



Microsoft Dynamics 365 GxP Guidelines

White paper

July 2020

DISCLAIMER

© 2020 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. In addition, for your convenience, this document references one or more Microsoft agreements and summarizes portions of such agreements and is intended for information purposes only. You should refer to the actual text in the most current version of the Microsoft agreements for the exact legal commitments.

This document does not constitute legal advice; you should consult your own counsel for legal guidance on your specific scenarios. This document does not provide you with any rights to any intellectual property in any Microsoft product or service. You may copy and use this document only for your internal, reference purposes. You bear all risk of using it.

Foreword

More and more life science organizations are looking to leverage cloud-based solutions that can be used anywhere, on any device, to support "good practice" quality guidelines and regulations (GxP). To carry out their digital transformation, customers in regulated industries trust Microsoft cloud services such as Microsoft 365, Azure, and Dynamics 365 to shorten their time to market, reduce costs, increase operational efficiency, and accelerate scientific innovation.

Each year Microsoft invests billions of dollars in designing, building, and operating innovative cloud services. But in this highly regulated industry, for you to even consider our services, we must earn and retain your trust. Microsoft cloud services are built around key tenets of security, privacy, transparency, and compliance; and we invest more each year to increase the confidence of our life sciences customers in Microsoft cloud services.

Microsoft aims to ensure the confidentiality, integrity, and availability of data, documents, and GxP applications for life science organizations. With each service, customer data benefits from multiple layers of security and governance technologies, operational practices, and compliance policies to enforce data privacy and integrity at specific levels.

Over time, we intend to make it easier for life sciences organizations to use Microsoft cloud services for their *full* portfolios of applications. We believe that this GxP guidance document is a key step toward that goal. Given the shared responsibilities of the cloud model, life science customers rely on the fact that Microsoft has implemented appropriate technical and procedural controls to manage and maintain the cloud environment in a state of control. Microsoft's quality practices and secure development lifecycle encompass similar core elements as would be found in many life sciences customers' internal Quality Management Systems and meet or exceed industry standards.

This guide should help demonstrate that you can develop and operate GxP applications on Microsoft Dynamics 365 with confidence and without sacrificing compliance with GxP regulation.

We look forward to working with you to help you achieve your digital transformation initiatives using Microsoft Dynamics 365.

Daniel Carchedi – Sr. Director Business Development & Strategy

Microsoft Corporation

July 2020

Executive Summary

Life sciences organizations, ranging from large multinational pharmaceutical manufacturers to smaller biotechnology startups, all face the same pressure to streamline processes, increase efficiency, and reduce costs while ensuring patient safety, product quality, and data integrity. This pressure, combined with the unique benefits of cloud technology that include rapid on-demand scalability as well as global reach, is driving an increasing number of life sciences organizations to consider moving GxP systems to the cloud.

The goal of this GxP guideline document is to provide life sciences organizations with a comprehensive toolset for using Microsoft Dynamics 365 while adhering to industry best practices and applicable regulations. It identifies the shared responsibilities between Microsoft and its life sciences customers for meeting regulatory requirements, such as FDA 21 CFR Part 11 Electronic Records, Electronic Signatures (21 CFR Part 11), and EudraLex Volume 4 – Annex 11 Computerised Systems (Annex 11).

While considering the use of cloud technology to host GxP computerized systems, it is important for life sciences organizations to assess the adequacy of the cloud service provider's processes and controls that help to assure the confidentiality, integrity, and availability of data that is stored in the cloud. When stored in Dynamics 365, customer data benefits from multiple layers of security and governance technologies, operational practices, and compliance policies to enforce data privacy and integrity at very specific levels. This document highlights the extensive controls implemented as part of Microsoft's internal development of security and quality practices, which help to ensure that Dynamics 365 meets its specifications and is maintained in a state of control. Dynamics 365 procedural and technical controls are regularly audited and verified for effectiveness by independent third-party assessors. The latest certificates and audit reports are available to customers in the [Service Trust Platform \(STP\)](#).

Of equal importance are those processes and controls that must be implemented by Microsoft life sciences customers to ensure that GxP computerized systems are maintained in a secured and validated state. This guideline includes recommendations based on proven practices of existing life sciences customers as well as industry standards for qualification and validation of GxP applications. By establishing a well-defined cloud strategy and robust governance model, customers can ensure the following:

- ✓ Risks associated with hosting GxP applications in the cloud are identified and mitigated.
- ✓ Internal quality and information technology procedures are adapted for using cloud-based applications and customer personnel are appropriately trained.
- ✓ Due diligence/assessment of the cloud service provider is performed.
- ✓ Systems are designed to preserve system resiliency, performance, data security, and confidentiality.
- ✓ Virtual infrastructure components and services are maintained in a qualified state.
- ✓ Data integrity and compliance with regulatory requirements is verified.
- ✓ Data backup/recovery procedures are in place and tested.

By working together and focusing on their respective areas of expertise, Microsoft and its life sciences customers can help usher in a new era in which cloud-based GxP systems are no longer seen as a

compliance risk, but rather as a safer, more efficient model for driving innovation and maintaining regulatory compliance.

Authors

The production of this GxP guidance document was driven by the Microsoft Health and Life Sciences Team and was developed in collaboration with several functional team members whose responsibilities include compliance, engineering, life sciences, technology, strategy, and account management. We collaborated with our longstanding life sciences industry partner, [Montrium](#), to review Microsoft quality and development practices and to provide expert guidance concerning industry best practices for cloud compliance and GxP computerized systems validation. Montrium is a highly regarded knowledge-based company that uses its deep understanding of GxP processes and technologies to help life sciences organizations improve processes and drive innovation while maintaining compliance with GxP regulations. Montrium works exclusively in the life sciences industry and has provided services to over 200 life sciences organizations around the globe, including organizations in North America, Europe, and Asia.

Table of contents

Foreword.....	3
Executive Summary.....	4
Authors.....	6
1 Introduction	9
1.1 Purpose.....	9
1.2 Audience and scope.....	10
1.3 Key terms and definitions.....	10
1.3.1 Customer.....	10
1.3.2 Dynamics 365 Online Services	10
1.3.3 GxP	10
1.3.4 GxP regulations	10
1.3.5 Microsoft Azure and the Azure platform	11
2 Overview of Microsoft Dynamics 365.....	12
2.1 Dynamics 365 applications.....	12
2.2 Certifications and attestations	14
2.2.1 SOC 1 & SOC 2	14
2.2.2 CSA Security, Trust & Assurance Registry (STAR).....	15
2.2.3 FedRAMP.....	16
2.2.4 ISO/IEC 27001:2013	16
2.2.5 ISO/IEC 27018:2014	16
2.2.6 ISO 9001:2015	17
2.2.7 ISO/IEC 20000-1:2011	17
2.2.8 HITRUST.....	18
2.2.9 EU GDPR.....	18
2.3 Microsoft Quality Management System	18
2.3.1 Roles and responsibilities.....	19
2.3.2 Policies and standard operating procedures	21
2.3.3 Microsoft personnel and contractor training	21
2.3.4 Documented information	22
2.3.5 Design and development of Dynamics 365 products and services	22
2.3.6 Operations management	27

2.3.7	Performance evaluation.....	35
2.3.8	Improvement	35
3	Considerations for satisfying GxP requirements	36
3.1	Data integrity controls.....	36
3.1.1	Considerations for FDA 21 CFR Part 11 compliance	37
3.2	Dynamics 365 governance recommendations	42
3.2.1	Shared responsibility model	43
3.2.2	Service agreements.....	44
3.2.3	Governance policies and procedures.....	45
3.3	GxP Use Cases.....	51
3.4	Considerations for implementing a risk-based validation strategy.....	51
3.4.1	GAMP 5 Software Category	52
3.4.2	Application Stakeholders	53
3.4.3	Computerized system life cycle approach	53
4	Conclusion.....	61
5	Document Revision	61
6	References	62
6.1	Industry guidance and standards	62
6.2	Regulations and regulatory guidance.....	62
7	Appendices.....	62
Appendix A.	Glossary, Abbreviations and Acronyms	64
Appendix B.	Coverage of SLA / Quality Agreement Requirements with Microsoft Agreements	65
Appendix C.	US FDA 21 CFR Part 11 Electronic Records; Electronic Signatures - Shared Responsibilities	69
Appendix D.	EudraLex Volume 4 Annex 11 Computerised Systems - Shared Responsibilities	78

1 Introduction

1.1 Purpose

As adoption of cloud-based technologies continues to accelerate globally and across industries, Microsoft recognizes that the life sciences industry has unique needs when leveraging Microsoft Dynamics 365 services to support regulated (GxP) activities. Working in a highly regulated environment requires life sciences organizations to consider potential compliance impacts before fully embracing new technologies. This GxP guidance document embodies the continued focus and commitment of Microsoft to supporting the life sciences industry as it seeks to benefit from the full potential of cloud-based solutions.

Microsoft's goal is to provide life sciences organizations with a comprehensive toolset for using Dynamics 365 while adhering to industry best practices and applicable regulations. To achieve this goal, we identified proven practices of existing life sciences customers and partners who currently use Microsoft cloud services as the basis for their GxP validated applications. We also collaborated with Montrium to review our internal quality and development practices, while collaborating with industry subject matter experts and regulatory agencies to identify critical elements that have GxP relevance. Together, we defined recommendations for organizations seeking to use Dynamics 365 in support of GxP activities.

While Microsoft continues to publish comprehensive information concerning its internal security, privacy, and compliance controls, this document consolidates and further clarifies topics that are paramount to our life sciences customers. These GxP-relevant topics include:

- Increased visibility into crucial areas of internal Microsoft quality management, IT infrastructure qualification, and software development practices
- Recommendations for customer GxP compliance readiness, including an approach for validating Dynamics 365 SaaS (software as a service)
- Description of GxP-relevant tools and features within Dynamics 365
- In-depth analysis of shared responsibilities concerning US FDA 21 CFR Part 11 and EudraLex Volume 4 Annex 11 regulatory requirements and current industry standards, such as ISPE's GAMP[®] 5 and related Good Practice Guides

Achieving a compliant cloud-based solution requires well-defined controls and processes, with shared responsibilities between Microsoft and its customers. We have implemented a series of technical and procedural controls to help ensure the dependability (accessibility, availability, reliability, safety, integrity, and maintainability) of Microsoft systems and services. Of equal importance are the controls enforced by Microsoft customers in protecting the security and privacy of their data.

This guidance document begins with an initial focus on internal Microsoft quality and development practices, followed by recommendations to help life sciences industry customers successfully implement Dynamics 365 in support of their GxP activities.

Microsoft focus ¹	Life sciences customer focus ²
<ul style="list-style-type: none">• Overview of Dynamics 365 products and services• Certifications and attestations• Quality Management System• Software development and infrastructure qualification	<ul style="list-style-type: none">• Cloud strategy and governance recommendations• Potential impacts to customers' QMS, including data integrity and operations management controls• Qualification considerations for SaaS-based GxP applications• GxP-relevant tools and features within Dynamics 365

¹ **Section 2** includes details about internal Microsoft systems, controls, and processes.

² **Section 3** includes recommendations for customers using Dynamics 365 to support GxP regulated activities.

1.2 Audience and scope

Life sciences organizations using Dynamics 365 to manage GxP-regulated processes and/or data can benefit from the information contained in this guidance document. The life sciences industry consists of organizations operating in various segments, including pharmaceuticals, biotechnology, medical device, clinical research, and veterinary medicine.

Dynamics 365 may be used across these industry segments to support various GxP business processes and to store a diverse range of GxP data. The specific GxP processes and data managed within the customer's Microsoft 365 environment are not addressed in this document, as the customer (regulated user) is responsible for defining the requirements and validating the GxP business process supported by Dynamics 365.

1.3 Key terms and definitions

1.3.1 Customer

Within the context of this guidance document, the customer is any person or organization using Dynamics 365 online services to manage GxP regulated content or to support GxP regulated activities.

1.3.2 Dynamics 365 Online Services

Online business application suite that integrates the Customer Relationship Management (CRM) capabilities and its extensions with the Enterprise Resource Planning (ERP) capabilities.

1.3.3 GxP

GxP is a general abbreviation for the "good practice" quality guidelines and regulations (see GxP regulations).

1.3.4 GxP regulations

The term GxP regulations refers to the underlying international pharmaceutical requirements, such as those outlined in the US FD&C Act, US PHS Act, FDA regulations, EU Directives, Japanese regulations, or other applicable national legislation or regulations under which an organization operates. These include, but are not limited to:

- Good Manufacturing Practice (GMP) (pharmaceutical, including Active Pharmaceutical Ingredient (API), veterinary, and blood)
- Good Clinical Practice (GCP)
- Good Laboratory Practice (GLP)
- Good Distribution Practice (GDP)
- Good Quality Practice (GQP) (refer to Japan [MHLW Ministerial Ordinance No. 136](#))
- Good Pharmacovigilance Practice (GVP)
- Medical Device Regulations (MedDev)
- Prescription Drug Marketing Act (PDMA)

1.3.5 Microsoft Azure and the Azure platform

The Azure platform refers to the collection of integrated IaaS and PaaS cloud services offered by Microsoft and includes personnel, processes, technology, software, and physical infrastructure which together deliver the complete service offering. Throughout this document, the terms Microsoft Azure, Azure platform, and Azure are used interchangeably.


2 Overview of Microsoft Dynamics 365

[Microsoft Dynamics 365](#) is a cloud-based business applications platform that combines components of customer relationship management (CRM) and enterprise resource planning (ERP), along with productivity applications and artificial intelligence tools.

Microsoft Dynamics 365 resides within the [Microsoft Azure](#) multi-tenant platform. When referring to Azure this encompasses the underlying infrastructure supporting Microsoft Dynamics 365 online services, including the teams which manage them. The Microsoft Dynamics 365 organization has been consolidated in the Microsoft Azure organization since mid-2018.

At Microsoft, trust is a focal point for service delivery, contractual commitments, and industry accreditation, which is why we embraced the Trusted Cloud initiative. The Trusted Cloud Initiative is a program of the [Cloud Security Alliance](#) (CSA) industry group created to help cloud service providers develop industry-recommended, secure and interoperable identity, access and compliance management configurations and practices. This set of requirements, guidelines, and controlled processes ensures we deliver our cloud services with the highest standards regarding engineering, legal, and compliance support. Our focus is on maintaining data integrity in the cloud, which is governed by the following three (3) key principals:



 Visit the [Trust Center](#) to learn more about what Microsoft is doing to earn our customers' trust.

2.1 Dynamics 365 applications

Dynamics 365 consists of the following offerings:

- [Dynamics 365 AI Customer Insights](#): help build a deeper understanding of customers. Connect data from various transactional, behavioral, and observational sources to create a 360-degree customer view. Use these insights to drive customer-centric experiences and processes.
- [Dynamics 365 Business Central](#): business management solution for small and mid-sized organizations that automates and streamlines business processes and helps manage the business. Highly adaptable and rich with features, Business Central enables companies to manage their business, including finance, manufacturing, sales, shipping, project management, services, and more.

- [Dynamics 365 Commerce](#): delivers a comprehensive omnichannel solution that unifies back-office, in-store, call center, and digital experiences. Enables build brand loyalty building through personalized customer engagements, increase revenue with improved employee productivity, optimize operations to reduce costs and drive supply chain efficiencies, ultimately delivering better business outcomes.
- [Dynamics 365 Customer Engagement](#): a cloud-based customer relationship management (CRM) business solution that can help you drive sales productivity and improve the value of your marketing efforts through social insights, business intelligence, and campaign management.
- [Dynamics 365 Customer Service](#): gives actionable insights into critical performance metrics, operational data, and emerging trends from customer service systems. Built-in dashboards, interactive charts, and visual filters provide views into support operations data across channels, and highlight areas for improvement that can have the greatest impact, helping to quickly evaluate and respond to key performance indicators (KPIs) and customer satisfaction levels.
- [Dynamics 365 Field Service](#): business application helps organizations deliver onsite service to customer locations. The application combines workflow automation, scheduling algorithms, and mobility to set mobile workers up for success when they're onsite with customers fixing issues.
- [Dynamics 365 Finance](#): assess the health of your business, improve financial controls, optimize cash flow, and make strategic decisions faster to drive growth by using real-time, unified global financial reporting, embedded analytics, and predictive insights.
- [Dynamics 365 Fraud Protection](#): focuses on payment fraud protection and related scenarios in e-commerce. It helps e-commerce merchants drive down fraud loss, increase bank acceptance rates to yield higher revenue, and improve the online shopping experience for its customers.
- [Dynamics 365 Human Resources](#): provides the workforce insights needed to build data-driven employee experiences across multiple areas, including: compensation, benefits, leave and absence, compliance, payroll integration, performance feedback, training and certification, self-service programs.
- [Dynamics 365 Marketing](#): marketing-automation application that helps turn prospects into business relationships. The application is easy to use, works seamlessly with Dynamics 365 Sales, and has built-in business intelligence.
- [Dynamics 365 Portals](#): create external-facing websites that allow users outside their organizations to sign in with a wide variety of identities, create and view data in Common Data Service, or even browse content anonymously.
- [Dynamics 365 Project Service Automation](#): helps organizations efficiently track, manage, and deliver project-based services, from the initial sale all the way to invoicing.
- [Dynamics 365 Sales](#): enables salespeople to build strong relationships with their customers, take actions based on insights, and close sales faster. Use Dynamics 365 Sales to keep track of accounts and contacts, nurture sales from lead to order, and create sales collateral. It also allows the creation marketing lists and campaigns, and even follow service cases associated with specific accounts or opportunities.
- [Dynamics 365 Supply Chain Management](#): allows organizations to streamline planning, production, inventory, warehouse, and transportation to maximize operational efficiency,

product quality, and profitability using predictive insights from AI and the Internet of Things (IoT).


2.2 Certifications and attestations

The Dynamics 365 online services and its underlying infrastructure employ a security framework that encompasses industry best practices and spans multiple standards, including the ISO 27000 family of standards, NIST 800, and others. As part of our comprehensive [compliance offering](#), Microsoft regularly undergoes independent audits performed by qualified third-party accredited assessors for ISO (27001, 27701, 27018 & 9001), SOC (1, 2, 3), Health Information Trust Alliance (HITRUST), [US Federal Risk and Authorization Management Program \(FedRAMP\)](#), and Payment Card Industry (PCI). The latest certificates and audit reports are available to customers in the [Service Trust Platform \(STP\)](#).

Although there are no certifications specifically for GxP compliance, the preceding certifications and attestations have many similarities with the controls required to meet regulatory requirements, such as those stipulated in the FDA’s 21 CFR Part 11 and EU’s EudraLex Volume 4 Annex 11.

The following table identifies the certifications and attestations that Microsoft has achieved which include Dynamics 365 online services in their scope, which we believe are most relevant to our life sciences customers. The audited controls are verified and re-assessed periodically at the audit frequencies specified in the table.

Standard	Audit frequency	Governance Body / Auditor
SOC 1 SSAE18 Type II	Quarterly	Deloitte
SOC 2 AT 101 Type II	Quarterly	Deloitte
SOC 3 AT 101 Type II	Quarterly	Deloitte
ISO/IEC 27001:2013	Semi-annually	Shellman & Company, LLC
ISO/IEC 27701:2019	Semi-annually	Shellman & Company, LLC
ISO/IEC 27018:2019	Semi-annually	Shellman & Company, LLC
ISO 9001:2015	Annually	Coalfire ISO
ISO/IEC 20000-1:2011	Annually	Coalfire ISO
HITRUST CSF® v9.2	Annually	Coalfire

 The latest certificates and audit reports are available to customers in the [Service Trust Platform \(STP\)](#).

Additional Resources:

- [Overview of Microsoft Azure Compliance](#)

2.2.1 SOC 1 & SOC 2

Microsoft is audited quarterly according to the [Service Organization Controls \(SOC\)](#) framework developed by the [American Institute of Certified Public Accountants \(AICPA\)](#). Service audits based on the SOC framework fall into two categories—SOC 1 and SOC 2—that apply to in-scope Dynamics 365 services.

The SOC 1 Type 2 Service Auditor’s Reports are conducted in accordance with the professional standard known as Statement on Standards for Attestation Engagements (SSAE) No. 18. The SOC 1 audits are

geared toward reporting on controls at service organizations that are relevant to internal control over financial reporting (ICFR); they replaced the SAS 70 auditing standard.

The SOC 2 framework is a comprehensive set of criteria known as the Trust Services Criteria, which are composed of the following:

- **Security** means information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet objectives.
- **Availability** means information and systems are available for operation and use to meet the entity's objectives.
- **Processing integrity** means system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality** means information designated as confidential is protected to meet the entity's objectives.
- **Privacy** means personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

During the SOC examination, the independent auditor performs a variety of tests to confirm the effectiveness of the controls supporting the trust services criteria, the results of which are included in the SOC audit reports. Any exceptions identified in the audit are addressed by management in the last section of the audit report.



The latest SOC1 and SOC2 audit reports are available to customers in the [Service Trust Platform \(STP\)](#).

Note: *As presented in the SOC 2 audit report, the examination resulted in an "Unqualified" opinion result, which means no significant exceptions were found during the audit. In other words, a positive outcome. This clarification is mentioned here as the term "unqualified" may confuse those who are not familiar with SSAE standard terminology and because the term "unqualified" may have a different connotation to Microsoft life sciences customers.*

2.2.2 CSA Security, Trust & Assurance Registry (STAR)

The [Cloud Security Alliance \(CSA\) STAR Attestation](#) involves a rigorous independent audit of a cloud provider's security controls based on a SOC 2 Type 2 audit in combination with the CSA's [Cloud Controls Matrix \(CCM\) Criteria](#). The Cloud Security Alliance Cloud Controls Matrix (CCM) is a controls framework that covers fundamental security principles to help cloud customers assess the overall security risk of a cloud service provider.

Microsoft has attained Level 1 (CSA STAR Self-Assessment) as well as Level 2 (CSA STAR Certification and Attestation) and is currently the only major public cloud service provider to earn this certification with the highest possible Gold Award for the maturity capability assessment.



The following resources are available for download to help Microsoft customers better understand our security practices and how we conform to CSA best practices:

- [Microsoft Azure Cloud Controls Matrix \(CCM\)](#)

2.2.3 FedRAMP

The [US Federal Risk and Authorization Management Program \(FedRAMP\)](#) was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA), and to accelerate the adoption of secure cloud solutions by federal agencies. The mandatory [NIST 800-53](#) standards establish security categories of information systems—confidentiality, integrity, and availability—to assess the potential impact on an organization should its information and information systems be compromised.

The scope of the FedRAMP audit for Azure Commercial includes the information security management system that encompasses infrastructure, development, operations, management, and support of in-scope services for Dynamics 365.



The Letter from the Joint Authorization Board (JAB) Federal Risk and Authorization Management Program is available to customers in the [Service Trust Platform \(STP\)](#).

2.2.4 ISO/IEC 27001:2013

The [ISO/IEC 27001:2013](#) standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

Compliance with these standards, confirmed by an accredited auditor, demonstrates that Microsoft uses internationally recognized processes and best practices to manage the infrastructure and organization that support and deliver its services. The certificate validates that Microsoft has implemented the guidelines and general principles for initiating, implementing, maintaining, and improving the management of information security.



The latest ISO/IEC 27001 audit report is available to customers in the [Service Trust Platform \(STP\)](#).

2.2.5 ISO/IEC 27018:2014

[ISO/IEC 27018:2014](#) establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect personally identifiable information (PII) according to the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

By following the standards of ISO/IEC 27001 and the code of practice embodied in ISO/IEC 27018, Microsoft—the first major cloud provider to incorporate this code of practice—demonstrates that its privacy policies and procedures are robust and in line with its high standards.



The latest ISO/IEC 27018:2014 certificate is available to customers in the [Service Trust Platform \(STP\)](#).

2.2.6 ISO 9001:2015

The Microsoft's Quality Management System is certified according to the requirements of [ISO 9001:2015](#).

ISO 9001:2015 is a standard that sets out the requirements for a quality management system to help businesses and organizations improve customer satisfaction and efficiency. The standard is based on the following seven quality management principles:

- **Customer focus**; meet and exceed customer expectations
- **Leadership**; provide purpose, direction and engagement
- **Engagement of People**; Recognition, empowerment and enhancement of skills and knowledge.
- **Process Approach**; Understand processes to optimize performance.
- **Improvement**; maintain current performance and to create new opportunities.
- **Evidence-based decision making**; facts, evidences and data analysis for decision making.
- **Relationship management**; manage relationship with interested parties to optimize performance.

Achieving the ISO 9001:2015 certification underscores how Microsoft focuses on delivering quality products and maintaining a constant state of improvement to exceed customer expectations.



The latest ISO 9001:2015 audit report is available to customers in the [Service Trust Platform \(STP\)](#).

Additional Resources:

- [ISO Quality Management Principles](#)

2.2.7 ISO/IEC 20000-1:2011

ISO/IEC 20000-1:2011 is an international standard for the establishment, implementation, operation, monitoring, and review of an information technology service management system (SMS). The standard is based on requirements for designing, transitioning, delivering, and improving services to fulfill agreed service requirements and to provide value to both customers and service providers. ISO 20000-1 helps organizations provide assurance to customers that their service requirements will be fulfilled.

Achieving the ISO/IEC 20000-1 certification demonstrates that Microsoft has implemented the right IT service management procedures to deliver efficient and reliable IT services that are subject to regular monitoring, review, and improvement.



The latest ISO/IEC 20000-1:2011 audit report is available to customers in the [Service Trust Platform \(STP\)](#).

Additional Resources:

- [Preview of ISO/IEC 20000-1:2011](#)

2.2.8 HITRUST

The Health Information Trust Alliance (HITRUST) is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework (CSF), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner. The CSF builds on HIPAA and the HITECH Act and incorporates healthcare-specific security, privacy, and other regulatory requirements from existing frameworks such as the PCI DSS, ISO 27001, EU GDPR, NIST and MARS-E.

HITRUST provides a benchmark—a standardized compliance framework, assessment, and certification process—against which cloud service providers and covered health entities can measure compliance. HITRUST offers three degrees of assurance or levels of assessment: self-assessment, CSF-validated, and CSF-certified. Each level builds with increasing rigor on the one that precedes it. An organization with the highest level, CSF-certified, meets all the CSF certification requirements.

Microsoft is one of the first hyperscale cloud service providers to receive certification for the [HITRUST CSF](#).



The latest HITRUST Letter of Certification is available to customers in the [Service Trust Platform \(STP\)](#) in scope of this assessment are; Dynamics 365 Sales, Dynamics 365 Customer Service, Dynamics 365 Marketing, Dynamics 365 Field Service and Dynamics 365 Project Service Automation

Additional Resources:

- [HITRUST CSF Version](#)

2.2.9 EU GDPR

As of May 25, 2018, the European Unions Regulation 2016/679 also referred to as the General Data Protection Regulation (GDPR) has been in effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations which offer goods and services to people in the European Union (EU), or which collect and analyze data tied to EU residents. The GDPR applies no matter where you are located.

Microsoft designed Dynamics 365 with industry-leading security measures and privacy policies to safeguard data in the cloud, including the categories of personal data identified by the GDPR. Dynamics 365 provides the capabilities to help reduce risks and achieve GDPR compliance.



Additional Resources:

- [European Commission - EU data protection rules](#)
- [Regulation \(EU\) 2016/679 - General Data Protection Regulation](#)
- [Microsoft Privacy and GDPR Resources](#)

2.3 Microsoft Quality Management System

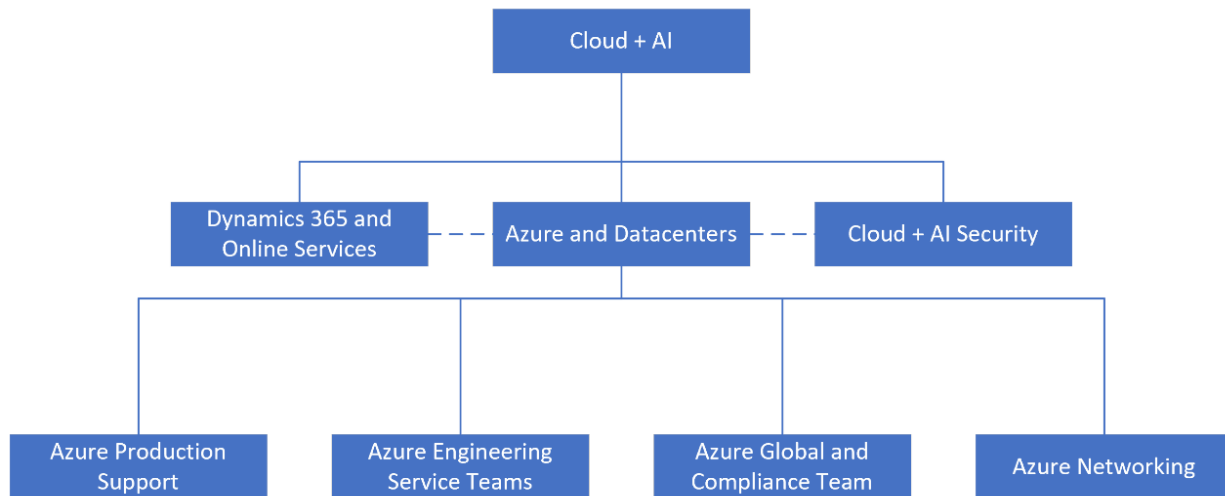
The Global Ecosystem and Compliance Team has established a Quality Manual that identifies the primary objectives of the Quality Management System (QMS), which is aligned with the ISO 9001:2015 standard. The QMS governs the core quality practices that deal with the delivery and management of the Dynamics 365 online services.

The scope of the Quality Manual encompasses the quality-related activities performed by the Engineering, Infrastructure, Operations, Security, Privacy, and Compliance Teams responsible for managing the Dynamics 365 online services.

By implementing a modern quality system and risk management approach that complies with the ISO 9001:2015 standard, the QMS has many of the same core elements as those of our life sciences customers. These elements include a clearly defined organizational structure with roles, responsibilities, and documented procedures, all of which govern internal processes that guide resources toward achieving Microsoft quality objectives as described in the following sections.

2.3.1 Roles and responsibilities

Microsoft personnel responsible for the successful delivery and management of Dynamics 365 services are distributed across the following groups:



Although quality responsibilities are embedded into each functional group, overall quality oversight is managed by the Global Ecosystem and Compliance Team, which has ownership of the Quality Manual. The general responsibilities of each group are as follows:

2.3.1.1 Dynamics 365 and Online Services Teams

Online Services Teams manage the service lifecycle of the finished SaaS services that use the underlying Dynamics 365 online services and datacenter infrastructure. They are responsible for the development of new features, operational support, and escalations.

2.3.1.2 Cloud + AI Security Team

The Cloud + AI Security Team works to make a secure and compliant cloud platform by building common security technologies, tools, processes, and best practices. The Cloud + AI Security Team is involved in the review of deployments and enhancements of cloud services to facilitate security considerations at every level of the Security Development Lifecycle (SDL). They also perform security reviews and provide security guidance for the datacenters. This team consists of personnel responsible for:

- Security Development Lifecycle
- Security incident response
- Driving security functionality within service development work

2.3.1.3 Production Support Team

The Azure Production Support Team is responsible for build-out, deployment, and management of Azure services. This team consists of the following:

- **Azure Live Site:** Monitors and supports the Azure platform; proactively addresses potential platform issues; and reacts to incidents and support requests
- **Azure Deployment Engineering:** Builds out new capacity for the Azure platform and deploys platform and product releases through the release pipeline
- **Azure Customer Support:** Provides support to individual customers and multinational enterprises from basic break-fix support to rapid response support for mission-critical applications
- **Dynamics 365 Customer Support:** Provides support to customers using Dynamics 365 online services

2.3.1.4 Azure Engineering Service Teams

The Azure Engineering Service Teams manage the service lifecycle. Their responsibilities include:

- Development of new services
- Serving as an escalation point for support
- Providing operational support for existing services (DevOps model)

The teams include personnel from the Development, Test, and Program Management (PM) disciplines for design, development, and testing of services, and provides technical support as needed.

2.3.1.5 Azure Global and Compliance Team

The Global Ecosystem and Compliance Team is the owner of the Microsoft Quality Manual and is responsible for developing, maintaining, and monitoring the Information Security (IS) program, including the ongoing risk assessment process and supporting inspection requests.

As part of managing compliance adherence, this Team drives related features within the Azure product families. The team consists of personnel responsible for:

- Training
- Privacy
- Risk assessment
- Internal and external audit coordination

2.3.1.6 Azure Networking Team

The Networking Team is responsible for implementing, monitoring, and maintaining the Microsoft network. This team consists of personnel responsible for:


- Network configuration and access management

- Network problem management
- Network capacity management

2.3.2 Policies and standard operating procedures

Policies and processes that accompany the Information Security program provide a framework to assess risks to the Dynamics environment, develop mitigation strategies, and implement security controls. The objective of the Information Security Program is to maintain the Confidentiality, Integrity, and Availability (CIA) of information while complying with applicable legislative, regulatory, and contractual requirements.

Team-specific standard operating procedures (SOPs) have been developed to provide implementation details for carrying out specific operational tasks required for the management of the Dynamics 365 online services. SOPs are stored and managed electronically in a controlled environment with version control and user access management to ensure the SOPs are only accessible to authorized individuals.

 Additional details, including a list of process areas governed by procedural controls, can be found in the "Description of Controls" section of the SOC 2 report available to customers in the [Service Trust Platform \(STP\)](#).

2.3.3 Microsoft personnel and contractor training

Microsoft has implemented a training program to ensure that personnel and contractors responsible for the Dynamics platform are adequately trained on internal processes and are qualified to perform their duties. New employees receive orientation and predetermined training requirements based on their role and job functions. Corporate policies are communicated to employees and relevant external parties during the orientation process and as part of the annual security training and awareness education program.

An internal learning management tool is used to manage critical course content and employee training traceability. This tool includes a dashboard and reporting capabilities for managers to see overall training completion. Security training is performed annually, according to Microsoft security education and awareness procedures, and individual training records are retained in accordance with a corporate retention policy.

Both the FDA's 21 CFR Part 11 and EU's EudraLex Volume 4 Annex 11 regulations require adequate training and education of personnel involved in the management of qualified computerized systems used in the context of GxP regulated activities. Annex 11 states, "all personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties." Likewise, 21 CFR Part 11 requires "that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks."

These regulatory requirements correlate closely with the SOC 2 Trust Services Criteria - CC1.4. This trust principle stipulates, "COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives." Microsoft is regularly audited by independent third-party assessors to assess the effectiveness of the processes and controls related to personnel training.

2.3.4 Documented information

The QMS defines and manages the quality standard that serves to protect the confidentiality, integrity, availability, and security of critical documents and data. A documentation and records management procedure governs the complete lifecycle of system documents, from creation to approval, distribution, and withdrawal.

System documents, including SOPs, security and hardening standards, network and facility diagrams, and system build-out documentation are maintained in a secure internal site and made available to authorized personnel. Access to system documentation is restricted to the respective Microsoft teams based on their job roles. Documents are subject to levels of protection that are appropriate to their classification level.

Documents are vetted using an approval process and reviewed periodically per the Microsoft Responsibility Matrix for Documents to ensure accuracy. Documents are kept in accordance with a corporate retention policy.

Recordkeeping and retention processes have been implemented to ensure the retrievability, storage, and protection of various types of records, including:

- Technical documents
- Data dictionaries
- Systems design documents
- System procedures
- Operational protocols for data recovery
- Systems security protocols
- Documents for system support
- Troubleshooting documentation
- Support metrics and trending
- Training records
- Testing records
- Change records
- Third-party vendor audit records

These records are periodically reviewed as part of Microsoft internal auditing activities, as well by external third-party auditors during SOC audits and ISO certification processes.

2.3.5 Design and development of Dynamics 365 products and services

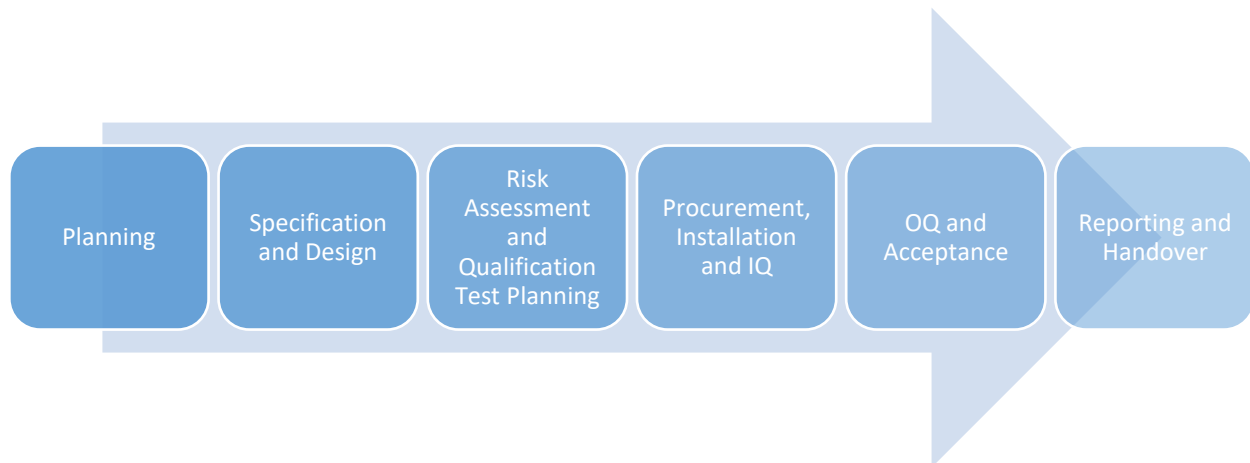
Traditionally, the regulated company has been responsible for all aspects of their IT infrastructure, such as physical security, environmental controls, and server and network management. In contrast, with the cloud service model, the regulated company must rely on cloud vendors to properly manage the IT infrastructure services they provide.

Microsoft understands that IT infrastructure qualification is an essential aspect of GxP computerized system compliance for the life sciences industry. The ISPE *GAMP Good Practice Guide for IT Infrastructure Control and Compliance (Second edition)* defines qualification as “a process of demonstrating the ability of an entity to fulfill specified requirements. In the context of an IT Infrastructure, this means demonstrating the ability of components such as servers, clients, and peripherals to fulfill the specified requirements for the various platforms regardless of whether they are specific or of a generic nature.” (Ref. [8]). According to GAMP guidance, the following critical elements should be considered during IT infrastructure qualification:

- Supplier assessment and management
- Installation and operational qualification of infrastructure components (including facilities)
- Configuration management and change control of infrastructure components and settings in a highly dynamic environment
- Management of risks to IT infrastructure
- Involvement of service providers in critical IT infrastructure processes
- Service level agreements with XaaS (that is, IaaS, PaaS, SaaS) providers and third-party datacenter providers
- Security management in relation to access controls, availability of services, and data integrity
- Data storage, and in relation to this security, confidentiality, and privacy
- Backup, restore, and disaster recovery
- Archiving

Microsoft teams have implemented a series of processes and technical controls that deal with these critical elements related to infrastructure qualification. Many of the activities commonly performed during a qualification effort are governed by the Security Development Lifecycle (SDL) and Dynamics 365 change and release management processes. The fundamental goal of these processes is to ensure Dynamics 365 components can satisfy their specified requirements and quality standards consistently and reliably.

For the benefit of Microsoft life sciences customers, we have mapped the vital activities performed as part of the Dynamics 365 internal development, operations, and quality practices to the phases of the GAMP IT Infrastructure Life Cycle Model, as depicted in the following graphic.



2.3.5.1 Planning

The processes governed by the Security Development Lifecycle (SDL) as well as the change and release management processes require teams to produce plans before taking any action that may affect the security or functionality of the platform. During the engineering planning phase, business goals, priorities, and scenarios are identified and agreed upon through a series of detailed requirements, operational planning, and test plans, which are managed within various test planning tools, including Team Foundation Server. Planning is divided into semesters with built-in checkpoints, which are driven by improvements in quality of existing product and innovation (that is, development of new features).

2.3.5.2 *Specification and design*

The SDL and change and release management processes also govern how the Dynamics 365 development teams work with various stakeholders to collect requirements and develop design documentation for each feature.

The generic nature of the Dynamics 365 online services components and service offerings was designed to support a broad spectrum of customer needs across multiple industries, including many of which are heavily regulated. The overarching business goal of the platform is to provide customers with a secured and controlled environment that encompasses the following requirements:

- **Confidentiality:** Ensuring that information is secure and accessible only to those authorized to have access
- **Integrity:** Safeguarding the consistency, accuracy, and completeness of information and processing methods
- **Availability:** Ensuring that authorized users have access to information and associated assets when required

Microsoft [Operational Security Assurance](#) (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape, and data from industry standard tools. OSA defines the aspects of these domains by first establishing baseline requirements that each service should meet or exceed. These baseline requirements are then used to establish a test plan that can be used to validate a service's security during an assessment.

Operational Security Assurance (OSA) consists of a set of practices that aim to improve operational security in cloud-based infrastructure:

1. Provide Training
2. Use Multi-Factor Authentication
3. Enforce Least Privilege
4. Protect Secrets
5. Minimize Attack Surface
6. Encrypt Data in Transit and at Rest
7. Implement Security Monitoring
8. Implement A Security Update Strategy
9. Protect Against DDOS Attacks
10. Validate the Configuration of Web Applications and Sites
11. Perform Penetration Testing

The three key processes of OSA are:

- Ensuring that OSA inputs (such as organizational learning, threat intelligence, and security technologies) are up-to-date and relevant
- Developing and applying centralized review processes to consolidate all requirements to establish the OSA baseline requirements
- Engaging and implementing the new requirements and baselines

After the baseline requirements are defined, the OSA team can test services, both before and during operation. OSA requirements for some domains involve collecting documentation or training staff to ensure that they have skills that ensure work of appropriate quality. Requirements for other domains

can take advantage of automated solutions that demonstrate operational baseline requirements are being addressed.

To ensure quality is embedded into the design of Dynamics 365 environment, it is important to have a strong understanding of the data flow. Physical network diagrams are maintained for all Microsoft datacenters, with general data flows that provide functional level detail on load balancers, routers, firewalls, and other network infrastructure. Diagrams are stored in a secured location with access restricted to the appropriated individuals.

2.3.5.3 Risk assessment and qualification test planning

The Risk Management Program provides a structured approach to identifying, prioritizing, and directing risk management activities for the Microsoft cloud infrastructure. The methodology is based on the ISO/IEC 27005: Information Security Risk Management standard and National Institute of Standards and Technology (NIST) Special Publication 800-53 in support of government requirements, such as the Federal Risk and Authorization Management Program (FedRAMP).

The Risk Management Program consists of six processes:

1. **Establish context:** Setting the context or scope of the risk assessment includes establishing many characteristics before beginning the assessment to ensure appropriate data is collected and evaluated. The type of details captured while determining the assessment context include: the geographical locations of the information assets and equipment; how information is exchanged internally and with external parties; and what legal, regulatory, policy, and contractual requirements apply given the locations involved.
2. **Identify critical assets:** After the risk assessment context has been established, asset owners evaluate which assets are critical and which are not in a process that often reuses analyses conducted for asset management or business continuity planning efforts. The assets considered include:
 - a) **Primary assets:** Business processes, activities, and information
 - b) **Supporting assets:** Hardware, software, network devices, personnel, and facilities
3. **Identify risks:** Workshops or interviews are used to solicit input from asset owners and business managers in teams that support the given scope of the assessment. Also, operational data is evaluated to identify risks.
4. **Assess risks:** The potential business impact and the likelihood of occurrence are investigated in this phase, which also includes looking for and estimating the effectiveness of potential controls that are used to reduce or eliminate the impact of risks.
5. **Report and review risks:** Provide management with the data to make effective business decisions. This phase includes risk determination, including whether to take measures to avoid, reduce, transfer, or accept risks.
6. **Treat and manage risks:** This phase involves identifying accountable risk owners and applying risk treatment plans to those risks that management decided to reduce, transfer, or avoid in the previous phase. Possible treatments include authorizing special projects intended to address those risks.

Detailed test planning is performed in accordance with the SDL and Dynamics 365 change and release management processes.

2.3.5.4 Procurement, installation, and IQ

As a prerequisite of the procurement process, supplier scorecards have been developed to allow comparison and visibly monitor the performance of Microsoft suppliers using a balanced scorecard approach.

Internal teams work together to protect against supply chain threats throughout the supply chain lifecycle, which includes creating purchase orders, accelerating deliveries, performing quality checks, processing warranty claims, and obtaining spares. Third-party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Microsoft personnel, and included in signed contractual agreements prior to engaging in third-party services. The engaging team within Microsoft is responsible for managing their third-party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.

The Business Applications Group controls the installation and removal of information system components through the datacenter operations ticketing system. Installation and removal of information system components are authorized by system owners. A formal policy has been implemented that requires assets (the definition of asset includes data and hardware) used to provide Dynamics 365 online services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets.

For critical hardware components, manufacturers are required to perform previously agreed upon tests before delivery of the hardware. After delivery, hardware qualification tests are conducted in a non-production environment using synthetic workloads to stress-test the hardware and to ensure the hardware meets its specifications.

The Cloud + AI Security team develops security configuration standards for systems in the physical environment that are consistent with industry-accepted hardening standards. These configurations are documented in system baselines and are reviewed annually, and relevant configuration changes are communicated to affected teams.

Dynamics 365 has a server onboarding procedure that begins once the machines are released to Dynamics 365 from Azure. Dynamics 365 maintains appropriate supplementary settings and configurations for the different classes of server used – front-end web servers, application servers, database servers, and management servers. The baselines for each service are maintained in version control tools.

2.3.5.5 OQ and acceptance

Formal functional, security, and quality assurance testing is performed before software is released through each pre-production environment (that is, development and staging) based on defined acceptance criteria. The results of the quality assurance testing are reviewed and approved by the appropriate representatives before moving the release to production.

The Microsoft [Security Development Lifecycle \(SDL\)](#) encompasses multiple phases of development activities, including robust software testing/verification, to ensure developers build secure software and address security compliance requirements. The verification phase of the SDL includes the following types of tests, as applicable:

- **Dynamic analysis:** Consists of performing run-time verification checks of software functionality using tools that monitor application behavior for memory corruption, user privilege issues, and other critical security problems.
- **Fuzz testing:** Consists of inducing program failure by deliberately introducing malformed or random data to reveal potential security issues before release.
- **Attack surface review:** Consists of reviewing attack surface measurement upon code completion to ensure that any design or implementation changes to an application or system have been considered and that any new attack vectors created because of the changes have been reviewed and mitigated including threat models.

The SDL incorporates within it a detailed set of procedures that encompass how each Dynamics 365 product release is tested throughout a series of quality gates. This testing is managed and documented within software development tools, such as Team Foundation Server.

As part of the acceptance process, Dynamics 365 software releases are reviewed for their adherence to established change and release management procedures before closure. After deployment, releases are monitored for success; failed implementations are immediately rolled back, and the release is not considered complete until it is implemented and verified to operate as intended. Similarly, hardware and network changes have established verification steps to evaluate adherence with the build requirements.

Testing records are kept in accordance with a corporate retention policy.

[2.3.5.6 Reporting and handover](#)

A release manager receives notification when a release is ready for deployment into the specified target environment and verifies that release prerequisites are satisfied before approving the release job for the target environment. Each stage of the release management process has specific entry and exit criteria, which are tracked and signed-off electronically by the respective component teams. A pre-acceptance review is performed on all releases before final acceptance in the release pipeline.

[2.3.6 Operations management](#)

The following sections provide an overview of Microsoft processes and controls corresponding to the topics as recommended within *GAMP Guidance for IT Infrastructure Control and Compliance* (Ref. [8]).

[2.3.6.1 Change management](#)

A change management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It also controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Dynamics 365 service teams provide oversight for change control via the change management processes through peer and managerial reviews depending on the type of change. Major system changes must be approved in a Governance Risk Compliance (GRC) review which serves as the Dynamics 365 committee before implementation into the environment.

The change management process governs the following activities:

- Identification and documentation of planned changes
- Identification of business goals, priorities, and scenarios during product planning
- Specification of feature/component design
- Operational readiness review based on predefined criteria/checklist to assess overall risk/impact
- Testing, authorization, and change management based on entry/exit criteria for DEV (development), INT (Integration Testing), STAGE (Pre-production), and PROD (production) environments as appropriate.

A centralized ticketing tool has been implemented to document changes and their approvals. Change records are kept in accordance with a corporate retention policy.

2.3.6.1.1 Software and configuration changes

Software and configuration changes include major releases, minor releases, and hotfixes. Change requests are documented, assessed for their risks, evaluated, and independently approved for acceptance by the designated Microsoft personnel. Changes are requested, approved, tracked, and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment, and post-deployment support phases.

Changes made to the source code are controlled through an internal source code repository. The tool tracks the identity of the person who checks source code out and what changes are made. Permission to make changes to the source code is provided by granting write access to the source code branches, which limits the access to confined project boundaries per job responsibilities. In addition, source code builds are scanned for malware prior to production release.

Formal security and quality assurance tests are performed before release through each pre-production environment (that is, development and stage) based on defined acceptance criteria. The results of the quality assurance testing are independently reviewed and approved by the appropriate individual before moving the release to production.

Changes are reviewed for their adherence to established change and release management procedures before closure. After being deployed, changes are monitored for success; failed implementations are immediately rolled back, and the change is not considered complete until it is implemented and verified to ensure intended operation. Automated mechanisms are used to perform periodic integrity scans and detect system anomalies or unauthorized changes.

Microsoft maintains and notifies customers of potential changes and events that may affect security or availability of the services through an online [Service Dashboard](#).

2.3.6.1.2 Hardware changes

Hardware changes are managed through formal change and release management procedures and a centralized ticketing system. The Azure Build-Out Team evaluates hardware changes against the release entrance criteria, which forms the acceptance criteria for build-out of hardware. As with software changes, infrastructure changes are discussed and planned through daily meetings with representatives from service and component teams.

The Azure Build-Out Team coordinates the change release and deployment into the production environment. The Team performs the build-out of hardware devices and post build-out verification in conjunction with the Azure Deployment Engineering Team to verify adherence with the hardware build requirements for new clusters. Azure Operations Managers perform a final review, sign off on new deployments, and the Azure Build-Out Team closes the ticket.

2.3.6.1.3 Network changes

Network changes include configuration changes, emergency changes, access control list (ACL) changes, patches, and new deployments. ACL changes that are identified and categorized as standard are considered as pre-approved and may be implemented on peer review. Non-standard changes are reviewed for their characteristics and risks, and independently approved by representatives from the Cloud + AI Security and Networking Teams. Reviews and approvals are also tracked in a centralized ticketing system. Changes are performed by authorized change implementers who are part of a designated security group. Independent qualified individuals perform post-change reviews to evaluate the change success criteria.

2.3.6.2 Configuration management

Configuration changes to the Dynamics 365 online services are tested based on established criteria prior to production implementation.

Technical standards and baselines have been established and communicated for operating system deployments. Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions and deviations from the baseline in the production environment.

Operating system and component teams review and update configuration settings and baseline configurations at least annually.

2.3.6.3 Information security and access management

A security policy has been established that defines the information security rules and requirements for the service environment. Microsoft performs periodic information security management system (ISMS) reviews and results are reviewed with management. This process involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

The Dynamics 365 online services are specially designed and architected to prevent the possibility of production data being moved or replicated outside of the Dynamics 365 cloud environment. These controls include:

- Physical and logical network boundaries with strictly enforced change control policies

- Segregation of duties requiring a business need to access an environment
- Highly restricted physical and logical access to the cloud environment
- Strict controls based on [SDL](#) and [Operational Security Assurance](#) (OSA) that define coding practices, quality testing, and code promotion
- Ongoing security, privacy, and secure coding practices awareness and training
- Continuous logging and audit of system access
- Regular compliance audits to ensure control effectiveness

To help combat emerging and evolving threats, Microsoft employs an innovative assume breach strategy and uses highly specialized groups of security experts, known as the Red Team, to strengthen threat detection, response, and defense for its enterprise cloud services. Microsoft uses Red Teaming and live site testing against Microsoft managed cloud infrastructure to simulate real-world breaches, conduct continuous security monitoring, and practice security incident response to validate and improve the security of Dynamics 365.

The Cloud + AI Security Team carries out frequent internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. Services are scanned for known vulnerabilities; new services are added to the next timed quarterly scan, based on their date of inclusion, and follow a quarterly scanning schedule thereafter. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify vulnerabilities. The scanning reports are reviewed by appropriate personnel and remediation efforts are promptly conducted.

All unused IO ports on edge production servers are disabled by operating system-level configurations that are defined in the baseline security configuration. Continuous configuration verification checks are enabled to detect drift in the operating system-level configurations. In addition, intrusion detection switches are enabled to detect physical access to a server.

Procedures to investigate and respond to malicious events detected by the Microsoft monitoring system in a timely manner have been established.

Microsoft employs the principles of separation of duties and [least privilege](#) throughout Microsoft operations. Access to customer data by Microsoft support personnel requires customer's explicit permission and is granted on a "just-in-time" basis that is logged and audited, then revoked after completion of the engagement.

Within Microsoft, operations engineers and support personnel who access its production systems use hardened workstation PCs with virtual machines (VMs) provisioned on them for internal corporate network access and applications (such as email, intranet, and so on). All management workstation computers have [Trusted Platform Modules \(TPMs\)](#), the host boot drives are encrypted with BitLocker, and they are joined to a special organizational unit (OU) in the primary Microsoft corporate domain.

System hardening is enforced through Group Policy, with centralized software updating. For auditing and analysis, event logs (such as security and AppLocker) are collected from management workstations and saved to a central location. In addition, dedicated jump-boxes on the Microsoft network that require two-factor authentication are used to connect to the Dynamics 365 production network.

2.3.6.4 *Server management*

Server management relates to the ability to manage information stored on servers. This function is accomplished through the implementation of various processes performed on the servers, which include:

- Server security (→ see **Section 2.3.6.3**)
- Data backup (→ see **Section 2.3.6.9**)
- Monitoring (→ see **Section 2.3.6.11**)

2.3.6.5 *Client management*

Microsoft staff must adopt and follow appropriate security practices when using mobile computing devices such as phones, tablets, and laptops to protect against the risks of using mobile equipment. Such risks relate to the mobile nature of these devices, and the security practices adopted by Microsoft to mitigate these risks may include, but are not limited to, mobile device physical protection, access controls, cryptographic requirements, and malware protection.

Physical as well as logical controls must be put in place to ensure the security of the remote site is comparable to primary work facilities. Microsoft staff who connect remotely must adhere to applicable remote access policies for gaining access to Microsoft networks.

2.3.6.6 *Network management*

The Azure Networking Team maintains a logging infrastructure and monitoring processes for network devices. Given the impact on both security and availability, Azure requires a proactive and real-time method for detecting and fixing errors in the network connectivity policies. The Networking Team has developed a monitoring infrastructure that uses a tool for continuously verifying network policies.

2.3.6.7 *Incident and problem management*

An incident management framework has been established with defined processes, roles, and responsibilities for the detection, escalation of, and response to incidents. Incident management teams perform 365x24x7 monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. Events, thresholds, and metrics have been defined and configured to detect incidents and alert the appropriate teams.

Microsoft's logging and monitoring infrastructure encompasses the Dynamics 365 online services and does not vary by tenant. Detected incidents are isolated or contained most effectively depending on the nature of the event. Incidents that require a change would then go into the standard change process (which can include emergency changes). Incident records are kept in accordance with a corporate retention policy.

Microsoft has developed robust processes to facilitate a coordinated response to a security incident if one was to occur. A security incident may include, among other things, unauthorized access resulting in loss, disclosure, or alteration of data. Security incident response plans and collection of evidence adheres to ISO/IEC 27001 standards. Microsoft has also established processes for evidence collection and preservation for troubleshooting incidents and analyzing their root cause.

In addition, Microsoft has established procedures to receive, generate, and disseminate security alerts from external organizations, as necessary. The [Security Incident Response Lifecycle](#) consists of the activities described in the following table:

Phase	Activity description
1 - Detect	First indication of an event investigation.
2 - Assess	An on-call incident response team member assesses the impact and severity of the event. Based on the evidence, the assessment may or may not result in further escalation to the security response team.
3 - Diagnose	Security response experts conduct the technical or forensic investigation and identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, parallel execution of the Customer Incident Notification process begins in parallel.
4 - Stabilize, Recover	The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining affected systems may occur immediately and in parallel with the diagnosis. Longer term mitigations may be planned that occur after the immediate risk has passed.
5 - Close/ Postmortem	The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the incident.

Microsoft maintains a Customer Support website that describes the process for customers and other external users to inform about potential security issues and submit complaints. Reported issues are reviewed and addressed per documented incident management procedures.

[2.3.6.8 Help Desk](#)

Microsoft provides delivery guidance for activities performed by account managers and field engineers. The guidance helps the service team successfully plan, deliver, and manage proactive and reactive services with measurable outcomes for on-premises IT infrastructure optimization, cloud productivity, and developer application quality.

[2.3.6.9 Backup, restoration, and archiving](#)

The backup, restoration, and archiving process defines activities for initiating, applying, monitoring, restoring, and testing the backup process for servers and data. Backups are managed by the Azure Data Protection Services (DPS) team and scheduled on a regular frequency established by the respective component teams.

The DPS Team has implemented a secure backup system infrastructure to provide secure backup, retention, and restoration of data in the Microsoft Online Services environment per documented procedures. Data is encrypted prior to backup and in transit where applicable.

Backup restoration tests and integrity checks are performed periodically by appropriate individuals. Results of the tests are captured, and any findings are tracked to resolution.

2.3.6.10 Disaster recovery

Microsoft has established an organization-wide enterprise business continuity management (EBCM) framework that serves as a guideline for developing the Business Continuity and Disaster Recovery Program. The program includes business continuity policy, a disaster recovery plan (DRP), implementation guidelines, business impact analysis (BIA), risk assessment, dependency analysis, a business continuity plan (BCP), an incident management plan, and procedures for monitoring and improving the program.

The DRP is used by Azure incident managers for recovering from high-severity incidents (disasters) for its critical processes.

The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.

Disaster recovery is a feature of Dynamics 365 to recover from a planned or unplanned service interruption. An example of a planned service interruption is regular and periodic data center system maintenance. An example of an unplanned service interruption is a failure of a key computer system or network component in a data center.

Planned service interruptions are preceded by a public notice in the web application or Dynamics 365 for Outlook identifying the date and time of the service maintenance so that customers can plan for the interruption in accessing their organization's data. Unplanned service interruptions result in a notice that the organization is currently undergoing unplanned maintenance.

When a failure or a disaster occurs, well-defined processes are applied by the administrators of the Dynamics 365 data center to recover from a service interruption. The processes and software to recover from these service interruptions is known as disaster recovery failover. Dynamics 365 data centers maintain a duplicate and synchronized (alternate) copy of the customer's data on a different server. Should a disaster occur in the data center where customers no longer have access to their data, the administrators monitoring the data center can switch access from the primary organization to this alternate organization, thereby minimizing the service interruption. When the failure has been corrected, service access to the primary organization can be restored.

Production environments are configured with Azure disaster recovery support that includes the following:

- Azure SQL active-geo replication for primary databases, with a Recovery Point Estimate (RPO) of < 5 seconds. For more information, see [Overview: Failover groups and active geo-replication](#).
- Geo-redundant copies of Azure blob storage (containing document attachments) in other Azure regions.
- Same secondary region for the Azure SQL and Azure blob storage replication.

2.3.6.11 Performance monitoring

Several system and application performance monitoring tools are used to monitor network devices, servers, services, and application processes. Multiple levels of monitoring, logging, and reporting are implemented to ensure secure execution of services running in the Dynamics 365 environment. Reporting on these metrics drives continuous improvement of the services and the overall information security management system (ISMS), which is continuously adapted to the evolving environment.

The following operational processes are in place:

- Proactive capacity management based on defined thresholds or events
- Hardware and software subsystem monitoring for acceptable service performance and availability, service utilization, storage utilization, and network latency

Microsoft employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, the network backbone, internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause.

Proactive monitoring continuously measures the performance of critical subsystems of the Microsoft Cloud services platform against the established boundaries for acceptable service performance and availability.

2.3.6.12 Supplier management

Contracts are in place with Microsoft suppliers to identify responsibilities and ensure that procedures are followed to periodically monitor and review activities for inconsistencies or non-conformance. Third-party suppliers are required to comply with Microsoft security policies and undergo a review process through Global Procurement. An approved supplier list has been established and supplier audit records are kept in accordance with a corporate retention policy.

Purchase orders to engage a third party require a Microsoft Master Vendor Agreement (MMVA) to be established or a review to be performed by Corporate, External, and Legal Affairs (CELA). In addition to an MMVA, a signed NDA is also required.

Vendors who require access to source code need to be approved by the General Manager (GM) and CELA and sign a Source Code Licensing Agreement. Third parties have the same obligations as Microsoft employees when managing customer data.

2.3.6.13 System retirement

Measures are in place to ensure the secure disposal and complete removal of data from all storage media, ensuring that data is not recoverable by any computer forensic means.

Hard disk drive destruction guidelines have been established for the disposal of hard drives. Offsite backup tape destruction guidelines are established, and destruction certificates are retained for expired backup tapes.

When customers delete data or leave Dynamics 365, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

2.3.7 Performance evaluation

The Azure Global and Compliance Team has implemented a robust monitoring program to actively monitor, identify, correct, and prevent system and product non-conformities. The process includes identifying key performance indicators (KPIs) to adequately measure performance and effectiveness across the QMS. Independent-entity managed assessments are conducted over the design and operating effectiveness of the control environment—these assessments allow monitoring and measurement to determine the effectiveness of the operating controls.

As part of continuous monitoring, Microsoft documents are updated to reflect any newly identified or remediated security issues. In addition, all identified vulnerabilities are tracked through closure using the vulnerability scanning processes.

Microsoft has an internal audit function that reports directly to the Audit Committee of the Board of Directors, which is constituted solely of independent directors. The Azure Global and Compliance Team, which manages the information security management system (ISMS), ensures that cloud services are secured, meet the privacy requirements of our customers, and comply with complex global regulatory requirements and industry standards.

Regular audits performed by qualified assessors and accredited third-party assessment organizations for ISO (20000, 27001, 27018, and 9001), SOC (1, 2, and 3), PCI, and FedRAMP demonstrate Microsoft's continued compliance with established standards. Audit reports provide documentation of compliance observations, which the change authorization board (CAB) reviews for continuous improvement of the ISMS. When changes to the ISMS are required, they are executed by the CAB or through service team-specific change management procedures.

2.3.8 Improvement

The Information Security Management Forum (ISMF) acts as the governance program within the ISMS and performs periodic reviews, the results of which are reviewed with management. The review involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. As with the other programs in the ISMS, the ISMF is organized to align with the ISO/IEC 27001 standard. Applying the practices defined in ISO/IEC 27001 enables Microsoft cloud infrastructure teams to consolidate and improve information security governance efforts.

The ISMF consists of a series of regularly scheduled management meetings throughout the year that are designed to review key aspects of program governance. Certain meetings enable senior management to focus on long-term strategies while other meetings address the short-term tactics being used to manage information security risks.

Elements of these meeting series have been formalized to ensure attendance by the appropriate managers and service owners, particularly when they are responsible for providing a report or hold decision-making authority.

3 Considerations for satisfying GxP requirements

Achieving a compliant cloud-based solution requires well-defined controls and processes, with shared responsibilities between Microsoft Dynamics 365 and our customers. As discussed in previous sections, Dynamics 365 teams have implemented a series of technical and procedural controls to help ensure the dependability (availability, reliability, security, integrity, accessibility, and maintainability) of Dynamics 365 systems and services.

Since data integrity is one of the most crucial aspects of any cloud-based system, -- and one which many regulatory agencies around the world are increasingly focused on; we will begin by looking at the data integrity controls available to Dynamics 365 customers and how these controls can be used to help support their GxP compliance requirements.

3.1 Data integrity controls

Data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA). To ensure data integrity, it is essential to have control over the people, processes, systems, and environment in which records are generated/managed and a strong understanding of the data flow.

Data integrity is an essential element of GxP compliance, and in recent years, several regulatory agencies around the world have published draft guidance related to this topic:

- [FDA - Data Integrity and Compliance with CGMP - Guidance for Industry \(April 2016\)](#)
- [MHRA - GXP Data Integrity Definitions and Guidance for Industry \(March 2018\)](#)
- [WHO - Guidance on Good Data and Record Management Practices \(May 2016\)](#)
- [PIC/S \(PI 041-1\): Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments \(Draft3 – November 2018\)](#)

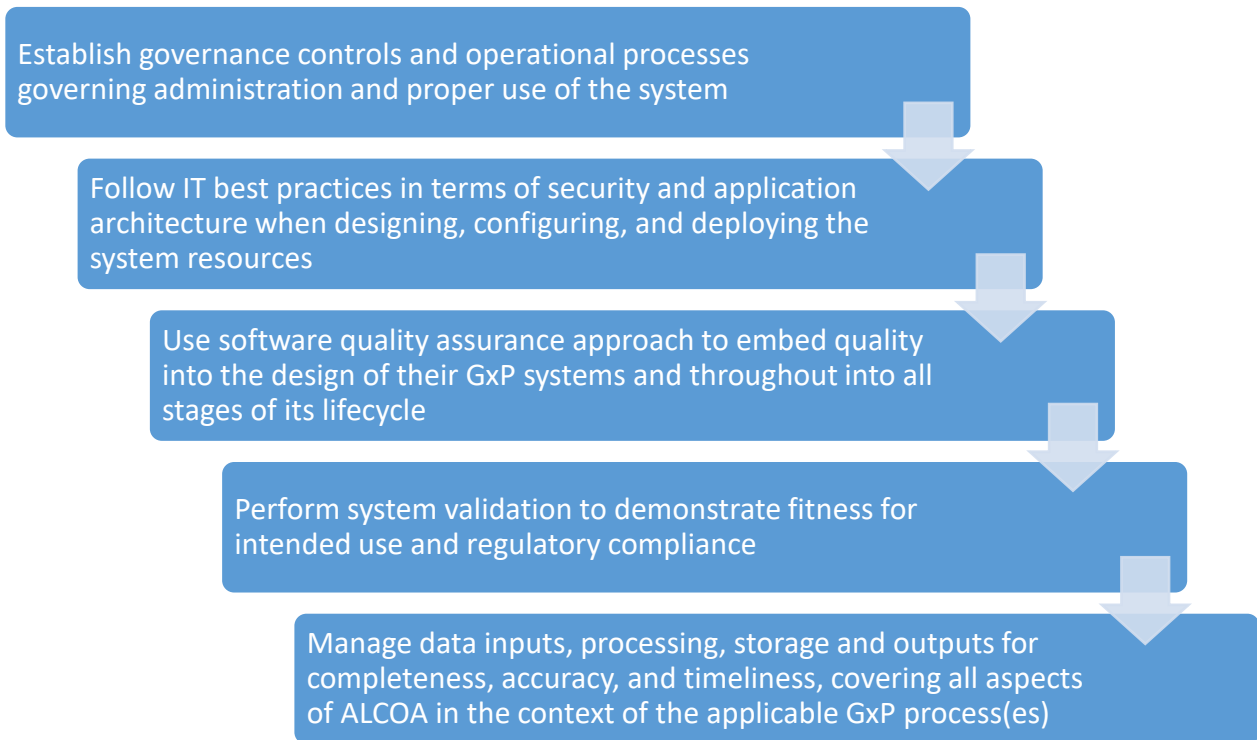
Various GxP regulations, such as [21 CFR Part 11](#), [21 CFR Part 211](#), [21 CFR Part 212](#), [EudraLex Annex 11](#), [ICH Q7](#) and [HIPAA](#), as well as international standards such as [ISO 27001](#), lay out requirements and safeguards for data protection and data integrity. It is a shared responsibility between Microsoft and our GxP regulated customers to implement sufficient mechanisms to meet these obligations.

Specifically, Microsoft provides a secure, compliant platform for services, applications, and data. The integrity of customer data within Dynamics 365 is protected by a variety of technologies and processes, including various forms of logical security controls and encryption. Furthermore, Microsoft follows industry best practices for infrastructure control, software development, service delivery and has implemented robust risk and quality management processes to assure quality of delivered products and services.

Customers must design, configure and manage their cloud environment to ensure the [security, confidentiality and integrity](#) of their information assets. Dynamics 365 includes several services and capabilities which provide a foundation for control of data integrity, privacy, security, and availability. Together with a well-defined cloud governance model (→ see **Section 3.2**) and computer system

validation program (→ see **Section 3.4**), life sciences customers can demonstrate their GxP applications have been designed with proper data integrity controls.

Customers should also consider the following activities as part of their compliance strategy to help ensure overall integrity of systems and data stored within Dynamics 365:



3.1.1 Considerations for FDA 21 CFR Part 11 compliance

The following sections highlight some of the Dynamics 365 features and capabilities that customers can leverage to support requirements of the FDA’s [21 CFR Part 11 \(Subpart B\)](#) regulations pertaining to the management of electronic records.

3.1.1.1 *Validation of systems [21 CFR Part 11.10 (a)]*

As described in **Sections 2.3.5** and **2.3.6**, Microsoft has implemented a series formal controls governing the design, development, delivery and operation of the Dynamics 365 software and hardware. Formal quality assurance testing is performed prior to the software release based on defined acceptance criteria. The results of the quality assurance testing are reviewed and approved by the appropriate representatives prior to moving the release to production. Changes are reviewed for their adherence to established change and release management procedures prior to closure. The change is not considered as completed until it is implemented and validated to operate as intended.

Any application that supports GxP processes subject to FDA regulations should be assessed by the customer as to whether it generates or manages (that is, creates, modifies, maintains, archives, retrieves, or distributes) electronic records based on FDA 21 CFR Part 11 [regulations](#) and [guidance](#). The outcome of the assessment and intended use of the application should determine which regulatory

requirements are applicable and which functional capabilities will be validated to ensure proper functionality and data integrity.

[Lifecycle Services \(LCS\) for Microsoft Dynamics](#) is a collaboration portal that provides an environment and a set of regularly updated services that can help customers manage the application lifecycle of their Microsoft Dynamics 365 for Finance and Operations implementations.

[Azure DevOps](#) is a SaaS application hosted by Microsoft that customers can leverage as part of their system validation toolset. It provides the ability to support the entire system lifecycle including planning, development, testing, delivery, operation and change management.

→ See **Section 3.4** for additional recommendations

[3.1.1.2 Generation of accurate and complete copies of records \[21 CFR Part 11.10 \(b\)\]](#)

To generate accurate and complete copies of records contained within Dynamics 365, customers can also leverage the Dynamics 365 [Data Export Service](#). The Data Export Service is an add-on service made available on Microsoft AppSource that synchronizes Microsoft Dynamics 365 data to a Microsoft Azure SQL Database store in a customer-owned Microsoft Azure subscription. Data Export intelligently synchronizes the entire Dynamics 365 schema and data initially and thereafter synchronizes on a continuous basis as changes occur (delta changes) in the Dynamics 365.

Regardless of the mechanism used, it is important for customers to ensure they can extract accurate and complete copies of the electronic records stored within their systems and applications, as needed based on applicable regulatory requirements.

[3.1.1.3 Protection of records throughout the records retention period \[21 CFR Part 11.10 \(c\)\]](#)

Customers are responsible for defining the retention period of their records in accordance with regulatory, legal, or other business requirements.

There are several Dynamics 365 capabilities that can be used to support the protection of records to enable their accurate and ready retrieval, including: Data Segregation, Data Encryption and Data Backup.

- **Data Segregation:** Microsoft works continuously to ensure that the multi-tenant architecture of Dynamics 365 supports security, confidentiality, privacy, integrity, and availability standards. Microsoft cloud services were designed with the assumption that all tenants are potentially hostile to all other tenants, and we have implemented security measures to prevent the actions of one tenant from affecting the security or service of another tenant, or accessing the content of another tenant.

The two primary goals of maintaining tenant isolation in a multi-tenant environment are:

- Preventing leakage of, or unauthorized access to, customer content across tenants; and
- Preventing the actions of one tenant from adversely affecting the service for another tenant

Multiple forms of protection have been implemented throughout Dynamics 365 to prevent customers from compromising Dynamics 365 services or applications or gaining unauthorized

access to the information of other tenants or the Dynamics 365 system itself, including logical isolation of customer content within each tenant for Dynamics 365 services is achieved through Azure Active Directory authorization and role-based access control, as well as storage level provides data isolation mechanisms.

- **Data Encryption:** [Multiple encryption methods](#), protocols, and algorithms are used to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure, including:
 - Encryption of data in transit to protect data while it transferred between customers and Microsoft datacenters. All public endpoints are secured using industry-standard TLS. TLS effectively establishes a security-enhanced browser-to-server connection to help ensure data confidentiality and integrity between desktops and datacenters.
 - All instances of Dynamics 365 use [Microsoft SQL Server Transparent Data Encryption](#) (TDE) to perform real-time encryption of data when written to disk (at rest).
- **Data Backup:** Backups of information system documentation, as well as user-level information contained in Dynamics 365 information system consists of daily incremental and weekly full backups. Critical information and services are deployed in redundant data centers in an active-active configuration. Full backups of system-level information contained in Dynamics 365 information system are performed on weekly basis. The confidentiality, integrity, and availability of backup information is protected in all storage locations.

[3.1.1.4 Limiting system access to authorized individuals \[21 CFR Part 11.10 \(d\)\]](#)

Limiting system access to authorized individuals is an essential requirement for GxP-regulated applications. [Azure Active Directory](#) provides identity management and access control for Dynamics 365. Azure Active Directory provides the ability to require [multi-factor authentication](#) as a means of further enhancing security around user access to the platform infrastructure, services, and data.

[Conditional Access policies](#) can further enhance access control by blocking or granting user access based on the following criteria:

- Requiring multi-factor authentication for users with administrative roles
- Requiring multi-factor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Requiring trusted locations for Azure Multi-Factor Authentication registration
- Blocking or granting access from specific locations
- Blocking risky sign-in behaviors
- Requiring organization-managed devices for specific applications

[3.1.1.5 Secure, computer-generated, time-stamped audit trails \[21 CFR Part 11.10 \(e\)\]](#)

Dynamics 365 has a built-in [audit feature](#) that provides the ability to track changes made to data records, as well as each time a user accesses Dynamics 365. The auditing feature is designed to meet the auditing, compliance, security, and governance policies of many regulated enterprises. Once configured, the auditing feature may be used to:

- Analyze the history of changes (create, read, update, delete) on records

- Changes to the sharing privileges of a record
- Changes to security roles
- Audit changes at the entity, attribute, and organization level. For example, enabling audit on an entity

Dynamics 365 information system protects audit information and audit tools from unauthorized access, modification, and deletion.

[3.1.1.6 Enforcing permitted sequencing of events \[21 CFR Part 11.10 \(f\)\]](#)

Customers must identify their requirements when it comes to establishing the permitted sequencing of steps and events depending on their use case and GxP process(es) supported by their GxP application. Dynamics 365 provides a [customizable workflow tool](#) that customers can use to support their process automation needs.

A workflow can be configured help support or control a wide array of business and GxP processes. If a specific workflow is used to support of critical or high-risk process, it should be validated in accordance with the customer's computer system validation policy or procedure, to ensure the workflow functions correctly and that it is fit for its intended use.

[3.1.1.7 Authority checks \[21 CFR Part 11.10 \(g\)\]](#)

[Security roles and privileges](#) can be specified within Dynamics 365 to ensure users can only perform permitted activities based on their role or job function. Depending on the business process and specific use case, various controls can be used to define which tasks a user can perform record on a record, including:

- **Role-based security** provides the ability to group together a set of privileges that limits the tasks which can be performed by a given user. This is an important capability, especially when people change roles within an organization.
- **Record-based security** provides the ability to restrict access to specific records.
- **Field-level security** provides the ability to restrict access to specific high-impact fields, such as personally identifiable information (PII).

[Azure Active Directory \(Azure AD\)](#) helps protect each instance of Dynamics 365 from unauthorized access by simplifying the management of users and groups and facilitating the assignment and revoking of privileges. Azure AD includes tools such as Multi-Factor Authentication for highly-secure sign-in. Additionally, [Azure AD Privileged Identity Management](#) helps reduce risks associated with administrative privileges through access control, management, and reporting.

[3.1.1.8 Device checks \[21 CFR Part 11.10 \(h\)\]](#)

Customers must determine whether there is a need to implement device checks, where certain devices have been selected as legitimate sources of data input or commands. [Azure AD Conditional Access](#) and [Azure AD device management](#) can be used together to ensure access to resources in the customers environment is only possible with managed devices. Devices in Azure Active Directory can be managed using Mobile Device Management (MDM) tools like Microsoft Intune, Microsoft Endpoint Configuration Manager, Group Policy (hybrid Azure AD join) and Mobile Application Management (MAM) tools.

[Azure Storage firewalls and virtual networks](#) can be also used to limit access to storage accounts and other Azure services from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network.

3.1.1.9 Personnel training [21 CFR Part 11.10 (i)]

As described in **Section 2.3.3**, Microsoft has implemented a training program to ensure that personnel and contractors responsible for the Dynamics 365 online services are adequately trained on internal processes and are qualified to perform their duties.

Customer personnel may require additional training based on their job function to ensure they have the qualifications needed to develop, deploy, and maintain cloud-based applications within their Dynamics 365 environment. Platform owners/administrators, and GxP process owners who have the responsibility of configuring, securing, and managing and maintaining the validated state of the applications may require more in-depth training for the cloud services at their disposal.

Dynamics 365 provides a wealth of training material and learning resources on its [online training site](#) to help customers develop the skills needed to implement their cloud-based solutions successfully. With the release of new features, the published material is continuously updated, allowing customers to take full advantage of the latest technological advancements made by the Dynamics 365 engineering teams.

3.1.1.10 Written policies for accountability [21 CFR Part 11.10 (j)]

Customers are responsible for establishing and enforcing written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures. This requirement is typically fulfilled by instituting standard operating procedure(s) that describe the proper operational use of the application, in conjunction with proper user training.

3.1.1.11 Appropriate controls over systems documentation [21 CFR Part 11.10 (k)]

As described in **Section 2.3.4**, Microsoft has implemented documentation and records management procedures governing the complete lifecycle of systems documentation that Microsoft is responsible for maintaining as the cloud service provider.

Customers must also implement appropriate controls over systems documentation, which includes documents describing how their systems operate and are maintained, as well as standard operating procedures. These controls should limit access and distribution of documentation to authorized individuals. Revision and change control procedures must also be implemented to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Customers can leverage services such as [Dynamics 365](#), which includes records management capabilities as part of their documentation management strategy. Customers can also use [Azure DevOps](#), to effectively manage system requirements, design specifications and source code in a controlled manner.

3.1.1.12 Controls for open systems [21 CFR Part 11.30]

Computerized systems that exchange data electronically with other systems over the internet should include appropriate built-in checks for the correct and secure entry and processing of data to minimize risk.

For data at rest, Dynamics 365 organization databases are using SQL TDE (Transparent Data Encryption, compliant with FIPS 140-2) to provide real-time I/O encryption and decryption of the data and log files for data encryption at-rest.

For data in transit, Microsoft uses some of the strongest, most secure encryption protocols in the industry to provide a barrier against unauthorized access to customer data. Protocols and technologies examples include:

- Transport Layer Security/Secure Sockets Layer (TLS/SSL), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network.
- Internet Protocol Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it is transferred across the network.
- Advanced Encryption Standard (AES)-256, the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology

Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured. [Azure Key Vault](#) helps safeguard cryptographic keys and secrets used by cloud applications and services. By using Key Vault, customers can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) with keys that are protected by industry-standard algorithms, key lengths, and hardware security modules (HSMs). Microsoft does not see, or extract customer keys stored within Key Vault.



Additional Resources:

- [ISPE, GAMP Guide: Records & Data Integrity](#)
- [Encryption in the Microsoft Cloud](#)

3.2 Dynamics 365 governance recommendations

To achieve and maintain compliance of a cloud-based GxP system a comprehensive governance model should be established. We recommend performing the following activities to help facilitate the successful governance of Dynamics 365:

- Identify roles and responsibilities for ensuring data integrity based on the shared responsibility model
- Train personnel responsible for using and administering Dynamics 365
- Review and ensure adherence with service agreements
- Perform routine monitoring and evaluation of Dynamics 365 service capabilities
- Establish governance processes that are aligned to the cloud model, including:
 - Client and application security
 - Change management
 - System configuration
 - Data recovery

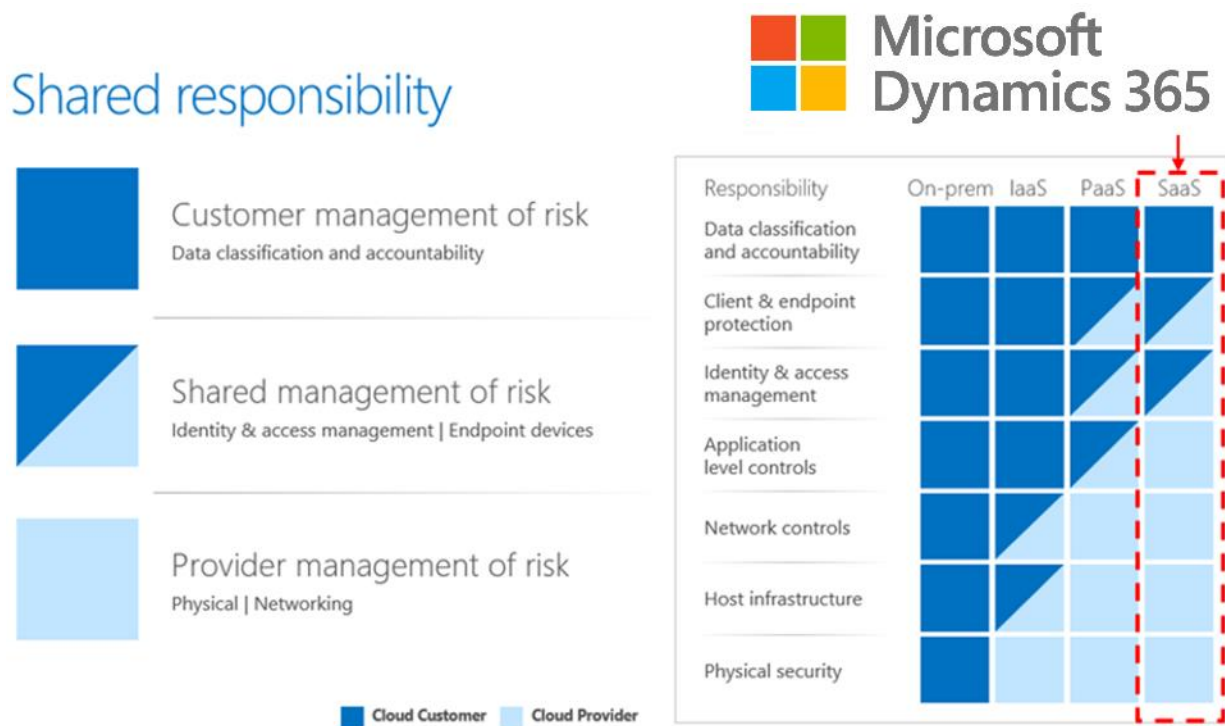
- Monitoring and logging
- Data classification and retention
- Plan validation of GxP processes with process owners and key stakeholders

The sections that follow provide recommendations for developing a cloud strategy and governance model to help Microsoft life science customers successfully manage their GxP processes in Dynamics 365. The proposed methodology is based upon proven practices used by Microsoft customers and partners in life sciences.

3.2.1 Shared responsibility model

Due to the nature of cloud service delivery models, certain responsibilities shift with respect to the qualification and management of the underlying cloud infrastructure. While implementing the governance strategy, it is essential to understand how different cloud service models affect the ways [responsibilities are shared](#) between cloud service providers and their customers.

The left-most column in the following figure shows responsibilities, all of which contribute to the overall security, privacy, and reliability of cloud computing environments.



Customers remain responsible for establishing proper data governance and rights management, managing client endpoints, as well as account and access management, and Microsoft is responsible for all aspects surrounding physical host, physical network, and datacenter. Other responsibilities listed, including identity & directory infrastructure, application, network controls, and operating system, vary depending on the deployment model (that is, IaaS, PaaS, or SaaS).

3.2.2 Service agreements

GxP regulated users of cloud-based systems are expected to have service agreements in place with their service providers, as described in the FDA's draft [Guidance for Industry](#) (Ref. [20]), as well as the recently released *GAMP Guidance for IT Infrastructure Control and Compliance (Second Edition)* (Ref. [8]).

Dynamics 365 online services are governed by a series of contractual agreements. These agreements describe Microsoft service level assurances for system availability, as well as Microsoft commitments and responsibilities as they relate to customer data security and privacy. A summary of the relevant agreements is provided in the following sections.

Customers may also refer to [Appendix B](#) for a mapping of the contractual agreements we establish with our customers against the recommended content for service level agreements and quality agreements, as recommended within the GAMP guidance (Ref. [20]).

3.2.2.1 Service level agreements

Dynamics 365 online services are accompanied by a [Service Level Agreement](#) (SLA) that describes Microsoft commitments regarding delivery or performance of the service regarding uptime and connectivity. The product SLAs also describe the conditions for obtaining service credits and the process for submitting claims.

3.2.2.2 Online Services Terms and Online Services Data Protection Addendum

The [Online Services Terms](#) (OST) in conjunction with the [Online Services Data Protection Addendum](#) (DPA) explain Microsoft contractual commitments to our customers covering various aspects of the services delivery and data protection, including:

- Data Ownership
- Privacy
- Data Security
- Data Transfers and Location
- Organization of Information Security
- Asset management
- Human resources security
- Physical and environmental security
- Location of customer data at rest
- Data recovery procedures
- Encryption of data
- Access Control
- Communication and Operations Management
- Data retention and Deletion
- Information Security Incident Management
- Security incident notification
- Business continuity Management
- Acceptable use policy
- Compliance with laws
- Retirement of services

The DPA also covers audit compliance which include commitments to:

- initiate audits by qualified, independent, third party at least annually
- audits performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework
- provide audit reports
- mitigate audit findings

The OST describe Microsoft commitments related to supporting features and providing notice before removing features or discontinuing a service.

3.2.2.3 *HIPAA Business Associate Agreement*

The [HIPAA Business Associate Agreement](#) (BAA) clarifies and limits how the business associate (Microsoft) can handle protected health information (PHI) and sets forth additional terms for each party related to the security and privacy provisions outlined in HIPAA and the HITECH Act. The BAA is automatically included as part of the OST and applies to customers who are covered entities or business associates and are storing PHI.

3.2.2.4 *Other agreements*

Additional contractual terms may be specified within Enterprise Agreements, enrollment agreements, business, and services agreements, as well as agreement appendices, contingent on specific engagement scenarios with the customer.

[Dynamics 365 support plans](#) including Professional Direct, and Standard are subject to terms defined within the customer’s Enterprise Agreement.

3.2.3 Governance policies and procedures

To ensure proper management of their cloud-based GxP application(s), customers may need to review and update internal quality and operational procedures. The following topics should be covered within customers’ internal governance procedures:

Quality processes	Operational and IT processes
✓ Computerized system validation	✓ Application security
✓ Training management	✓ System administration and user access management
✓ Documentation management	✓ Change management
✓ Records lifecycle management	✓ System configuration management
✓ Supplier management	✓ Data backup and recovery
✓ Periodic review	✓ Monitoring and logging
	✓ Incident and problem management

3.2.3.1 *Quality governance processes*

3.2.3.1.1 *Computerized system validation*

A policy should be in place to describe the processes and controls implemented to ensure the correct validation of computer systems. These validation processes will provide documented evidence that the system is compliant and is fit for its intended use.

This policy should define the responsibilities, activities, and deliverables required to achieve and maintain computer systems in a validated state and in compliance with applicable GxP regulations.

3.2.3.1.2 Training management

An internal training program should be in place to ensure personnel have the competencies required to access and work with Dynamics 365. Additional training requirements may need to be defined for each controlled Dynamics 365 application.

Customer personnel may require additional training based on their job function to ensure they have the qualifications needed to use and administer Dynamics 365. GxP process owners, platform administrators, and system owners who have the responsibility of configuring, securing, and managing content within their Dynamics 365 instance may require more in-depth training.

Dynamics 365 provides a wealth of training material and learning resources on its online [training site](#) to help customers develop the skills needed to use and maintain their environment successfully. With the release of new features, the published material is continuously updated, allowing customers to take full advantage of the latest technological advancements made by the Dynamics 365 engineering teams.



Additional Resources:

- [Dynamics 365 Training Center](#)

3.2.3.1.3 Documentation management

Procedures should be in place to establish the framework under which official documents and records are created and managed. The intent is to ensure that the organization's business areas have the appropriate governance, supporting structure and resources established to manage documents in a controlled manner (that is, planned, monitored, recorded, and audited).

3.2.3.1.4 Records lifecycle management and data retention

Procedures should be in place to ensure all records are properly classified and retention policies are aligned with applicable regulations and requirements.

Customers are responsible for determining their recordkeeping requirements based on internal policies and regulatory requirements. Customer data stored within the customer's Dynamics 365 environments remains accessible throughout the term of the contract with Microsoft and for a defined period upon contract termination as stipulated in the [Online Services Data Protection Addendum](#) (DPA). Microsoft commitments regarding the protection of customer data retained within the Dynamics 365 online services are also described in the DPA.

The [Dynamics 365 Data Archival and Retention app](#) provides the ability to export data from Dynamics 365 Customer Engagement into a COSMOS DB and Blob storage using Azure Services.

3.2.3.1.5 Supplier management

A formal process should be in place to ensure that cloud service providers are identified, assessed, selected, and managed in a formal and controlled manner.

Because of the business criticality of many GxP computerized systems, life sciences customers often perform a vendor assessment or audit before selecting a product vendor or service provider. The need for performing an audit and the type of audit is typically based on:

- Initial risk assessment / overall system impact
- System novelty and complexity
- Categorization of components

The FDA provides the following recommendations for performing vendor audits within the recently released draft industry guidance titled, "[Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11 – Questions and Answers](#)" (**Error! Reference source not found.**):

“Sponsors and other regulated entities often perform audits of the vendor’s electronic systems and products to assess the vendor’s design and development methodologies used in the construction of the electronic system or the product, as well as the vendor’s validation documentation. To reduce the time and cost burden, sponsors and other regulated entities should consider periodic, but shared audits conducted by trusted third parties.”

As discussed in Section 2.2, Dynamics 365 regularly undergoes independent audits performed by qualified third-party accredited assessors regarding several ISO, SOC, HITRUST, FedRAMP, and attestations. The SOC 2 Type 2 audit report is especially significant as it provides a high degree of visibility into the assessment and verification criteria used during the evaluation process. Microsoft provides customers with access to the latest audit reports via the [Service Trust Portal](#), which customers may review during their vendor assessment process.

Auditors should familiarize themselves with the principles covered within the ISO and SOC audit reports so that they can use the information contained within these reports during the assessment process. Although the SOC 2 attestation does not focus on GxP regulations, many of the control objectives are very similar to those required by 21 CFR Part 11 and Annex 11. To assist with this process, we have included in the appendices of this document, a thorough analysis of the regulatory requirements of 21 CFR Part 11 (see [Appendix C](#)) and Annex 11 (see [Appendix D](#)). This analysis highlights the shared responsibilities between Microsoft and our customers and identifies the various controls that Dynamics 365 has implemented. The analysis also maps to a specific control ID as referenced within the latest SOC 2 report for Dynamics 365. Since addressing these regulatory requirements involves shared responsibilities between Microsoft and our customers (that is, regulated users), we have also included recommended customer activities corresponding to each regulatory requirement.

3.2.3.1.6 Periodic review

Procedures should be in place to define the process for performing a documented assessment of the documentation, procedures, records, and performance of a computer system to determine whether it is still in a validated state and what actions, if any, are necessary to restore its validated state. The frequency of review is dependent upon a system’s complexity, criticality, and rate of change.

3.2.3.2 Operational and IT governance processes

3.2.3.2.1 Logical security

Procedures should be in place to describe the security measures for cloud applications systems to protect against unauthorized access to cloud platform administrative console and regulated application components. The procedures should ensure workstations used to access the Dynamics 365 admin center are appropriately hardened and that time-out mechanism are employed for inactive sessions.

3.2.3.2.2 System administration and access management

Procedures should be in place to provide instruction for the technical management and engineering practices used in the operation and maintenance of cloud applications. This includes procedures for user access management, which establish clear standards for issuing accounts, creating passwords, and managing accounts. The procedures should also describe how administrative accounts are managed, including segregation of duties.

Customer personnel who are responsible for operations and maintenance activities, such as system administrators and support personnel, should be given the appropriate level of access to the resources they need to perform their job function, while adhering to the principle of least privilege. Depending on the size of the organization, customers may want to designate several administrators who serve different functions. Dynamics 365 includes a security model that enables separation of administration based on roles.

Customers should develop a permissions strategy to keep the environment manageable and secure. An effective permissions strategy will enhance the manageability and performance of the system, ensure compliance with the organization's data governance policies, and minimize the cost of maintenance.

→ See **Section 3.1.1.4 and 3.1.1.7** for additional recommendations

3.2.3.2.3 Change management

A formal process should be in place for change management that will ensure that application changes are implemented in a controlled manner. This process must also establish the framework for proposing, reviewing, and approving changes to the application.

As part of their Dynamics 365 governance strategy, customers may need to adapt their processes regarding change management to better align with the cloud model. With the cloud model, changes may be performed to the underlying platform infrastructure or the provided software, which are not under customer control. However, this does not imply that changes are out of control.

Dynamics 365 enables customers and partners to test the latest capabilities which are part of the updates early in the cycle. Customers can get access to Dynamics 365 updates before they are deployed in the production environment. Major updates can be validated in a sandbox environment in advance of the update release. This release strategy allows administrators, change managers, or anyone else responsible for Dynamics 365 updates to prepare for the upcoming changes by letting them:

- Test and validate new updates before they are released to all the users in the organization.
- Prepare user notification and documentation before updates are released worldwide.
- Prepare internal help-desk for upcoming changes.
- Go through compliance and security reviews.
- Use feature controls, where applicable, to control the release of updates to end users.

The [Online Services Terms](#) agreement describes Microsoft commitments related to support of features and notification for changes that involve the removal of material feature or functionality or discontinuation of a service.

Release processes for Dynamics 365 - Finance and Operations

Each new release is designed and developed by the Dynamics 365 team. Any new release is first validated by the feature team, then by the Finance and Operations teams. During this time, extensive testing is done on various test topologies. A compatibility checker also runs tests to ensure backward compatibility. In addition, a Release Validation Program is available for customers to join. This program allows customers to share artifacts, such as databases and code, that is used for benchmarking and tested with automation to provide an additional layer of quality assurance.

The experience for service updates consists of four distinct steps:

<p>1. Configure</p>	<p>Customers can select a maintenance window, based on their business constraints. A calendar of upcoming updates is available in the Microsoft Dynamics Lifecycle Services (LCS) to help customers plan ahead. Users must opt- in to new features and turn them on. All updates are applied first to the user acceptance testing (UAT) environment and then to the production environment. Therefore, customers have time to do any validation that is required. Customers can select the environment that is updated. They can also pause an update for up to three months.</p>
<p>2. Notice</p>	<p>Release plans will be available to help you plan ahead and understand what is changing. Customers can learn about upcoming features up to three months in advance. The What's new topics provide details about the updates for specific months.</p> <p>Additionally, a notification email is sent five days in advance, and a notification will appear in LCS just before an update.</p>
<p>3. Update</p>	<p>After notifications have been sent, Microsoft will apply the update (auto update) during the designated maintenance window. After this operation is completed, a notification email will be sent to indicate the status of the update. Customers will also be able to self-update by using the standard update experience in LCS.</p> <p>Customers who participate in the First release program will have an opportunity to update their sandbox environment and other environments early.</p>
<p>4. Validate</p>	<p>After an update is completed in the UAT environment, a business process test can be executed to validate the environment. To support this effort, customer may use the no-code automation Regression Suite Automation Tool.</p> <p>Some customers have both external data integrations and internal data integrations. We recommend that these customers use the Data task automation tool for testing.</p>

Release processes for Dynamics 365 - Model-driven apps (Marketing, Sales, Customer Service, Field Service, Project Service Automation)

For model-driven apps, Dynamics 365 has adopted a biannual functional release cadence which aims to lower upgrade costs, provide all users access to the latest capabilities, performance improvements and offer a better support experience. These updates will be backward compatible so customer specific apps

and customizations will continue to work post update. New features with major, disruptive changes to the user experience are off by default. This means administrators will be able to first test before enabling these features for their organization.

In addition to the two major updates, regular performance and reliability improvement updates are deployed throughout the year. Deployments are phased over several weeks following safe deployment practices and updates are monitored closely for any issues.

To provide early visibility and help customers get ready for the new updates, we publish a [release schedule](#) and [release notes](#), which provide a summary of all the new features and improvements and information on when they are planned to be available. Release notes are published months prior to each major update to help customers plan for the new capabilities.

3.2.3.2.4 System configuration management

Procedures should be in place to ensure that all updates to baseline items (configuration items) are controlled and traceable.

The Admin center within Dynamics 365 Portal provides the ability to administer the configuration of certain settings within a customer's Dynamics 365 subscription. Information about the configuration settings, can be viewed within the portal.

3.2.3.2.5 Data recovery

Procedures should be in place to define the strategy for data recovery in the event of intentional or unintentional destruction and/or corruption of data. Customers have multiple options to recover their data in Dynamics 365 and can use the capabilities described below to select the appropriate process for each situation.

When using model-driven apps in Dynamics 365, such as Dynamics 365 Sales and Dynamics 365 Customer Service, data is stored within an Azure SQL Database System in which automated [backups occur continuously](#). System backups for production environments that have been created with a database and have one or more Dynamics 365 applications installed are retained up to 28 days. System backups for production environments which do not have Dynamics 365 applications deployed in them are retained for 7 days. Customer administrators can also initiate an unlimited number of manual backups, which do not count against storage limits.

When using Dynamics 365 for Finance and Operations, customers can use Microsoft Dynamics Lifecycle Services (LCS) to do [a point-in-time restore \(PITR\)](#) of the production database to a user acceptance testing (UAT) sandbox environment. Microsoft maintains automated backups of the business and financial reporting databases for 28 days for Production environments and 7 days for Sandbox environments.

3.2.3.2.6 Monitoring and logging

Procedures should be in place to describe the tools used to monitor the cloud application(s) to ensure consistent availability and performance. Customers can make use of the numerous monitoring capabilities and services embedded in the Dynamics 365 online services as part of their operations and maintenance strategy.

The [Security & Compliance Center](#) can track user and administrator activities, malware threats, data loss incidents, and more. The Reports dashboard is used for up-to-date reports related to the security and compliance features in the organization. Azure AD reports can be used to stay informed on unusual or suspicious sign-in activity.

Special consideration may be needed regarding the data generated by [audit logs](#) which retain collected data for 90 days or up to 1 year . If customers need to retain audit log information for a longer duration, it is possible to programmatically download data from the Microsoft 365 audit log using the [Office 365 Management Activity API](#).

3.2.3.2.7 Incident and problem management

A formal process should be in place to ensure that issues are raised, recorded, investigated, and resolved in a formal and controlled manner.

For [Dynamics 365 Finance and Operations](#), support tickets can be raised with Microsoft support personnel directly within the Support tile of the [Lifecycle Services tool](#) which provides an efficient way of communicating and [tracking the status](#) of an incident until it is resolved.

For model-driven apps (Sales, Customer Service, Field Service, and Project Service Automation), Admins can use the Help + support experience in the [Power Platform admin center](#) to get self-help solutions in real-time for their issue.

3.3 GxP Use Cases

As a highly configurable content management platform, Dynamics 365 may be configured to support a wide range GxP processes and activities. Some examples of these types of GxP processes include:

- Drug Supply Chain Management
- Commercial Data Warehouse
- Medical CRM
- Hospital Response management using Customer service
- [Modernize field service with Dynamics 365 Remote Assist](#)

3.4 Considerations for implementing a risk-based validation strategy

In the context of a public SaaS cloud service model, the customer does not have control over the underlying infrastructure hardware and software components, nor to the application itself. The cloud service provider is responsible for managing and maintaining these components according to internal quality, development and operational practices, such that they remain qualified.

Qualification is defined as “a process of demonstrating the ability of an entity to fulfill specified requirements. In the context of an IT Infrastructure, this means demonstrating the ability of components such as servers, clients, and peripherals to fulfill the specified requirements for the various platforms regardless of whether they are specific or of a generic nature.”¹

¹ ISPE, GAMP Good Practice Guide: IT Infrastructure Control and Compliance (**Error! Reference source not found.**)

As described in **Section 2.3**, the Microsoft has implemented a series of processes and controls to help ensure the quality of service and maintain a state of control over the physical infrastructure elements. These elements include the physical hosts, physical networks, and datacenters. Periodic audits performed as part of the Microsoft ISO and SOC certification and attestation processes, as described in **Section 2.2**, help to ensure the people, processes, and technology that make up the Dynamics 365 operating environment work together to maintain a state of control and compliance.

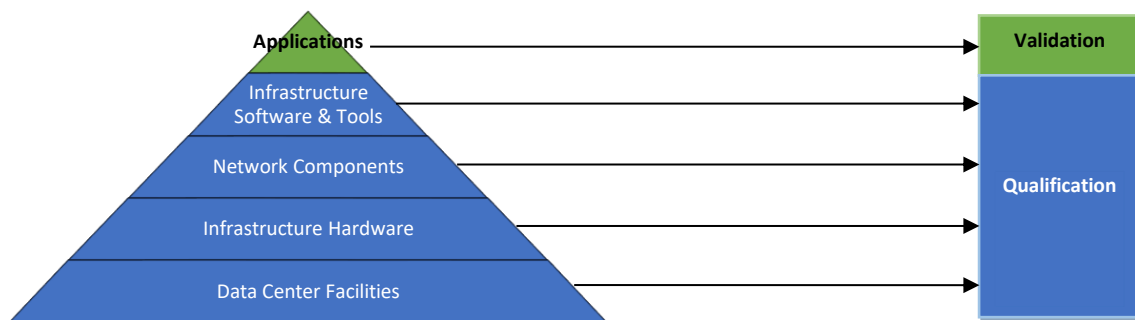


Figure 1 – Qualification of Infrastructure vs. Validation of Applications

Validation consists of demonstrating, with objective evidence, that a system meets the requirements of the users and their processes and is compliant with applicable GxP regulations. To remain in a validated state, appropriate operational controls must be implemented throughout the life of the system. As such, validation is performed by the regulated users (customer) of Dynamics 365.

The ISPE’s *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems* (Ref. [7]) provides a starting point from which life sciences customers may adapt their approach to validating their GxP application(s). In GAMP 5, computerized system validation is defined as, “achieving and maintaining compliance with applicable GxP regulations and fitness for intended use by:

- *the adoption of principles, approaches, and life cycle activities within the framework of validation plans and reports*
- *the application of appropriate operational controls throughout the life of the system.”*

The regulated user (customer) should determine the appropriate validation strategy supported by an analysis of risk, intended use, and regulatory compliance requirements associated with their GxP processes.

3.4.1 GAMP 5 Software Category

The ISPE’s *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems* (Ref. [7]) provides recommendations on how to analyze and categorize software components of a GxP computerized system. Along with a risk assessment and a supplier assessment, these categories can be used to determine a suitable system life cycle strategy.

From the perspective of a customer using out-of-the box Dynamics 365 functionality for GxP-regulated processes (i.e. as a document repository), Dynamics 365 may be considered a GAMP 5 Software **Category 4** – Configured Product. A configured product refers to a commercially available software product which is configured to meet the needs of a specific user business process.

Additionally, customers can develop custom GxP applications that interface with or feed data into Dynamics 365. Such custom-development should be treated as a GAMP 5 Software **Category 5** – Custom Application and tested appropriately. Because Dynamics 365 was not explicitly developed for any specific GxP business process, the regulated user (customer) should verify their configuration of the platform is appropriate for their intended use.

3.4.2 Application Stakeholders

The following application stakeholders should take an active role in the planning and execution of each validation project:

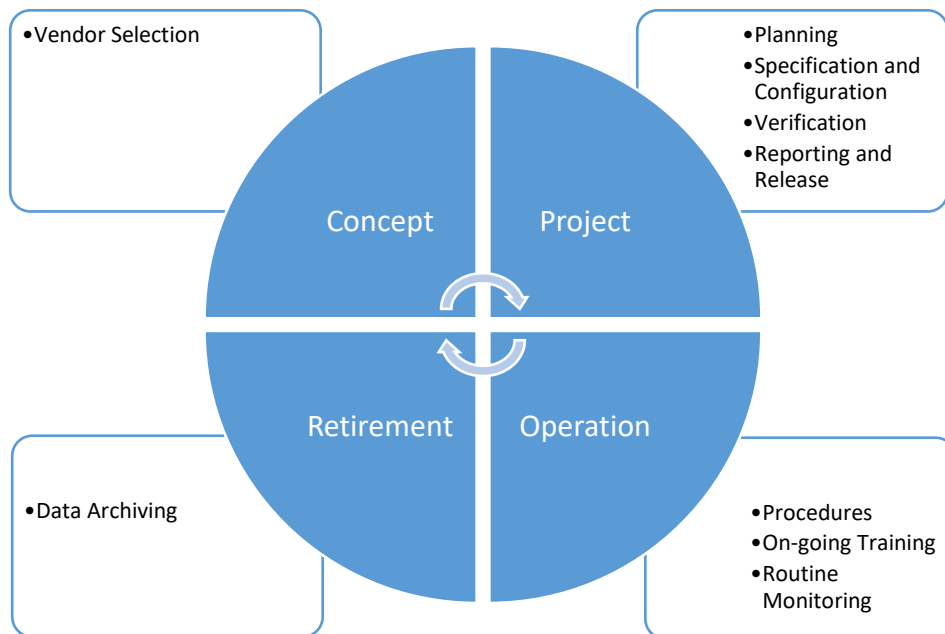
- **Process Owner:** The Process Owner acts as a subject matter expert for the business processes carried out within the system and is responsible for ensuring the system is fit for its intended use and operated in accordance with appropriate procedures (SOPs). The Process Owner represents the user group or department/business unit using the system. As such, there may be more than one Process Owner if more than one business process is being carried within Dynamics 365. The Process Owner(s) should be involved in the verification of the system, defining appropriate test strategies and executing tests and/or reviewing test results.
- **System Owner:** The System Owner is responsible for ensuring the Dynamics 365 is supported in accordance with appropriate procedures (SOPs). The System Owner is responsible for system access control and for ensuring that system administration activities are carried out in accordance with appropriate procedures (SOPs).
- **Quality Representative:** The Quality Representative is responsible for ensuring that validation activities are carried out and documented in accordance with appropriate procedures (SOPs).

Validation artefacts (documentation) should be approved by application stakeholders and maintained as quality records in accordance with the customer's document management procedures.

3.4.3 Computerized system life cycle approach

The ISPE's *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems* (Ref. [7]) defines a strategy for achieving compliance and fitness for intended use using the life cycle approach. This approach "entails defining activities in a systematic way" through the entire life cycle of a computerized system.

As illustrated below, the life cycle includes the following key phases: Concept, Project, Operation, and Retirement. Numerous supporting processes must be maintained throughout the life cycle approach, including: Risk Management, Change and Configuration Management, Traceability, and Document Management.



The following sections discuss the various life cycle phases and corresponding validation deliverables that GxP-regulated customers may generate for cloud-based GxP applications. The intent is not to prescribe a specific methodology, but rather to highlight the overall goal of each step in the process and corresponding deliverables which provide evidence that the GxP application meets quality objectives and is fit for its intended use. We recommend that customers follow documented processes and produce system documentation that adds business value and communicates relevant information to the intended audience.

Additional Resources:

- [U.S. FDA, Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application](#)
- [ISPE, ISPE GAMP 5 - A Risk-Based Approach to Compliant GxP computerized systems](#)
- [ISPE, GAMP Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems \(Second Edition\)](#)
- [PIC/S - Good Practices for Computerised Systems in Regulated “GxP” Environments](#)

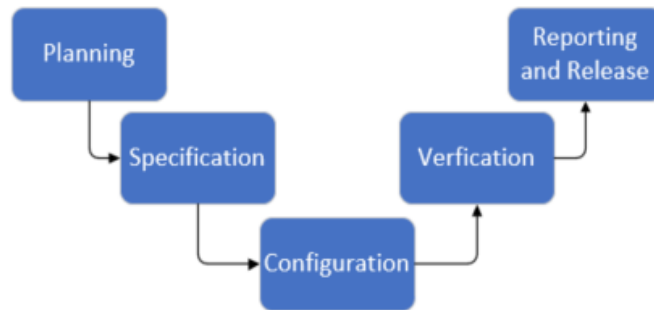
3.4.3.1 Concept

During the Concept phase, opportunities to improve business activities or to correct a deficiency are identified. Initial requirements for new business processes or the enhancement of an existing business process are defined. These requirements are detailed enough to support the estimation of costs, resource planning, and the exploration of potential solutions.

For purposes of this document, it is assumed that the activities of the Concept phase have been completed and Dynamics 365 has already been selected as the preferred business solution.

3.4.3.2 Project

During the Project phase, the regulated user (customer) works to implement the chosen solution and demonstrate, with objective evidence, that the system is fit for its intended use. The Project phase consists of five stages, as illustrated and discussed below.



3.4.3.2.1 Planning

Initial planning begins by defining the project scope, key activities, and responsibilities for producing validation deliverables (including SOPs, specifications, and verification documentation). Planning will likely continue throughout subsequent project stages as quality and regulatory impacts are evaluated and project-related risks are mitigated.

The validation approach should be commensurate with the risk associated with the types of records being managed in Dynamics 365. Planned activities should be scaled according to:

- The outcome of an initial risk analysis, in which the intended use of Dynamics 365 is assessed to evaluate potential system impact of patient safety, product quality, and data integrity.
- The complexity of the system architecture (organization of site collections, sites, libraries)
- The outcome of supplier evaluation, in which the supplier’s capabilities are assessed (see Section 3.2.3.1.5)

A documented **Risk assessment** should analyze potential risk areas and evaluate the expected impact on the application regarding availability, data loss, security, business disruption, and regulatory compliance. Risk mitigation activities that could eliminate or reduce risk to an acceptable level should be identified. According to the ISPE GAMP Good Practice Guide, *A Risk-Based Approach to Testing of GxP Systems* (Ref. [9]), the following controls may be appropriate to mitigate any identified risks or perceived deficiencies regarding the cloud-based solution or the service provider:

- Train and support the cloud service provider (supplier management)
- Execute additional testing
- Select another cloud service provider
- Change to a different cloud model, e.g. Dynamics Online Service (SaaS) versus Dynamics 365 (on-premise) installed on Azure (IaaS)

Other possible risk mitigation strategies include:

- The deployment of various automatic performance, diagnostic, alarm, and security monitoring tools, which greatly reduces the likelihood of undetected harm
- Updated or new policies or governance procedures
- Additional end user education or training
- Updated contractual agreements (for example, SLAs)
- Identification of new or updated roles and responsibilities

A project-specific **Validation plan** document is typically produced to capture the planned activities and assigned responsible actors. The plan should be endorsed through approval by various application stakeholders (process owner, system owner, quality representative).

Effective planning is facilitated by a thorough understanding of requirements gathered through collaboration with various application stakeholders (process owner, system owner, quality representative). **Requirements** should be documented and elaborated sufficiently to support subsequent risk analysis, configuration, and verification activities. The identification of any regulatory requirements that may be impacted by the configuration of the GxP application should be prioritized. Requirements should also address the correction of any shortcomings or risk mitigation activities noted during the initial risk analysis and supplier evaluation.

To help ensure a successful implementation, the following elements should be considered when establishing the requirements:

- Business process needs
- Interfaces with other business applications
- Security and privacy
- Capacity
- Availability
- Backup and recovery
- Monitoring (auditing and logging)
- Geographic location of stored data
- Relevant regulations
- Non-functional requirements, including governance procedures and contractual documents that the customer must have in place

Customers should be aware of local legislation regarding data privacy and when implementing solutions that span multiple geographies, because some regulatory requirements may have an impact on the overall solution design or architecture. For example, the [European Union's General Data Protection Regulation \(GDPR\)](#) is a privacy regulation that requires organizations that collect, host, or analyze personal data of EU residents to use third-party data processors who guarantee their ability to implement the technical and organizational requirements of the GDPR. Microsoft is [committed](#) to GDPR compliance across its cloud services. GDPR-related assurances are provided in our [contractual commitments](#). Customers can select a region during the initial setup of services to satisfy their data location and residency requirements.



Additional Resources:

- [EU General Data Protection Regulation \(GDPR\) Compliance with Azure FAQ](#)
- [Multi-Geo Capabilities in OneDrive and SharePoint Online](#)

3.4.3.2.2 Specification

Documented specifications provide numerous benefits, including offering a reference to help relevant application stakeholders as well as regulatory inspectors understand how Dynamics 365 will be implemented and used within context of the customer's business processes. At the base, a System Description should be available to describe, in common language, what Dynamics 365 does. This description may be embedded within other validation documents or written as a standalone document.

Functional specifications should be documented to describe how Dynamics 365 will meet stated requirements for electronic records management and additional business process needs. These specifications may be used to support subsequent risk assessment and verification activities.

Functional specifications should consider and describe the key Dynamics 365 features that may be used to support GxP regulated activities, for example:

- Functionality pertaining to audit logging
- Functionality pertaining to record retention.
- System access and security controls
- Data encryption

Configuration specifications should be documented to establish the wireframe that will ensure Dynamics 365 will meet stated requirements and functional specifications. These specifications may be used to support subsequent verification and configuration management activities.

Configuration specifications should consider the following elements:

- Dynamics 365 administration settings, including the configuration of relevant password policies, multi-factor authentication settings, and information rights management settings
- Information governance settings, including the configuration of retention policies

The customer may choose to conduct Design Review(s) to ascertain that the specifications, if implemented, will result in a system that satisfies the detailed requirements.

3.4.3.2.3 Configuration

Upon approval of the specifications, the customer can proceed with the configuration of Dynamics 365. The configuration should be performed in accordance with controlled process supported by the customer's Change and Configuration Management procedures (as outlined in Section 3.2.3.2.4).

The customer should ensure that access to the Dynamics 365 admin center is restricted to qualified individuals (administrators) only.

3.4.3.2.4 Verification

All verifications should be based on approved test plans with predetermined acceptance criteria.

A risk-based approach is widely adopted within the life sciences industry and is advocated by regulatory agencies and industry standards for GxP computerized system compliance. The outcome of the risk assessment should help customers focus the scope of verification and testing on processes and functionality that are associated to areas presenting higher business and regulatory risks.

Configuration verification should be performed to ensure Dynamics 365 is configured in accordance with documented specifications. Verifications should focus on key security and content management settings with GxP impact.

These verifications should be repeated in each environment (e.g. Test, QA, Production) where GxP records will be created and/or maintained.

The availability of relevant system documentation (such as specifications, service agreements) along with relevant procedures (governance policies and SOPs, as outlined in Section 3.2.3) should be verified and ensured. This provides assurance that, upon release to operations, Dynamics 365 will be used and maintained in a controlled manner.

By using the Dynamics 365 online services, the customer is effectively outsourcing the management and operations of the physical infrastructure (datacenter, network, and hosts) and software (installation and maintenance) to Microsoft.

Functional verification should be performed against predefined acceptance criteria to verify critical system features behave as expected.

User acceptance verification should be performed to ensure that specified requirements are satisfied, with focus on the configured business process(es) and functionality associated with greater risks to data integrity and security.

A process for Traceability should be in place to support verification activities. With a **Traceability matrix**, the relationship between detailed requirements and specifications is established. Moreover, the Traceability matrix associates the requirements to any relevant controls that have been implemented by the customer and Microsoft, including testing, governance procedures, audits/assessments, and contractual agreements that serve to ensure the requirements are satisfied.

3.4.3.2.5 Reporting and release

Upon completion of the verification activities, the test results should be summarized, and the overall acceptance criteria confirmed within a **Validation summary report**. This report should provide a statement amount the fitness for intended use of the system and be approved by application stakeholders (process owner, system owner, quality representative). Approval of this report may serve as a stage gate to release the system for operational use.

3.4.3.2.6 Checklist of recommended validation project deliverables

The following table provides a listing of the validation deliverables that are recommended for a validation project. The deliverables can be developed as standalone documents or embedded into other deliverables, as deemed appropriate and in accordance with the customer's internal policies governing computerized system validation.

Validation Deliverable	Description
✓ Risk assessment	The Risk assessment considers the intended use of Dynamics 365. It evaluates potential system impact of patient safety, product quality, and data integrity and describes mitigation strategies designed to reduce or eliminate the overall risk. The outcome of the risk assessment may be used to focus the scope of verification/testing.
✓ Validation plan	The Validation plan defines the project scope and validation approach. The validation plan should also list the deliverables to be produced, roles and responsibilities, and overall project acceptance criteria.
✓ Requirements specification	The Requirements specification defines how a system should function to satisfy business needs and comply with applicable regulations.
✓ Functional specifications	The Functional specifications describe how Dynamics 365 will meet stated requirements for electronic records management and additional business process needs.
✓ Configuration specifications	The Configuration specifications capture how Dynamics 365 must be configured to meet stated requirements and functional specifications.
✓ Configuration verification	The goal of configuration verification is to produce documented evidence that the customer’s Dynamics 365 instance is configured according to specifications.
✓ Functional verification	The goal of the functional verification is to produce objective and documented evidence that the configured Dynamics 365 components function according to specifications.
✓ User acceptance verification	The goal of user acceptance verification is to produce documented evidence that specified requirements are met and users are satisfied with the implemented solution.
✓ Traceability matrix	The traceability matrix establishes the relationship between the requirements and any relevant controls that have been implemented by the customer and Microsoft, including testing, procedural controls, audits/assessments, and contractual agreements that serve to ensure the requirements are satisfied.

Validation Deliverable	Description
✓ Validation summary report	The validation summary report summarizes the entire effort and confirms that all deliverables required by the approved validation plan are complete. The validation summary report would include a summary of results obtained during the various verification stages.

Note: The term “verification” has been intentionally adopted in place of traditional “qualification” terminology. However, individuals may consider the following mapping of terms:

- Configuration verification = Installation Qualification (IQ)
- Functional verification = Operational Qualification (OQ)
- User acceptance testing = Performance Qualification (PQ)

3.4.3.3 Operation

Once in the Operation phase, the customer must turn his focus on ensuring a state of control and compliance is maintained. This is accomplished through the implementation of up to date Quality and Operational governance policies and procedures as defined in Section 3.2.3.

A training program must be in place to ensure that Dynamics 365 administrators and system end-users are familiar with procedures that cover the use, maintenance and management of the GxP application.

Continuous monitoring and diagnostics are a crucial part of maintaining quality of service targets. Built-in diagnostic tools allow administrators to monitor Dynamics 365 [service health](#), including critical issues affecting service availability (active incidents) and posted advisories which help with application troubleshooting.

To maintain the validated state over time, a periodic review of the system, associated system documentation, procedures, records, and performance monitoring metrics should be conducted to ensure the system continues to meet regulatory requirements and business needs. A periodic review should also be conducted to ensure assigned access rights remain appropriate.

Feedback collected during system operation, training, monitoring, and periodic review may reveal opportunities for improvement. The implementation of these improvements would be overarched by Change and Configuration Management procedures and would initiate a new round of life cycle activities.

3.4.3.4 Retirement

At the Retirement phase, the system is effectively withdrawn from active operations such that data may no longer be added to the system. Considerations for retirement include:

- Removal of user access (user deactivation)
- Disabling interfaces between Dynamics 365 and other customer applications
- Retention of a special-access user for online GxP records

- Planning for offline data repatriation

According to the [Online Services Data Protection Addendum](#) (DPA), the customer will always have the ability to access, extract and delete his data during the subscription terms. Microsoft will retain the customer's data for 90 days after expiration or termination of the subscription so that the customer may extract his data. After the 90-day retention period, Microsoft may delete the customer's data.

Data in Dynamics 365 can be exported using the comprehensive entity export capabilities. Using Data management and integration entities, the customer may utilize provided entities, create new, or extend existing entities for a repeatable data export to Excel or a number of other common formats using Data import and export jobs. Alternatively, many lists can be exported to a static Excel file to facilitate data extraction.

When repatriating data, customers may choose to use an "on-premise" Dynamics 365 instance to store exported content.

Alternatively, the [Dynamics 365 Data Archival and Retention app](#) may be used = to export data from Dynamics 365 Customer Engagement into a COSMOS DB and Blob storage using Azure Services.

4 Conclusion

By combining state-of-the-art technology and industry standards, Microsoft delivers services and solutions that offer built-in capabilities for compliance with a wide range of regulations and privacy mandates. Extensive controls that are implemented as part of internal development, security, and quality practices help to ensure that the Dynamics 365 online services meets its specifications and is maintained in a state of control and compliance. Microsoft maintains secure, consistent, and reliable performance through a series of tried and tested access, security, and privacy controls. These processes and controls are audited and verified on a continuous basis by qualified third-party accredited assessors.

Of equal importance are the controls that must be implemented by our life science customers while defining their cloud qualification strategies and governance models to ensure that GxP computerized systems are maintained in a secured and qualified state.

By working together and focusing on our respective areas of expertise, Microsoft and our life sciences customers can help usher in a new era in which cloud-based GxP systems are no longer seen as a compliance risk, but rather as a safer, more efficient model for driving innovation and maintaining regulatory compliance.

5 Document Revision

Date	Description
June 2020	Initial release

6 References

6.1 Industry guidance and standards

- Ref. [1] [NIST Cloud Computing Standards Roadmap](#)
- Ref. [2] [PIC / S PI 011-3 - Good Practices for Computerised Systems in Regulated “GxP” Environments](#)
- Ref. [3] [Evolution of the Cloud: A Risk-Based Perspective on Leveraging PaaS within a Regulated Life Sciences Company, ISPE, July 2016](#)
- Ref. [4] [ISO/IEC 17789:2014 - Information technology - Cloud computing - Reference architecture](#)
- Ref. [5] [ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements](#)
- Ref. [6] [ISO 9001:2015 Quality management systems — Requirements](#)
- Ref. [7] [ISPE, GAMP 5 - A Risk-Based Approach to Compliant GxP computerized systems, 2008](#)
- Ref. [8] [ISPE, GAMP Good Practice Guide: IT Infrastructure Control and Compliance \(Second Edition\), 2017](#)
- Ref. [9] [ISPE, GAMP Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems \(Second Edition\), 2012](#)
- Ref. [10] [ISPE, GAMP Good Practice Guide: Global Information Systems Control and Compliance \(Second Edition\), 2017](#)
- Ref. [11] [ISPE, GAMP Guide: Records & Data Integrity, 2017](#)
- Ref. [12] [Cloud Standards Customer Council: Practical Guide to Cloud Service Agreements, April 2015](#)
- Ref. [13] [Cloud Standards Customer Council: Impact of Cloud Computing on Healthcare, February 2107](#)
- Ref. [14] [Cloud Standards Customer Council: Practical Guide to Platform-as-a-Service, September 2015](#)
- Ref. [15] [AAMI TIR45:2012, Guidance on the use of Agile practices in the development of medical device software, 2012](#)

6.2 Regulations and regulatory guidance

- Ref. [16] [U.S. FDA, Code of Federal Regulations, Title 21 Part 11, Electronic Records; Electronic Signatures](#)
- Ref. [17] [U.S. FDA Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application, August 2003](#)
- Ref. [18] [EudraLex The Rules Governing Medicinal Products in the European Union - Volume 4 - Good Manufacturing Practice - Medicinal Products for Human and Veterinary Use- Annex 11: Computerised Systems](#)
- Ref. [19] [U.S. FDA Data Integrity and Compliance with CGMP - Guidance for Industry, December 2016](#)
- Ref. [20] [FDA, Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11-- Questions and Answers , August 2018.](#)

7 Appendices

Appendix A: Glossary

Appendix B: Coverage of SLA / Quality Agreement Requirements with Microsoft Agreements

Appendix C: US FDA 21 CFR Part 11 Electronic Records; Electronic Signatures

Appendix D: EudraLex Volume 4 Annex 11 Computerised Systems

Appendix A. Glossary, Abbreviations and Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants
CFR	Code of Federal Regulations
CRM	Customer Relationship Management
CV	Curriculum vitae
ERP	Enterprise Resource Planning
FDA	United States Food and Drug Administration
GAMP	Good Automated Manufacturing Practice
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
IaaS	Infrastructure as a service
ICFR	Internal control over financial reporting
IEC	International Electrotechnical Commission
IQ	Installation qualification
ISO	International Organization for Standardization
ISPE	International Society of Pharmaceutical Engineers
IT	Information technology
NDA	Non-disclosure agreement
NIST	National Institute of Standards and Technology
OS	Operating system
OQ	Operational qualification
PaaS	Platform as a service
PIC/S	Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme
SAS	Statement on Auditing Standards
SDL	Security Development Lifecycle
SDLC	Software Development Lifecycle
SLA	Service level agreement
SOC	Service organization controls
SOP	Standard operating procedure
SSAE	Statement on Standards for Attestation Engagements
SSL	Secure Sockets Layer
STB	Microsoft Server and Tools Business
TSP	Trust services principles
VM	Virtual machine
VPN	Virtual private network

Appendix B. Coverage of SLA / Quality Agreement Requirements with Microsoft Agreements

The following table includes the recommended SLA/quality agreement content, per the *GAMP Guidance: IT Infrastructure Control and Compliance (Second Edition)* (Ref. [8]), as well as a description of how the recommended content is addressed via the contractual agreements Microsoft has with its customers.

The typical content of an expected SLA/Quality Agreement, per the GAMP Good Practice Guide, has been analyzed and contrasted with the content of the contractual agreements Microsoft has with its customers. The following table provides a summary of this analysis. Customers should refer to the most current version of the following Microsoft [licensing terms](#) for the exact legal commitments:

- Volume Licensing Online Services Terms (OST)
- Volume Licensing Service Level Agreement for Microsoft Online Services (SLA)
- Volume Licensing Product Terms
- Volume Licensing Online Services Data Protection Addendum (DPA)

Typical SLA/Quality Agreement Content	Coverage
Contacts on either side	<p>For each Dynamics 365 subscription, customers must assign a subscription owner who is considered the customer’s primary contact. Contact information for subscription owners is maintained directly within the Management Portal.</p> <p>Depending on the engagement scenario, additional customer contacts may be specified in the Enrollment Agreement or Supplemental Contact Information Form.</p> <p>Microsoft Account Managers typically act as the primary point of contact between Microsoft and its customers.</p> <p>The Online Services Data Protection Addendum (DPA) contains a section on “How to Contact Microsoft,” which provides instructions for contacting Microsoft.</p>
Duration of validity and circumstances triggering reviews	<p>Microsoft will not modify the terms of customer Online Services SLAs during the initial term of their subscription; however, if the subscription is renewed, the version of the SLA that is current at the time of renewal will apply throughout the renewal term. Microsoft will provide at least 90 days’ notice for adverse material changes to the SLA.</p> <p>As stated in the SOC 2 audit report (see Trust Criteria A1.1), Microsoft management performs monthly reviews to evaluate compliance with customer SLA requirements.</p>
Prerequisites and customer deliverables or involvement	<p>Because of the generic nature of the Dynamics 365 service offerings, there are no specific prerequisites, customer deliverables, or involvement required in the delivery of the services to the customer.</p>

Typical SLA/Quality Agreement Content	Coverage
Scope and nature of the required services	A detailed description of the Dynamics 365 service offerings is available in Online Services section of the Product Terms.
Metrics in the form of KPIs	<p>Online Services SLAs contain service specific terms with relevant service performance metrics in the form of monthly uptime percentages.</p> <p>Microsoft monitors SLA performance and notifies customers if there is a lapse.</p> <p>Microsoft publishes information concerning the current health and status of Dynamics services on in the Microsoft 365 admin center.</p>
Records demonstrating fulfillment of specified service levels	<p>Per the Online Services Data Protection Addendum (DPA), Microsoft maintains several logs and records related to security and data protection commitments:</p> <ul style="list-style-type: none"> • Event logging: Microsoft logs, or enables customer to log, access and use of information systems containing customer data, registering the access ID, time, authorization granted or denied, and relevant activity. • Physical Access to Components: Microsoft maintains records of the incoming and outgoing media containing customer data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of customer data they contain. • Access Policy: Microsoft maintains a record of security privileges of individuals having access to customer data. • Access Authorization: Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain customer data. • Incident Response: Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, to whom the breach was reported, and the procedure for recovering data. • Data Recovery: Microsoft logs data restoration efforts, including the person responsible, the description of the restored data, and where applicable, the person responsible, and which data (if any) had to be input manually in the data recovery process. <p>As described in Section 2.3.4, a records management procedure exists that defines records retention for support metrics and trending, which are periodically reviewed as part of the internal Microsoft auditing process as well by external third-party auditors during the SOC audit and ISO certification processes.</p> <p>Per the Online Services Data Protection Addendum (DPA), to the extent needed to perform the audit, Microsoft will make the</p>

Typical SLA/Quality Agreement Content	Coverage
	<p>processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Microsoft, its Affiliates, and its Subprocessors available.</p>
<p>Pricing arrangements, including penalties in case of shortcomings</p>	<p>Pricing arrangements for enterprise customers are stipulated in the Enterprise Agreement.</p> <p>Online Services SLAs contain service specific terms outlining service credits that customers will receive should the services fail to meet the stated uptime performance metrics.</p>
<p>Reports, scope, frequency, distribution</p>	<p>Microsoft provides customers access to 3rd party audit reports, via the Service Trust Portal. As per the Online Services Data Protection Addendum (DPA), these audits will be initiated at least annually, and each audit will result in the generation of an audit report.</p>
<p>Audit provisions, including preparedness to facilitate inspections from regulatory authorities or other regulators</p>	<p>Per the Online Services Data Protection Addendum (DPA), Microsoft will conduct audits of the security of the computers, computing environment, and physical datacenters, as follows:</p> <ul style="list-style-type: none"> • Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service. • Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. • Each audit will be performed by qualified, independent, third-party security auditors at Microsoft’s selection and expense. <p>Each audit will result in the generation of an audit report that will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft audit report to the satisfaction of the auditor.</p> <p>Within its Security Policy, Microsoft defines technical and organizational measures to protect customer data. Microsoft will make that policy available to customers.</p> <p>Each Online Service follows a written data security policy (Information Security Policy) that complies with the following control standards and frameworks:</p> <ul style="list-style-type: none"> • ISO 27001 • ISO 27002 • ISO 27018 • SSAE 18 SOC 1 Type II • AT 101 SOC 2 Type II

Typical SLA/Quality Agreement Content	Coverage
	<p>Customers may contact their Microsoft Account Managers for support requests should additional information be requested by a regulatory authority.</p>
<p>Defined parameters for roles and responsibilities (for example, maintenance of quality system requirements and controls) as per quality agreements requirements for EU GMP Annex 11 [1]</p>	<p>Microsoft responsibilities, controls, and practices concerning the following quality related activities are defined within the Online Services Data Protection Addendum (DPA):</p> <ul style="list-style-type: none"> • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information security incident management • Business continuity management <p>Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to customer data.</p>
<p>Processes to be supported and managed between the two parties, and the service levels including escalation, (for example, parameters for backup frequency, retention periods, and retrieval times)</p>	<p>The Online Services Data Protection Addendum (DPA) includes a description of the Data Protection Terms, including the terms for Data Retention and Deletion which states that Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of a customer’s subscription so that the customer may extract the data.</p> <p>The customer’s selected support plan specified as part of the Enterprise Agreement will indicate the range of support coverage, incident response time commitments, and the type of escalation and account management services to be provided.</p>

Appendix C. US FDA 21 CFR Part 11 Electronic Records; Electronic Signatures - Shared Responsibilities

The objective of this analysis is to identify the procedural and technical controls that are required to satisfy the regulatory requirements of U.S. FDA 21 CFR Part 11, both internally within Microsoft and externally for Microsoft life sciences customers.

Microsoft responsibilities are mapped to Trust Criteria and Cloud Controls Matrix (CCM) Criteria evaluated as part of the most recent SOC2 report for Microsoft Azure/Dynamics 365. The Trust and CCM Criteria pertain to trust service principles and criteria that are met by control activities provided by Microsoft Azure and Microsoft datacenters.

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
Subpart B — Electronic Records	
Sec. 11.10 Controls for closed systems.	
<p>11.10 <i>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</i></p>	
<p>11.10 (a) <i>Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Perform and document the validation activities to demonstrate that any GxP system managing electronic records is fit for its intended use and conforms to the specified requirements. - Establish appropriate system performance monitoring to ensure consistent availability and performance of GxP system(s). <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Procedures and controls are in place to ensure the Dynamics 365 tools and applications are developed and tested in accordance with industry best practices and standards (for example, ISO 9001 and ISO/IEC 27001) to ensure quality, security, as well as consistent and reliable performance. (Refer to SOC 2 Trust Criteria: CC5.2, CC8.1; CMM Criteria: AIS-01, CCC-01, DSI-05, IVS-08, IVS-13, STA-03) - Controls have been implemented to ensure the integrity of virtual machine images and provide alerts to customers of potential changes and events that may affect security or availability of the services in a timely manner (Refer to SOC 2 Trust Criteria: CC2.2, CC2.3, CC3.1, PI1.1, CC7.1, CC8.1; CCM Criteria: CCC-02, CCC-05, DSI-02, GRM-02, GRM-08, GRM-10, IAM-09, STA-05, TVM-02)

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.10 (b) <i>The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Follow security best practices to secure and protect data transferred to Dynamics 365. - Verify electronic records copied from the GxP system(s) are accurate and complete, ensuring that data integrity is maintained. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Controls are implemented to ensure system output is complete, accurate, distributed, and retained to meet the processing integrity commitments and system requirements. (Refer to SOC 2 Trust Criteria: A1.1, A1.2, PI1.1, PI1.3, PI1.5; CCM Criteria: AIS-03, AIS-04, CCC-03, IPY-03) - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (Refer to SOC 2 Trust Criteria: A1.1, PI1.3; CCM Criteria: CCC-05, DSI-02, STA-05, STA-07)
<p>11.10 (c) <i>Protection of records to enable their accurate and ready retrieval throughout the records retention period.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Follow security best practices to secure and protect data transferred to Dynamics 365. - Implement appropriate security controls governing access to Dynamics 365 services and GxP system(s) including permissions to regulated data. - Ensure backup processes are tested so that data integrity is maintained. - Define record retention policies for regulated data. - Ensure disaster recovery and business continuity processes are in place and tested. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Security controls to protect Dynamics 365 services and infrastructure are in place (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02, DCS-06, DCS-07, DCS-09) - Controls are implemented to ensure data is stored and maintained completely, accurately, and in a timely manner for its specified lifespan. (Refer to SOC 2 Trust Criteria: A1.1, A1.2, PI1.1, PI1.3, PI1.5; CCM Criteria: AIS-03, IPY-03) - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (Refer to SOC 2 Trust Criteria: A1.1, PI1.3; CCM Criteria: CCC-05, DSI-02, STA-05, STA-07) - Controls are in place to oversee the service of data backup or mirroring (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC6.7, CC7.2, A1.2, A1.3, C1.1, C1.2, PI1.3, PI1.5; CCM Criteria: BCR-06, BCR-11, DSI-07, DCS-04, DCS-05, EKM-03)

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.10 (d) <i>Limiting system access to authorized individuals.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Establish appropriate logical security processes governing the administration of system users/administrators to ensure segregation of duties and assignment of permissions according to the principle of least privilege. - Verify control mechanisms for limiting access are properly configured. - Implement periodic review of assigned access rights. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Physical and logical security policies are in place to limit access to authorized individuals based on the individual's job duties. (Refer to SOC 2 Trust Criteria: CC1.3, CC1.5, CC2.2, CC6.1, CC6.3, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02)
<p>11.10 (e) <i>Use of secure, computer-generated time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system generates secure audit trails as required by predicate rules for regulated electronic records. - Implement appropriate security controls to restrict access to regulated audit trail data, for example, that audit trail functionality cannot be disabled. - Ensure that data backup processes are in place and have been tested for applicable audit trail data. - Establish record retention policies that include relevant audit trail data. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft has established an Audit Log Management policy. Access to the log is restricted to authorized individuals (Refer to SOC 2 CCM Criteria: IAM-01, IVS-01) - Security controls to protect cloud services and infrastructure are implemented (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02, DCS-06, DCS-07, DCS-09) - Controls are in place to oversee service of data backup or mirroring (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC6.7, CC7.2, A1.2, A1.3, C1.1, C1.2, PI1.3, PI1.5; CCM Criteria: BCR-06, BCR-11, DSI-07, DCS-04, DCS-05, EKM-03)
<p>11.10 (f) <i>Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system enforces permitted sequencing of steps and events, as required, based on the business process requirements supported by the GxP system(s). <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.10 (g) <i>Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that appropriate logical security policies are established, and training has been documented. - Implement appropriate user access management practices to ensure that users are assigned permissions based on their job functions. - Implement periodic review of assigned access rights. - Verify that any GxP system only permits authorized actions to be taken with respect to regulated content. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>11.10 (h) <i>Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system uses device checks to determine the data source validity, as required, based on the business process requirements supported by the GxP system(s). <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>11.10 (i) <i>Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Implement appropriate user, developer, and/or administrator training processes. - Ensure personnel have adequate experience/qualification/training to perform their job duties. - Maintain records of personnel training and qualifications (that is, training records, job descriptions, CV). <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Training procedures have been established to evaluate the competency of personnel based on their job function. (Refer to SOC 2 Trust Criteria: CC1.1, CC1.4, CC1.5, CC2.2, CC2.3, CC5.3; CCM Criteria: BCR-10, GRM-03, GRM-06, HRS-04, HRS-05, HRS-09)
<p>11.10 (j) <i>The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that appropriate training policies are established, and that training and personnel qualification are documented (that is, training records, CV). <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.10 (k) <i>Use of appropriate controls over systems documentation including:</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Documents under the scope of these requirements are procedures, requirements, specifications, validation documents, and so on. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Documents under the scope of these requirements are system descriptions, procedures, and technical specifications.
<p>11.10 (k)(1) <i>Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Implement procedural controls to manage the distribution, access, and use of system documentation for Dynamics 365 services which support GxP activities. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Procedural controls are in place to appropriately manage the distribution, access, and use of system documentation produced for Dynamics 365 operations and maintenance. (Refer to SOC 2 Trust Criteria: CC2.2, CC2.3, CC4.1, CC4.2, CC5.3, CC7.4, CC8.1, A1.1, A1.2, PI1.3, PI1.4; CCM Criteria: BCR-01, BCR-04)
<p>11.10 (k)(2) <i>Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure documentation and change management procedures are in place, as well as controls to maintain an audit trail that documents time-sequenced development and modification of systems documentation. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Documentation and change management controls (that is, procedures) are in place (Refer to SOC 2 Trust Criteria: CC7.1, CC8.1; CCM Criteria: CCC-02, CCC-03, CCC-05, GRM-01, TVM-02)
<p>Sec. 11.30 Controls for Open Systems</p>	
<p>11.30 <i>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Configure encryption and access controls to ensure that the integrity of data is maintained. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - A series of procedural and technical controls are in place to ensure the protection and confidentiality of customer data (Refer to SOC 2 Trust Criteria: CC2.2, CC2.3, C1.1, C1.2, PI1.1; CCM Criteria: AIS-04, CCC-03, DSI-02, HRS-03, HRS-06, STA-05, STA-09) - Internal communication where customer data is transmitted / involved is secured using SSL or equivalent mechanisms and travels within secured tunnel (Refer to SOC 2 Trust Criteria: CC6.1, CC6.6, CC6.7; CCM Criteria: DSI-03, EKM-03, EKM-04, IVS-10, IVS-12, IPY-04)
<p>Sec. 11.50 Signature manifestations</p>	

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.50 (a) <i>Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</i></p> <p>11.50 (a) (1) <i>The printed name of the signer;</i></p> <p>11.50 (a) (2) <i>The date and time when the signature was executed; and</i></p> <p>11.50 (a) (3) <i>The meaning (such as review, approval, responsibility, or authorship) associated with the signature.</i></p> <p>11.50 (b) <i>The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Sec. 11.70 Signature/record linking	
<p>11.70 <i>Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure that the use and elucidation of electronic signatures are defined with a procedure or policy. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Subpart C — Electronic Signatures	
Sec. 11.100 General requirements	
<p>11.100 (a) <i>Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure that the use and elucidation of electronic signatures are defined with a procedure or policy. - Ensure procedure controls are in place to govern the assignment of electronic signatures. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>11.100 (b) <i>Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure procedure controls are in place to govern the assignment of electronic signatures. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.100 (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.</p> <p>11.100 (c) (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.</p> <p>11.100 (c) (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that letter has been sent to FDA. Confirm applicability with the organization's quality assurance or compliance department. - Ensure procedure controls are in place to govern the assignment of electronic signatures including a form where users have signed an agreement indicating that their electronic signature is the legally binding equivalent of the signer's handwritten signature. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Sec. 11.200 Electronic signature components and controls	
<p>11.200 (a) Electronic signatures that are not based upon biometrics shall:</p>	
<p>11.200 (a) (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.</p> <p>11.200 (a) (2) Be used only by their genuine owners; and</p> <p>11.200 (a) (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure that the use and elucidation of electronic signatures are defined within a procedure or policy. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>11.200 (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure procedure controls are in place to govern the use and assignment of electronic signatures. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Sec. 11.300 Controls for identification codes/passwords.	

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.300 <i>Controls for identification codes/passwords. Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</i></p>	
<p>11.300 (a) <i>Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure procedure controls are in place to govern the assignment of electronic signatures. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>11.300 (b) <i>Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure procedure controls are in place to govern the assignment and management of electronic signatures. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>11.300 (c) <i>Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure that the use and management of electronic signatures are defined within a procedure or policy. - Ensure procedure controls are in place to assist in meeting this requirement. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>11.300 (d) <i>Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure that the use and management of electronic signatures are defined within a procedure or policy. - Ensure procedure controls are in place to assist in meeting this requirement. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

U.S. FDA 21 CFR Part 11	Customer / Microsoft responsibilities
<p>11.300 (e) <i>Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.</i></p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure procedure controls are in place to assist in meeting this requirement. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

Appendix D. EudraLex Volume 4 Annex 11 Computerised Systems - Shared Responsibilities

The objective of this analysis is to identify the procedural and technical controls that are required to satisfy the regulatory requirements of EudraLex Volume 4 Annex 11, both internally within Microsoft and externally for Microsoft life sciences customers.

The following tables show how Microsoft and customer responsibilities are shared. In addition, for each Microsoft responsibility, the corresponding controls in the Microsoft SOC 2 Report have been referenced as well as other control activities that Microsoft has in place.

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
General	
1. Risk Management	
Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Document the assessment of risks related to patient safety, data integrity, and product quality as part of the validation activities around the leveraged GxP relevant Dynamics 365 services. - Define and implement the necessary controls to mitigate risks and ensure data integrity. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Risk management is incorporated into processes around the development and maintenance of the Microsoft Dynamics 365 applications and tools (Refer to SOC 2 Trust Criteria: CC2.1, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC5.1, CC9.1; CCM Criteria: GRM-04, STA-05)
2. Personnel	

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Identify key stakeholders for all GxP relevant Dynamics 365 services. - Implement appropriate user, developer, and/or administrator training processes. - Ensure personnel have adequate experience/qualification/training to perform their job duties. - Ensure personnel training and qualifications are documented (that is, training records, CV). - Establish appropriate logical security processes that govern the administration of system users/administrators to ensure segregation of duties and assignment of permissions according to the principle of least privilege. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Training procedures have been established to evaluate the competency of personnel and engaged third parties (contractors) based on their job function. (Refer to SOC 2 Trust Criteria: CC1.1, CC1.4, CC1.5, CC2.2, CC2.3, CC5.3; CCM Criteria: BCR-10, GRM-03, GRM-06, HRS-04, HRS-05, HRS-09) - Physical and logical security policies are in place to limit access to authorized individuals based on the individual's job duties. (Refer to SOC 2 Trust Criteria: CC1.3, CC1.5, CC2.2, CC6.1, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02)
<p>3. Suppliers and Service Providers</p>	
<p>3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that formal agreements are implemented with suppliers that clearly define the roles and responsibilities of each party. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Contracts are in place with Microsoft suppliers to identify responsibilities, and procedures are followed to periodically monitor and review activities for inconsistencies or non-conformance. (Refer to SOC 2 Trust Criteria: CC9.2; CCM Criteria: IAM-09, STA-07, STA-08, STA-09) - Formal agreements are implemented between Microsoft and its customers that include statements of responsibilities as described with in the Online Services Data Protection Addendum (DPA).

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that the supplier assessment process is documented and provides rationale to support the method implemented to qualify a selected supplier. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Risks related to external parties are assessed and addressed (Refer to SOC 2 Trust Criteria: CC1.3, CC2.1, CC2.3, CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, CC8.1, CC9.2; CCM Criteria: CCC-02, DSI-02, GRM-02, GRM-08, GRM-10, GRM-11, SEF-01, IAM-07, STA-01, STA-05, STA-06, STA-07, STA-08, STA-09)
<p>3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Define regulated user requirements. - Review product documentation published on Dynamics 365 Documentation site and within the Service Trust Platform (STP) to ensure regulated user requirements are fulfilled. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft continuously publishes and updates content on the Dynamics 365 Documentation site and within the Service Trust Platform (STP) to ensure it accurately reflects the current product portfolio and capabilities. - Microsoft also provides extensive documentation in the form of websites, white papers, Microsoft employee blog entries, and video tutorials that describe the installation, configuration, and use of products and features on the Dynamics 365 training website.
<p>3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Review the most recent Microsoft Dynamics 365 ISO and SOC audit reports produced by independent third-party organizations and document the results of the assessment as necessary based on internal processes. - Ensure that supplier/vendor assessment information is available to inspectors when requested. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) (Refer to SOC 2 Trust Criteria: CC2.3)
<p>Project Phase</p>	
<p>4. Validation</p>	

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Implement a formal computer system validation policy or procedure that conforms to the specified requirements. - Perform and document the qualification/validation of the Dynamics 365 service based on a risk assessment. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Procedures and controls are in place to ensure the Dynamics 365 applications and tools are developed and tested in accordance with industry best practices and standards (for example, ISO 9001 and ISO/IEC 27001) to ensure quality and security as well as consistent and reliable performance. (Refer to SOC 2 Trust Criteria: CC5.2, CC8.1; CCM Criteria: AIS-01, CCC-01, IVS-13, STA-03) - Risk management is incorporated into processes around the development and maintenance of the Microsoft Dynamics 365 applications and tools (Refer to SOC 2 Trust Criteria: CC2.1, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC5.1, CC9.1; CCM Criteria: GRM-04, STA-05)
<p>4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Implement formal change control and deviation management processes in conjunction with validation of GxP applications. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - A formal change management process is defined governing how changes are made to the Dynamics 365 (including products, services, and supporting hardware) (Refer to SOC 2 Trust Criteria: CC7.1, CC8.1; CCM Criteria: CCC-02, CCC-03, CCC-05, GRM-01, TVM-02)

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.</p> <p>For critical systems, an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Implement formal change control and deviation management processes in conjunction with validation of GxP applications. - Ensure controls are established to maintain current copies of any system documentation required to manage applicable GxP computerized systems. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft maintains an inventory of key information assets. Procedures are established to review the inventory on a quarterly basis. (Refer to SOC 2 Trust Criteria: CC5.2, CC6.1, CC6.4; CCM Criteria: DSI-02, DSI-04, DSI-06, DCS-01) - Controls are in place to ensure the Dynamics 365 services and its supporting infrastructure (including products, services, and supporting hardware) are maintained in a state of control and compliance (Refer to SOC 2 Trust Criteria: CC5.2, CC8.1; CCM Criteria: AIS-01, AAC-03, CCC-01, IVS-13, STA-03) - A detailed system description of Azure services (including Dynamics 365) is contained with the SOC and ISO/IEC 27001 audit reports, which is available to customers via the Service Trust Platform (STP).
<p>4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Implement formal change control and deviation management processes in conjunction with validation of GxP applications. - Ensure controls are established to maintain current copies of any system documentation required to manage applicable GxP computerized systems. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft Dynamics 365 system requirements as they relate to the development of new features and major platform changes follow a defined approach based on the Security Development Lifecycle (SDL) (Refer to SOC 2 Trust Criteria: CC5.2, CC8.1; CCM Criteria: AIS-01, CCC-01, DSI-05, IVS-08, IVS-13, STA-03) - Formal risk assessments are performed on a regular basis (Refer to SOC 2 Trust Criteria: CC3.2, CC3.3, CC3.4; CCM Criteria: BCR-08, BCR-09, GRM-02, GRM-10)

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Review the most recent Microsoft Dynamics 365 ISO and SOC audit reports produced by independent third-party organizations and document the results of the assessment as necessary based on internal processes. - Ensure that supplier/vendor assessment information is available to inspectors when requested. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft regularly undergoes independent audits performed by qualified third-party accredited assessors for ISO (27001, 27018 & 9001), SOC (1, 2, 3), HITRUST, FedRAMP and PCI (Refer to Section 2.2) - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) (Refer to SOC 2 Trust Criteria: CC2.3)
<p>4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Establish controls to ensure the assessment of quality and performance metrics throughout the GxP computerized system’s lifecycle. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft Dynamics 365 development teams follow defined processes for verifying newly developed products and features, as well as for product changes and enhancements (Refer to SOC 2 CCM Criteria: CCC-01, CCC-03) - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) (Refer to SOC 2 Trust Criteria: CC2.3)
<p>4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure the implementation and use of a formal computer system validation policy or procedure that meets these requirements. - Document the qualification and validation testing activities in accordance with established processes. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft Dynamics 365 development teams follow defined processes for verifying newly developed products and features, as well as for product changes and enhancements (Refer to SOC 2 CCM Criteria: CCC-01, CCC-03) - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) (Refer to SOC 2 Trust Criteria: CC2.3)

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Establish data migration plan and testing strategy to ensure data integrity is maintained during the migration process. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>Operational Phase</p>	
<p>5. Data</p>	
<p>Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that encryption and access controls are in place so that the integrity of data is maintained. - Ensure that appropriate logical security policies are established, and training has been documented. - Implement appropriate user access management practices to ensure that users are assigned permissions based on their job functions. - Implement periodic review of assigned access rights. - Verify GxP system only permits authorized actions to be taken with respect to regulated content. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Encryption and access controls have been implemented to ensure that the integrity of data is maintained (Refer to SOC 2 Trust Criteria: CC6.1, CC6.6, CC6.7; CCM Criteria: DSI-03, EKM-03, EKM-04, IVS-10, IVS-12, IPY-04)
<p>6. Accuracy Checks</p>	
<p>For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Establish procedural controls to enforce review of manually entered data or implement automated accuracy check mechanisms as part of the GxP system design / configuration. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>7. Data Storage</p>	

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Follow security best practices to secure and protect data transferred to Dynamics 365. - Implement appropriate security controls governing access to Dynamics 365 services and GxP system(s) including permissions to regulated data. - Ensure backup processes and systems are tested so that data integrity is maintained. - Define record retention policies for regulated data. - Ensure disaster recovery and business continuity processes are in place and tested. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Security controls to protect Dynamics 365 online services and infrastructure are in place (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02, DCS-06, DCS-07, DCS-09) - Controls are implemented to ensure data is stored and maintained completely, accurately, and in a timely manner for its specified life span. (Refer to SOC 2 Trust Criteria: A1.1, A1.2, PI1.1, PI1.3, PI1.5; CCM Criteria: AIS-03, IPY-03) - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (Refer to SOC 2 Trust Criteria: A1.1, PI1.3; CCM Criteria: CCC-05, DSI-02, STA-05, STA-07) - Controls are in place to oversee the service of data backup or mirroring (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC6.7, CC7.2, A1.2, A1.3, C1.1, C1.2, PI1.3, PI1.5; CCM Criteria: BCR-06, BCR-11, DSI-07, DCS-04, DCS-05, EKM-03)

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that backup infrastructure and policies are in place and have been tested for applications/systems/data maintained within Dynamics 365 services. - Ensure appropriate governance of system administration activities around the management of Microsoft Dynamics 365 services. - Ensure that encryption and access controls are in place to ensure that the integrity of data is maintained. - Verify that any leveraged GxP relevant Dynamics 365 service conforms to the specified regulatory requirement. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (Refer to SOC 2 Trust Criteria: A1.1, PI1.3; CCM Criteria: CCC-05, DSI-02, STA-05, STA-07) - Physical and logical security policies are in place and followed (Refer to SOC 2 Trust Criteria: CC1.3, CC1.5, CC2.2, CC6.1, CC6.3, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02) - Controls are in place to ensure that actions of Microsoft personnel with access to production systems are limited and do not interfere with the integrity of customer data (Refer to SOC 2 Trust Criteria: C1.1, C1.2)
<p>8. Printouts</p>	
<p>8.1 It should be possible to obtain clear printed copies of electronically stored data.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure through verification that the transfer of data from applications/systems within the leveraged GxP relevant Dynamics 365 services (which may store data) does not affect data integrity. - Verify that any GxP relevant Dynamics 365 service employed conforms to the specified regulatory requirement. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP relevant Dynamics 365 service employed conforms to the specified regulatory requirement. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>9. Audit Trails</p>	

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Perform a risk assessment to determine where audit trails need to be implemented and verified within the GxP system(s). <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>10. Change and Configuration Management</p>	
<p>Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that appropriate logical security policies are established, and training has been documented. - Ensure that appropriate security controls are defined to govern application/system/Dynamics 365 access along with permissions related to data. - Ensure appropriate system administration practices are followed for Dynamics 365 applications/systems. - Ensure appropriate governance of system administration activities around the management of Microsoft Dynamics 365 services. - Ensure that backup infrastructure and policies are in place and have been tested for GxP related data maintained within Microsoft Dynamics 365. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Microsoft notifies customers of potential changes and events that may affect security or availability of the services (Refer to SOC 2 Trust Criteria: CC2.2, CC7.1, CC8.1; CCM Criteria: CCC-02, CCC-03, CCC-05, GRM-01, TVM-02)
<p>11. Periodic evaluation</p>	
<p>Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that procedural controls are in place to periodically review the state of GxP related Dynamics 365 services. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Controls are in place to periodically review the state of components deployed within Dynamics 365 to ensure their configuration is aligned with the baseline configuration (Refer to SOC 2 Trust Criteria: CC4.1, CC7.2; CCM Criteria: STA-04)
<p>12. Security</p>	

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.</p> <p>12.2 The extent of security controls depends on the criticality of the computerised system.</p> <p>12.3 Creation, change, and cancellation of access authorisations should be recorded.</p> <p>12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that appropriate security controls are defined to govern application/system/Dynamics 365 access along with permissions related to data. - Ensure that appropriate logical security policies are established, and training has been documented. - Ensure appropriate system administration practices are followed for Dynamics 365 applications/systems. - Ensure that audit trails have been properly defined and verified. - Ensure procedure controls are in place to help meet this requirement. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Security policies are in place (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02, DCS-06, DCS-07, DCS-09) - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (Refer to SOC 2 Trust Criteria: A1.1, PI1.3; CCM Criteria: CCC-05, DSI-02, STA-05, STA-07)
<p>13. Incident Management</p>	
<p>All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure procedure controls are in place to manage system incidents and perform root cause analysis to identify corrective and preventive actions. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Ensure procedure controls are in place to manage system incidents and perform root cause analysis to identify corrective and preventive actions (Refer to SOC 2 Trust Criteria: CC2.2, CC2.3, CC3.2, CC3.3, CC4.1, CC4.2, CC5.3, CC6.1, CC6.8, CC7.2, CC7.3, CC7.4, CC7.5; CCM Criteria: BCR-02, BCR-10, SEF-02 - SEF-05)
<p>14. Electronic Signature</p>	
<p>Electronic records may be signed electronically. Electronic signatures are expected to:</p> <ol style="list-style-type: none"> a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied. 	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure procedure controls are in place to govern the use and assignment of electronic signatures. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>15. Batch Release</p>	

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. - Ensure procedure controls are in place to govern the use and assignment of electronic signatures. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
<p>16. Business Continuity</p>	
<p>For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Ensure that mechanisms for disaster recovery and business continuity are in place and tested. - Ensure that backup infrastructure and policies are in place and have been tested. - Implement and test data repatriation plan(s). <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Ensure that mechanisms for disaster recovery and business continuity are in place and tested, should any issue arise with Dynamics online services (Refer to SOC 2 Trust Criteria: CC3.2, CC5.1, CC5.2, CC7.5, A1.1, A1.2, A1.3; CCM Criteria: BCR-01, BCR-02, BCR-05, BCR-08 - BCR-11) - Ensure that backup infrastructure and policies are in place and have been tested (Refer to SOC 2 Trust Criteria: A1.2, A1.3, PI1.3, PI1.5) - Implement and test data repatriation plan(s) (Refer to SOC 2 CCM Criteria: IPY-02) - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (Refer to SOC 2 Trust Criteria: A1.1, PI1.3; CCM Criteria: CCC-05, DSI-02, STA-05, STA-07)
<p>17. Archiving</p>	

EU Volume 4 Annex 11	Customer / Microsoft responsibilities
<p>Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.</p>	<p>Customer responsibilities</p> <ul style="list-style-type: none"> - Follow security best practices to secure and protect data transferred to Dynamics 365. - Implement appropriate security controls that govern access to Dynamics 365 services and GxP system(s) including permissions to regulated data. - Ensure backup processes and systems are tested so that data integrity is maintained. - Define record retention policies for regulated data. - Ensure disaster recovery and business continuity processes are in place and tested. <p>Microsoft responsibilities</p> <ul style="list-style-type: none"> - Security controls to protect Dynamics 365 online services and infrastructure are in place (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC7.3, CC7.4, CC7.5, PI1.4; CCM Criteria: DCS-02, DCS-06, DCS-07, DCS-09) - Controls are implemented to ensure data is stored and maintained completely, accurately, and in a timely manner for its specified life span. (Refer to SOC 2 Trust Criteria: A1.1, A1.2, PI1.1, PI1.3, PI1.5; CCM Criteria: AIS-03, IPY-03) - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (Refer to SOC 2 Trust Criteria: A1.1, PI1.3; CCM Criteria: CCC-05, DSI-02, STA-05, STA-07) - Controls are in place to oversee the service of data backup or mirroring (Refer to SOC 2 Trust Criteria: CC6.1, CC6.5, CC6.6, CC6.7, CC7.2, A1.2, A1.3, C1.1, C1.2, PI1.3, PI1.5; CCM Criteria: BCR-06, BCR-11, DSI-07, DCS-04, DCS-05, EKM-03)