Missing knowledge about physical data storage location	Dynamics 365 provides an overview of data centers within regions and allows to choose the geolocation within a subscription. Data will then be maintained within the data centers located in this geolocation. All data centers, where Dynamics 365 is hosted, are physically protected against unauthorized access and several other threats.	https://docs.microsoft.com/en-us/power-platform/admin/new-datacenter-regions https://www.microsoft.com/en-us/trust-center/privacy/data-location https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure
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 Dynamics 365. Together with conditional access this can be used to restrict access to certain data or services within Dynamics 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.	https://docs.microsoft.com/en-us/dynamics365/mobile-app/secure-manage-phones-tablets https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
Unauthorized access (e.g. by cloud provider admins or other cloud customers)	By default Microsoft personnel has no access to customer data. When access is required, Multi Factor Authentication is mandatory and least privilege and	https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

Cloud-specific threats	Conditions on Dynamics 365	References
	permanent logging and monitoring is applied. Isolation between customers (multitenancy) is realized on access, 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. To prevent unauthorized access to customer data, it is encrypted or can be encrypted at rest and during transfer, including transfer between Dynamics 365 data centers, using state of the art protocols and cryptography such as AES and TLS.	https://www.microsoft.com/en-us/trust-center/privacy/data-access https://docs.microsoft.com/en-us/azure/security/fundamentals/isolation-choices https://docs.microsoft.com/en-us/power-platform/admin/data-encryption https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365

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 added value 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 of time during and after migration.

The basic aspects must be investigated and appropriate answers need to be obtained before the offers are evaluated.[39] 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.[40]

[39] 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/

[40] https://www.microsoft.com/en/trust-center/compliance/due-diligence-checklist

Microsoft provides information for a thorough evaluation of Dynamics 365.[41] The following table lists information which should be gathered and assessed ahead of migrating to the cloud.

Table 7: Consideration before migration to Dynamics 365

Consideration to be made	Conditions on Dynamics 365	References
Publicly available information about the provider (reputation, ratings and rankings, core business, performance, cloud experience)	Cloud belongs to the core businesses of Microsoft and Microsoft belongs to the best rated cloud services providers according to various ratings. Dynamics 365 is constantly extended and updated. Microsoft publishes roadmaps and further information about planned updates for Dynamics 365 on their webpage. Exchange with other customer is possible in the Microsoft Tech Community to receive further information about Dynamics 365. Microsoft provides customer stories on their use of Dynamics 365. Microsoft provides the Service Health feature within Microsoft 365 admin center, which shows the current status of services, like Dynamics 365. Customers can check the service status page for known issues preventing customers from logging into their tenant.	https://www.microsoft.com/en-us/investor/default.aspx https://dynamics.microsoft.com/en-us/business-applications/product-updates/ https://docs.microsoft.com/en-us/dynamics365-release-plan/2021wave2/ https://techcommunity.microsoft.com/ https://dynamics.microsoft.com/en-us/customer-stories/ https://docs.microsoft.com/en-us/power-platform/admin/notifications-explained#service-health-dashboard
Due-Diligence	Microsoft provides a checklist for Due-Diligence activities. Microsoft provides a wide set of compliance offerings that can be used as a baseline for Due-Diligence activity.	https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist https://docs.microsoft.com/en-us/compliance/regulatory/offering-home
Access through cloud provider or third parties	Microsoft personnel has no access by default. When access is required, MFA is mandatory and least privilege and permanent logging and monitoring is applied. The customer isolation implemented in Dynamics 365 ensures that different customers cannot access the data of	https://www.microsoft.com/en-us/trust-center/privacy/data-access https://docs.microsoft.com/en-us/power-platform/admin/multiple-online-environments-tenants

[41] https://www.microsoft.com/en-us/trustcenter/guidance/evaluate

Consideration to be made	Conditions on Dynamics 365	References
	others, even if they are computed or stored on the same hardware. Data at rest and in transit is encrypted in Dynamics 365, so unauthorized parties cannot access the information contained.	https://docs.microsoft.com/en-us/power-platform/admin/data-encryption https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-encryption-in-microsoft-dynamics-365
Installation of additional software	Dynamics 365 can be used with the browser or with local installations of appropriate applications. Access to the later varies across subscription types.	https://docs.microsoft.com/en-us/dynamics365/customer-engagement/on-premises/system-requirements-required-technologies
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://aka.ms/dynamics_365_international_availability_deck https://www.microsoft.com/en-us/trust-center/privacy/data-location
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. This program assures that the rules and processes implemented in Microsoft are also 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.	https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List) https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426 (Microsoft Commercial Support Subcontractors) https://www.microsoft.com/en-us/trust-center/privacy/data-access https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx
Consideration of contractual basis and regulations	The Service Level Agreements and Microsoft's Online Services Terms are the standard stipulations governing the use of Dynamics 365 services. They are published on the webpage and accessible	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

Consideration to be made	Conditions on Dynamics 365	References
	without Microsoft subscription or Dynamics 365 account.	
Evaluation of services including warranties	Services descriptions, documentation and pricing information are published on the webpage of each service.	https://dynamics.microsoft.com/en-us/pricing/

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 Dynamics 365.The previously defined requirements must be considered, and at least the following points must be answered with respect to Dynamics 365.

Table 8: Content to be considered for drafting of contract

Contract documents	Conditions on Dynamics 365	References
Physical location of the services and cloud service provider	The cloud services are run from data centers located in the region that was chosen by the customer. 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 Dynamics 365, among others, will take place exclusively within Europe.	https://aka.ms/dynamics_365_international_availability_deck https://www.microsoft.com/en-us/trust-center/privacy/data-location https://www.microsoft.com/en-us/TrustCenter/Privacy/dynamics365-finance-operations https://azure.microsoft.com/en-us/global-infrastructure/regions/ https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098
Supervision of service delivery	Microsoft provides the Service Health feature within the Microsoft 365 admin center, which shows the current status of services, such as Dynamics 365. Customers can check the service status page for known issues	https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/check-online-service-health

Contract documents	Conditions on Dynamics 365	References
	without having to logging into their tenant.	
Subcontractors and third parties involved with service delivery	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.	https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List) https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426 (Microsoft Commercial Support Subcontractors) https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx
Rules concerning the personnel of the cloud service provider	The personnel (both internal and external) employed by Microsoft have all required competencies and are cleared according to internal policies.	https://www.microsoft.com/en-us/corporate-responsibility/empowering-employees https://docs.microsoft.com/en-us/compliance/assurance/assurance-human-resources
Rules concerning communication channels and contact persons	The account manager is the primary contact point for customer. The main communication channel for Dynamics 365 is the support menu within the administrative interface. Additional means of contacting Microsoft is the support webpage.	https://dynamics.microsoft.com/en-us/contact-us/
Rules concerning processes, working procedures and responsibilities	Dynamics 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). The division of responsibilities, processes and procedures are generally defined in the particular agreements. Furthermore, multiple possibilities for support, service monitoring and	https://www.microsoft.com/en-us/licensing/product-licensing/products https://docs.microsoft.com/en-us/compliance/regulatory/offering-home Subchapter 2.1 Shared Responsibility Model https://dynamics.microsoft.com/en-us/business-applications/product-updates/

Contract documents	Conditions on Dynamics 365	References
	further information exchange are offered to the customer for Dynamics 365. 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.	https://docs.microsoft.com/en-us/dynamics365-release-plan/2021wave2/
Provisions for ending the contractual agreement	Dynamics 365 is offered on an annual subscription basis. Early termination may be possible.	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services https://products.office.com/en-us/business/compare-more-office-365-for-business-plans Subchapter 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*
Secure deletion of data by the cloud service provider	When a paid subscription is terminated or ends, the Dynamics 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. Physical storage media will be securely destroyed on-site at the end of their service life.	https://www.microsoft.com/de-de/trustcenter/Privacy/You-are-in-control-of-your-data (in German) https://www.microsoft.com/en-us/trust-center/privacy/data-management https://aka.ms/DPA
Emergency preparedness	Dynamics 365 has defined rules for continuation of services to the level set out by the SLA. Corresponding safeguards include the geographical separation of the data centers and the continuous replication of data between them.	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services https://www.microsoft.com/en-us/trust-center/privacy/data-location

Contract documents	Conditions on Dynamics 365	References
Legal requirements	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.	https://www.microsoft.com/en-us/corporate-responsibility/lerr
Rules governing checks and audits	Dynamics 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. Cloud users have the ability to carry out penetration tests against their cloud services without notifying Microsoft, when the corresponding rules of engagement are adhered. The main restriction is that no Denial of Service (DoS) tests are allowed. Also other Dynamics 365 customers must not be disturbed by penetration tests.	https://docs.microsoft.com/en-us/compliance/regulatory/offering-home https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement
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 Adden-*	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

Contract documents	Conditions on Dynamics 365	References
	dum 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 also gives information on how cloud-customer can handle the GDPR requirements. Furthermore, Microsoft signed up to the EU Cloud Code of Conduct (EU Cloud CoC) and therefore certifies that their cloud services adhere to the rigorous European data protection requirements.	

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

This requirement focusses on the actual migration to a cloud service according to the considerations given in the migration security concept (see subchapter 3.5 *OPS.2.2.A5 Planning a Secure Migration to a Cloud Service*) 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 Dynamics 365.[42]

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

A business continuity concept should be developed as a preventive security safeguard for Dynamics 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[43]. Instead, this requirement covers the individual plan for an organization in the event of loss of the cloud service itself

[42] https://www.microsoft.com/en-us/fasttrack/
https://docs.microsoft.com/en-us/dynamics365/fasttrack/

[43] https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

or access to it. It also addresses situations where the applicable service levels do not cover the requirements.

Should the online service 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 Dynamics 365. In this case, a Dynamics 365 plan including desktop software needs to be chosen.

When using Dynamics 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 Internet service provider or provision for a redundant connection.

Furthermore, business continuity plans concerning the relevant business processes which depend on Dynamics 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).

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, both by the customer as well as the cloud service provider.

Table 9: Requirements to preserve information security

Requirements	Details on Dynamics 365	References
Documentation and policies (for example instruction manuals and procedures) need to be updated at regular intervals.	The review and update of policies at regular intervals is part of an effective ISMS. This process should be implemented within the document management process. Microsoft provides evidence of compliance to this requirement through certifications. The certificates can be accessed via the Service Trust Portal (STP).	https://servicetrust.microsoft.com/
The rendering of services should be checked regularly.	Dynamics 365 includes an integrated SLA Monitoring system ("Service Health") which enables checking the compliance of the services via the Microsoft 365 admin center. This includes receiving service notification on a mobile device.	https://docs.microsoft.com/en-us/power-platform/admin/notifications-explained#service-health-dashboard https://www.microsoft.com/licensing/terms/welcome/welcomepage

	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.	https://www.microsoft.com/en-us/procurement/contracting-terms-conditions.aspx
Cloud service provider supplies security certificates	Dynamics 365 offers, in this case, a variety of publications and verifications as well as applicable certifications. This can be verified by a user of Dynamics 365 on the public website as well as in the audit results which can be viewed in the Service Trust Portal (STP).	https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx https://docs.microsoft.com/en-us/compliance/regulatory/offering-home https://servicetrust.microsoft.com/Documents/ComplianceReports
Coordination talks should be held regularly between the cloud service provider and the organization using the cloud.	Dynamics 365 offers a variety of options for support and gathering of status information (e.g. with Service Health via Microsoft 365 admin center). Customers will be contacted in the event of significant service disruption.	https://docs.microsoft.com/en-us/power-platform/admin/notifications-explained#service-health-dashboard https://dynamics.microsoft.com/en-us/support/
Exercises and tests to simulate the response to system failures should be planned and performed.	This requirement is the responsibility of the customer. Dynamics 365 has defined rules for the continuation of services to the level set out by the SLA.	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services
Ensure proper administration of cloud services	This requirement is the responsibility of the cloud user. 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. The administration of Dynamics 365 is centralized in the Dynamics 365 admin center. Documentation for administrators is available.	https://docs.microsoft.com/en-us/dynamics365/marketing/dynamics-365-admin-center https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/security-architecture https://docs.microsoft.com/en-us/dynamics365/
Ensuring interoperability of cloud services	When using multiple cloud services, interoperability tests should be performed for each service to ensure proper collaboration between the different cloud services. Dynamics offers for example interoperability for Outlook.	https://www.microsoft.com/en-us/legal/interoperability/default.aspx https://docs.microsoft.com/en-us/dynamics365/outlook-addin/admin-guide/dynamics-365-for-outlook

		https://docs.microsoft.com/en-us/dynamics365/get-started/fasttrack/customer-engagement/microsoft-fasttrack-dynamics-365 Subchapter 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*
Proper execution of data backups	A proper performance of data backup must be ensured so that no critical business processes can be endangered by a failure. This requirement is the responsibility of the cloud user. 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 decided upon, the customer must ensure that all the requirements for backup and data security are fulfilled. Dynamics 365 backs up all instances continuously and backups are retained for 28 days. The cloud user can perform data backups on-demand on their responsibility.	https://docs.microsoft.com/en-us/dynamics365/admin/backup-restore-instances Subchapter 3.16 *OPS.2.2.A16 Implementing In-House Backups*
Control of technical safeguards to prevent the use of unauthorized services	This requirement is the responsibility of the cloud user. 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.	https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task https://docs.microsoft.com/en-us/cloud-app-security/
Performing audits, security checks, penetration tests or vulnerability analyses	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 (DoS) tests are allowed and that no other customers must be disturbed by the tests performed. Microsoft carries out penetration tests and vulnerability scans against	https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement https://servicetrust.microsoft.com

and audits of Dynamics 365. Reports are made available to cloud users at the Service Trust Portal.

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.

Dynamics 365 as well as Azure are continually audited, due to the requirements of multiple international and national compliance standards and certifications. The list of compliance standards for Dynamics 365 includes BSI C5, ISO 27001, ISO 27017 and ISO 27018[44] (see chapter 5 for more 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)[45], which provides direct access to many of the compliance reports and attestations.

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"[46] to its customers.

[44] https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

[45] https://servicetrust.microsoft.com/

[46] 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

In Dynamics 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 (See subchapter 3.16 *OPS.2.2.A16 Implementing In-House Backups*).

By default, Dynamics 365 data can be exported for 90 days upon contract termination. Customer data will be deleted within 180 days after the end of the agreed usage period or the cancellation of the user agreement.[47]

When terminating the Dynamics 365 contract as an online service, your organization should, among other things, ensure the following:

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

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.

Dynamics 365 supports various methods of data migration:

1. Using Dynamics 365 APIs, allowing access to customer data.[48]
2. Using the add-on service Data Export (e.g. for Customer Engagement) to replicate data from Dynamics 365 Germany to a Microsoft Azure SQL database.[49]
3. Migrating data to on-premises components.[50]
4. Use of third-party tools for Dynamics 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.[51] 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.[52]

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

[47] https://www.microsoft.com/en-us/TrustCenter/Privacy/You-are-in-control-of-your-data
https://www.microsoft.com/en-us/trust-center/privacy/data-management
https://aka.ms/DPA

[48] https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/data-entities/data-management-api

[49] https://appsource.microsoft.com/en-us/product/dynamics-365/mscrm.44f192ec-e387-436c-886c-879923d8a448

[50] https://www.microsoft.com/en-us/download/details.aspx?id=18039 (Microsoft Dynamics CRM Online Migration to Microsoft Dynamics CRM on-premises)

[51] DOCX-Files: 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-eff2-4b22-92b6-0738acd4475e
PST-Files: https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-pst/141923d5-15ab-4ef1-a524-6dce75aae546

[52] https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows

- Does the target environment offer the same features as Dynamics 365 (functionality, security, performance, scalability etc.)?
- Is the new platform able to process the exported data of Dynamics 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 Dynamics 365 data is lost, cloud services themselves are unavailable or data is lost due to user action (e.g., inadvertent deletion of data).

Customers should decide, whether the data recovery functions and options in Dynamics 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-Grundschutz module *CON.3 Data backup policy*[53] as a part of the IT-Grundschutz Compendium. Especially the content of requirement *CON.3.A1 Determining the factors influencing data backup, CON.3.A3 Identification of legal factors influencing data backups, CON.3.A6 Development of a data backup policy* and *CON.3.A8 Function tests and verification of recovery* should be considered for the decision making.

Dynamics 365 provides different possibilities for exporting and backing up data. For example, the Customer Engagement service is backed up by default[54]. Besides it runs on an Azure SQL database, which is also backed up by default.[55] Additionally an export to Excel[56] is applicable. Dynamics 365 data can be used with a local installation of Microsoft Dynamics CRM. The data can also be synchronized to an on-premises application.[57] Otherwise, if a bulk export needs to be performed, third-party solutions are available.

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?

[53] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2021.html (German Only)

[54] https://docs.microsoft.com/en-us/dynamics365/admin/backup-restore-instances

[55] https://docs.microsoft.com/en-us/azure/sql-database/sql-database-automated-backups

[56] https://www.microsoft.com/en-us/dynamics/crm-customer-center/export-data-to-excel.aspx

[57] https://www.microsoft.com/en-us/download/details.aspx?id=18039 (Microsoft Dynamics CRM Online Migration to Microsoft Dynamics CRM on-premises)

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. Microsoft Azure offers encryption for its Infrastructure as a Service, Platform as a Service, and Software as a Service options using encryption in a number of areas. Dynamics 365 is already protected by the secure backend in Microsoft Azure, where it runs. The cloud user has the option of activating encryption with standard or individual encryption technologies, depending on the selected service.[58] 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 Dynamics 365.

The following table illustrates the functionalities provided by Dynamics 365 to encrypt data at-rest, in-transit, and to securely manage secrets:

Table 10: Offerings regarding encryption and cryptography in Dynamics 365

Category	Details	References
Encryption of data-at-rest	The Customer Engagement apps (Dynamics 365 Sales, Dynamics 365 Customer Service, Dynamics 365 Field Service, Dynamics 365 Marketing and Dynamics 365 Project Service Automation) encrypts a number of standard table attributes that can contain sensitive information such as usernames and email passwords at the cell level. Dynamics 365 databases are encrypted using Azure SQL Database's FIPS 140-2 compliant Transparent Data Encryption (TDE). In addition, Microsoft offers field-level encryption in the SQL Database for Dynamics 365.	https://docs.microsoft.com/en-us/power-platform/admin/data-encryption https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365
Encryption of data-in-transit	Dynamics 365 encrypts connections using industry-standards such as AES and TLS/SSL.	https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365
Key management and own encryption mechanisms	As a SaaS application, it is not possible to implement your own encryption mechanism.	https://azure.microsoft.com/en-us/services/key-vault/

[58] https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365

Category	Details	References
	Microsoft provides a suitable key management for its online applications by its own trust center infrastructure.	https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365
	In addition, Dynamics 365 supports customer key in the context of Bring-Your-Own-Key (BYOK).	https://docs.microsoft.com/en-us/power-platform/admin/manage-encryption-key

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[59] 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 Dynamics 365 through Azure Active Directory for the management of users and groups in Dynamics 365.[60] There are three general ways to realized hybrid accounts with different advantages and disadvantages:[61]

- Password has synchronization (PHS):[62] 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):[63] 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):[64] 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.

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

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

[61] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

[62] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs

[63] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

[64] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

Azure Active Directory, supports the SAML 2.0 protocol[65] as well as WS-Federation and OpenID Connect.[66] The information contained in the SAML[59] tickets can be configured according to organizational requirements or the requirements of each application.[67]

The user rights should be regularly checked and it should be ensured, that a SAML[59] 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*[68] 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.[69]

Furthermore, checking the correct ticket issuing process of SAML[59] to authorized users should be part of audits and technical tests as part of the established ISMS. The fulfillment of this requirement is the responsibility of the customer.

3.19 OPS.2.2.A19 Security Vetting of Employees

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

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

In addition, Microsoft pursues a strict supplier policy. For successful supplier collaboration, Microsoft's Supplier Program (MSP) defines the way key business-critical and strategic suppliers do business with Microsoft, including the requirements and expectations of Microsoft and its customers.[70] 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.[71] 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.[72] Microsoft also offers the SCoC Training Program to provide training to supplier employees.[73]

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

[66] https://docs.microsoft.com/en-us/azure/active-directory/develop/id-tokens

[67] https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-saml-claims-customization

[68] 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/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html(German only)

[69] https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

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

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

[72] https://www.microsoft.com/en-us/procurement/msp-overview.aspx?activetab=pivot1:primaryr4

[73] 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[74] which apply 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 Dynamics 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*[74] can be implemented for Dynamics 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*[74] 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 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage*
NCD.2.1.02 Security Policy for External Cloud Usage	Subchapter 3.1 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage* Subchapter 3.2 *OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage*

[74] https://www.bsi.bund.de/DE/Themen/Oeffentliche-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 *OPS.2.2.A7 Drawing Up a Security Concept for Cloud Usage*
NCD.2.1.04 Emergency and Continuity Management	Subchapter 3.1 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage* Subchapter 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services* Subchapter 3.16 *OPS.2.2.A16 Implementing In-House Backups*
NCD.2.2.01 Implementation of Security Requirements	Subchapter 3.8 *OPS.2.2.A8 Careful Selection of a Cloud Service Provider* Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* Subchapter 3.13 *OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage*
NCD.2.2.02 Contractually Ensure Dealings with Subcontractors and Other External Third Parties	Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*
NCD.2.2.03 Ensure Jurisdiction by Contract	Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*
NCD.2.2.04 Ensure Location by Contract	Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*
NCD.2.2.05 Ensure that Disclosure Obligations and Investigative Powers are Contractually Guaranteed	Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider*
NCD.2.2.06 Regulating the Termination of the Contractual Relationship	Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* Subchapter 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*
NCD.2.2.07 Ensure Data Return and Data Deletion at the Cloud Service Provider by Contract	Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* Subchapter 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*
NCD.2.3.01 Integrate ISMS	Subchapter 3.7 *OPS.2.2.A7 Drawing Up a Security Concept for Cloud Usage* Subchapter 3.12 *OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations*
NCD.2.3.02 Verify Security Certifications	Subchapter 3.13 *OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage*

Requirement	Links
NCD.2.3.03 Check Performance	Subchapter 3.12 *OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations*
NCD.2.3.04 Comply with Information Obligations	Subchapter 3.4 *OPS.2.2.A4 Definition of Areas of Responsibility and Interfaces* Subchapter 3.12 *OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations*
NCD.2.3.05 Enable Two-Factor Authentication	No reference
NCD.2.4.01 Perform Data Return	Subchapter 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship* Subchapter 3.15 *OPS.2.2.A15 Ensuring the Portability of Cloud Services*
NCD.2.4.02 Conform Data Deletion	Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* Subchapter 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*
NCD.2.5.01 Shared Use of External Cloud Services	Subchapter 3.1 *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage* Subchapter 3.6 *OPS.2.2.A6 Planning the Secure Integration of Cloud Services* Subchapter 3.8 *OPS.2.2.A8 Careful Selection of a Cloud Service Provider* Subchapter 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* Subchapter 3.17 *OPS.2.2.A17 Use of Encryption When Using the Cloud*

4.1 NCD.2.1.01 Strategy for Cloud Usage

The institution must create a cloud usage strategy in accordance with the BSI IT-Grundschutz requirement *OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage* (see subchapter 3.1). As part of the cloud usage strategy, the institution must decide how it will deal with the risks associated with outsourcing to the cloud. After the cloud usage strategy has been created, it must be checked whether the use of Dynamics 365 meets the requirements. The use of Dynamics 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"[75] 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[76] and security measures that can be implemented by the cloud customer[77].

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 Dynamics 365 must create a security policy by the responsible persons. The *BSI's minimum standards for the use of external cloud services*[78] stipulate that the implementation of and compliance with the basic criteria according to the BSI's Cloud Computing Compliance Criteria Catalogue (C5)[79] 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)[79] for Dynamics 365. The SOC 2 report on the audit can be viewed in the Service Trust Portal (STP)[80].

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[81] and security measures that can be implemented by the cloud customer.

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*.

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

[76] https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

[77] https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/role-based-security
https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/security-architecture

[78] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html (German only)

[79] https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html

[80] https://servicetrust.microsoft.com/Documents/ComplianceReports

[81] https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

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*[82] also requires an assessment by the institution of how a failure of Dynamics 365 would affect the institution. In addition, it should be checked together with the responsible emergency officer whether the use of Dynamics 365 affects the previous disaster management and thus the previous preventive / reactive measures can be adapted.

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 a Cloud Service*.

4.5 NCD.2.2.01 Implementation of Security Requirements

Before concluding a contract, it must be assessed whether Dynamics 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*) and, as part of the use of Dynamics 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[83] and security measures that can be implemented by the cloud customer.

Microsoft permits audits by customers under terms and conditions set forth in the Microsoft Online Services Data Protection Addendum (DPA)[84]. If customer's audit requirements under the Standard Contractual Clauses or the Privacy Requirements cannot be adequately met by audit reports, documentation, or other compliance information that Microsoft makes generally available to Customer, Microsoft will provide the option to satisfy customer's additional audit requirements. Before an audit begins, Microsoft will determine with customer the scope, timing, duration, control and evidence requirements, and audit fees.

Microsoft constantly carries out its own audits in accordance with several national and international standards and has published corresponding certifications, proofs or audit reports in the Service Trust Portal (STP)[85]. The current SOC 2 report on the audit of the Cloud Computing Compliance Criteria Catalogue (C5)[79] can also be accessed there.

[82] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html (German only)

[83] https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

[84] https://aka.ms/DPA

[85] https://servicetrust.microsoft.com/Documents/ComplianceReports

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

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

Microsoft provides a list of subcontractors and offers access to standardized service agreements, guidelines and codes of conduct.[86] External auditors have determined compliance with the basic criteria according to the BSI Cloud Computing Compliance Criteria Catalogue (C5)[79] for Dynamics 365. The SOC 2 report on the audit can be viewed in the Service Trust Portal (STP)[87].

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.[88]

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

4.8 NCD.2.2.04 Ensure Location by Contract

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

Microsoft publishes the regions in which Dynamics 365 services are operated.[89] In addition, Microsoft publishes statistics on law enforcement requests from around the world twice a year.[90]

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.*

[86] https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx
https://www.microsoft.com/licensing/docs

[87] https://servicetrust.microsoft.com/Documents/ComplianceReports

[88] https://aka.ms/DPA

[89] https://dynamics.microsoft.com/en-us/availability-reports/georeport/

[90] https://www.microsoft.com/en-us/corporate-responsibility/lerr

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*[91] also requires the agreement of contractual penalties in the event of non-fulfilment.

Microsoft has an internal policy[92] on notifying affected parties during an information security incident. Information about obligations to inform subjects under the GDPR are published as well[93]. In addition, Microsoft publishes statistics on law enforcement requests from around the world twice a year.[94]

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

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

When drafting the contract (see also subchapters 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* and 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*), the 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.[95]

[91] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html (German only)

[92] https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification

[93] https://servicetrust.microsoft.com/ViewPage/GDPRBreach

[94] https://www.microsoft.com/en-us/corporate-responsibility/lerr

[95] https://www.microsoft.com/en-us/trust-center/privacy/data-management
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cancel-azure-subscription
https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

4.12 NCD.2.3.01 Integrate ISMS

Dynamics 365 as well as the cloud services used should be integrated into the ISMS of the institution. It should be noted that the requirements contained in the BSI Cloud Computing Compliance Criteria Catalogue (C5)[79], 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 subchapter 3.7 *OPS.2.2.A7 Drawing Up a Security Concept for Cloud Usage*

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*[96] and the customer's risk analysis. Furthermore, this requirement obliges the cloud customer to regularly review this evidence for compliance with security requirements.

Dynamics 365 holds several global and regional certifications[97]. In addition, audit reports and other compliance information, such as penetration tests[98] [99], are regularly published on Microsoft's website. The responsibility for defining the required certifications and verifying that Dynamics 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*.

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 Dynamics 365 migration and integration, see the following subchapters 3.5 *OPS.2.2.A5 Planning a Secure Migration to a Cloud Service* and 3.6 *OPS.2.2.A6 Planning the Secure Integration of Cloud Services*.

[96] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html (German only)

[97] https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

[98] https://servicetrust.microsoft.com/Documents/ComplianceReports

[99] https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3

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.

Microsoft publishes information on various scenarios and incidents in order to fulfil its information obligations. Further information can be found in the following subchapters 3.8 *OPS.2.2.A8 Careful Selection of a Cloud Service Provider*, 3.9 *OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider* and 4.9 *NCD.2.2.05 Ensure that Disclosure Obligations and Investigative Powers are Contractually Guaranteed*.

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)[100]. 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.[101]

4.17 NCD.2.4.01 Perform Data Return

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

Further information on retrieving data from Dynamics 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 3.14 *OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship*.

[100] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

[101] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

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*[102].

Microsoft publishes the generally applicable contract terms in the Licensing Portal[103]. Supplemental agreements should be provided by the contractor with whom the cloud is shared.

In Dynamics 365, communication data is encrypted using industry standards such as AES and TLS/SSL, and data-at-rest is also encrypted using various methods.[104] 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.[105] Together with conditional access, this can be used to restrict access to certain data or services in Dynamics 365.[106]

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*.

[102] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf (German only)

[103] https://aka.ms/licensingdocs

[104] https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview
https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365

[105] https://docs.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up

[106] 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 Dynamics 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 Dynamics 365[107].

The most important of these are:

- ISO 27001 (Information Security Management System)
- ISO 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services)
- ISO 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)
- Cloud Computing Compliance Criteria 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 Azure is currently being analyzed. Such a certification will greatly ease the cloud customer’s certification, but is not required.

[107] https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

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.
OPS.2.2 Cloud Use	OPS.2.2 Cloud-Nutzung	Module *OPS.2.2 Cloud use* provides recommendations for the secure use of cloud services. It describes cloud service specific threats and requirements to mitigate the risk associated with the impact of undesirable events.

English term	German term	Description
Requirement	Anforderung	Standard security requirement in IT-Grundschutz; Often used synonymously with "control".

Appendix B
References to Further Information

Topic	Information Pointer
Legal information	https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx https://www.microsoft.com/licensing/terms/welcome/welcomepage https://www.microsoft.com/licensing/docs https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services https://aka.ms/DPA
Due Diligence	https://azure.microsoft.com/en-us/overview/choosing-a-cloud-service-provider/ https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist https://www.microsoft.com/en-us/investor/default.aspx https://www.microsoft.com/en-us/corporate-responsibility/lerr
Compliance Information	https://servicetrust.microsoft.com/ https://docs.microsoft.com/en-us/compliance/regulatory/offering-home https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview https://www.microsoft.com/en-us/corporate-responsibility/lerr https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics-windows
Dynamics 365 services, tools and further information	https://info.microsoft.com/enterprise-cloud-strategy-ebook.html https://azure.microsoft.com/en-us/overview/choosing-a-cloud-service-provider/ https://docs.microsoft.com/en-us/power-platform/admin/notifications-explained#service-health-dashboard https://dynamics.microsoft.com/en-us/roadmap/overview/

Topic	Information Pointer
	https://docs.microsoft.com/en-us/dynamics365/get-started/availability https://aka.ms/dynamics_365_international_availability_deck 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 (Exit Planning for Microsoft Cloud Services) https://fasttrack.microsoft.com/
Security Aspects Dynamics 365	https://servicetrust.microsoft.com/ https://docs.microsoft.com/en-us/power-platform/admin/wp-security https://docs.microsoft.com/en-us/azure/active-directory/ https://docs.microsoft.com/en-us/office365/enterprise/hybrid-cloud-overview https://docs.microsoft.com/en-us/azure/active-directory/hybrid/ https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365 https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/dev-it-pro/data-entities/data-management-api https://docs.microsoft.com/en-us/rest/dynamics365/ https://docs.microsoft.com/en-us/cloud-app-security/ https://docs.microsoft.com/en-us/power-platform/admin/field-level-security
Microsoft Services Supplier List	https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List) https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426 (Microsoft Commercial Support Subcontractors)
BSI	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-2002_en_pdf.html 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_it_gs_comp_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)

Topic	Information Pointer
	https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html (German only) https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html

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

HiSolutions AG
Schloßstraße 1
12163 Berlin

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

HiSolutions AG
Branch Office
Frankfurt am Main
Brüsseler Str. 1-3
Tower One - Spaces
60327 Frankfurt am Main

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

HiSolutions AG
Branch Office
Bonn
Heinrich-Brüning-Straße 9
53113 Bonn

Fon: +49 228 52 268 175
Fax: +49 30 533 289-900

HiSolutions AG
Branch Office
Nürnberg
Bahnhofstraße 2
3. OG
90402 Nürnberg

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

HiSolutions AG
Branch Office
Düsseldorf
Kaiserswerther Straße 135
40474 Düsseldorf

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