Microsoft 365

Microsoft 365 GxP Guidelines

White paper

July 2020

DISCLAIMER

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 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 365.

Daniel Carchedi – Sr. Director Business Development & Strategy Life Sciences

Microsoft Corporation

July 2020

Executive Summary

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. By leveraging Microsoft 365 controls to help manage regulated GxP content, life science customers can configure the necessary protocols to help ensure the integrity and security of their data.

The purpose of this document is to demonstrate that as a cloud solution provider, Microsoft has the necessary technical and procedural controls to maintain the Microsoft 365 platform in a state of control by preserving the confidentiality, integrity and availability of our customers' data. This document identifies the shared responsibilities between Microsoft and our 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 content, 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 Microsoft 365, 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. This document highlights the extensive controls implemented as part of Microsoft 365's internal development of security and quality practices, which help to ensure that the Microsoft 365 platform meets its specifications and is maintained in a state of control. Microsoft 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 integrity of GxP content. This guidance document includes recommendations based on proven practices of existing life sciences customers as well as industry standards for 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 content 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 and assessment of the cloud service provider is performed.
- ✓ Systems are designed to preserve system resiliency, performance, data security, and confidentiality.
- ✓ Data integrity and compliance with regulatory requirements is verified.

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, ife sciences, technology, strategy, and account management. We collaborated with our longstanding life sciences industry partner, Montrium, to review Microsoft 365 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. In producing this document, Montrium took advantage of the extensive practical experience gained while managing their SharePoint-based GxP solutions suite, which is currently used by their life sciences customers to support various GxP-regulated processes and records.

Table of contents

Foreword 3

Executive summary 4

Authors 5

1 Introduction 9

1.1 Purpose 9

1.2 Document overview 9

1.3 Audience and scope 10

1.4 Key terms and definitions 10

1.4.1 Customer 10

1.4.2 GxP 10

1.4.3 GxP regulations 10

2 Overview of Microsoft 365 11

2.1 Establishing trust 12

2.2 Microsoft 365 certifications and attestations 13

2.2.1 SOC 1 and SOC 2 14

2.2.2 ISO/IEC 27001:2013 15

2.2.3 ISO/IEC 27017:2015 15

2.2.4 ISO/IEC 27018:2014 15

2.2.5 HITRUST 16

2.2.6 FedRAMP 16

2.3 Microsoft 365 Quality and Secure Development Lifecycle 16

2.3.1 Roles and responsibilities 17

2.3.2 Policies and standard operating procedures 19

2.3.3 Microsoft personnel and contractor training 19

2.3.4 Risk Management 20

2.3.5 Design and development of Microsoft 365 services 20

2.3.6 Operations management 22

2.3.6.1 Handover 22

2.3.6.2 Service management and performance monitoring 22

2.3.6.3 Incident management 23

2.3.6.4 Change management 23

2.3.6.5 Audits and review 24
2.3.6.6 Continuity management 24
2.3.6.7 Security and system administration 25
2.3.6.8 Records management 27
3 Recommendations for implementing a Microsoft 365 GxP compliance framework 27
3.1 Data integrity controls 28
3.1.1 Key Microsoft 365 features supporting data integrity 30
3.1.1.1 Sensitivity labels 30
3.1.1.2 Retention labels 31
3.1.1.3 Overarching site retention policies 31
3.1.1.4 Record metadata 31
3.1.1.5 Audit Log 32
3.1.1.6 Versioning 32
3.1.1.7 Library restore 32
3.1.1.8 Site Designs and Site Scripts 33
3.1.1.9 Power Automate 33
3.1.1.10 Microsoft Compliance Score 34
3.1.2 Considerations for FDA 21 CFR Part 11 compliance 35
3.2 Microsoft 365 governance recommendations 37
3.2.1 Shared responsibilities 37
3.2.2 Service agreements 38
3.2.2.1 Service level agreements 38
3.2.2.2 Online Services Terms and Online Services Data Protection Addendum 39
3.2.2.3 HIPAA Business Associate Agreement 39
3.2.2.4 Other agreements 39
3.2.3 Governance policies and procedures 40
3.2.3.1 Quality governance processes 40
3.2.3.2 Operational and IT governance processes 42
3.3 GxP Use Cases 46
3.4 Considerations for implementing a risk-based validation strategy 46
3.4.1 GAMP 5 Software Category 47
3.4.2 Application Stakeholders 48

3.4.3 Computerized system life cycle approach 48
3.4.3.1 Concept 49
3.4.3.2 Project 50
3.4.3.3 Operation 56
3.4.3.4 Retirement 56
4 Conclusion 58
5 Document Revision 58
6 References 59
6.1 Industry guidance and standards 59
6.2 Regulations and regulatory guidance 59
6.3 Microsoft resources and reference material 59
6.3.1 Additional resources and reference material 61
7 Appendices 61

1 Introduction

1.1 Purpose

At Microsoft, we understand that by leveraging Microsoft 365 to manage regulated GxP content, life sciences customers are relinquishing a portion of their control and trust us to help ensure the integrity and security of their data. The purpose of this document is to demonstrate that as a cloud solution provider, Microsoft has the necessary technical and procedural controls to maintain the Microsoft 365 platform in a state of control by preserving the confidentiality, integrity and availability of our customers' data.

In addition, this GxP guidance document outlines vital capabilities and features of Microsoft 365 that make it an optimal solution for managing GxP content. Our goal is to provide life sciences organizations with a comprehensive toolset for using Microsoft 365 while adhering to industry best practices and applicable regulations. To achieve this goal, we identified the proven practices of existing life sciences customers and partners who currently use Microsoft 365 to manage GxP content. 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.

1.2 Document overview

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

- Increased visibility into crucial areas of Microsoft's quality management, software development, and service delivery practices.
- Recommendations for customer GxP compliance readiness, including an approach for validating Microsoft 365 and establishing governance processes to support the management of GxP content within Microsoft 365.
- Description of GxP-relevant tools and features within Microsoft 365.
- In-depth analysis of shared responsibilities concerning 21 CFR Part 11 and 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 our customers. We have implemented a series of technical and procedural controls to help ensure the dependability (accessibility, availability, reliability, safety, integrity, and maintainability) of our systems and services. Of equal importance are the activities performed by our customers in protecting the security and privacy of their data.

This guidance document begins with an initial focus on internal Microsoft 365 quality and development practices, followed by a customer focus consisting of our recommendations to help life sciences industry customers seeking to leverage Microsoft 365 in the context of GxP regulated processes.

Microsoft 365 focus[1]

- Overview of Microsoft 365, including
  - Summary of relevant Microsoft 365 certifications and attestations
  - Description of Microsoft 365 software quality and secure development practices

Life sciences customer focus[2]

- Implementing an Microsoft 365 compliance lifecycle
  - Microsoft 365 governance recommendations
  - Considerations for US FDA 21 CFR Part 11 compliance
  - Valdiation considerations when using Microsoft 365 to manage GxP content

[1] Section 2 of this document includes details about internal Microsoft systems, controls, and processes.

[2] Section 3 of this document includes recommendations for customers using Microsoft 365 to support GxP regulated activities.

1.3 Audience and scope

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

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

Microsoft 365 consists of several applications; however, we will focus on the content management functionality of SharePoint Online and OneDrive for Business, as these can be used to support the management of electronic records generated by our life sciences customers. SharePoint Online and OneDrive for Business provide the ability to create content repositories that can be configured with built-in security, audit trail, versioning and retention functionality, allowing customers to store GxP regulated content in a compliant manner.

1.4 Key terms and definitions

1.4.1 Customer

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

1.4.2 GxP

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

1.4.3 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, US 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)

2 Overview of Microsoft 365

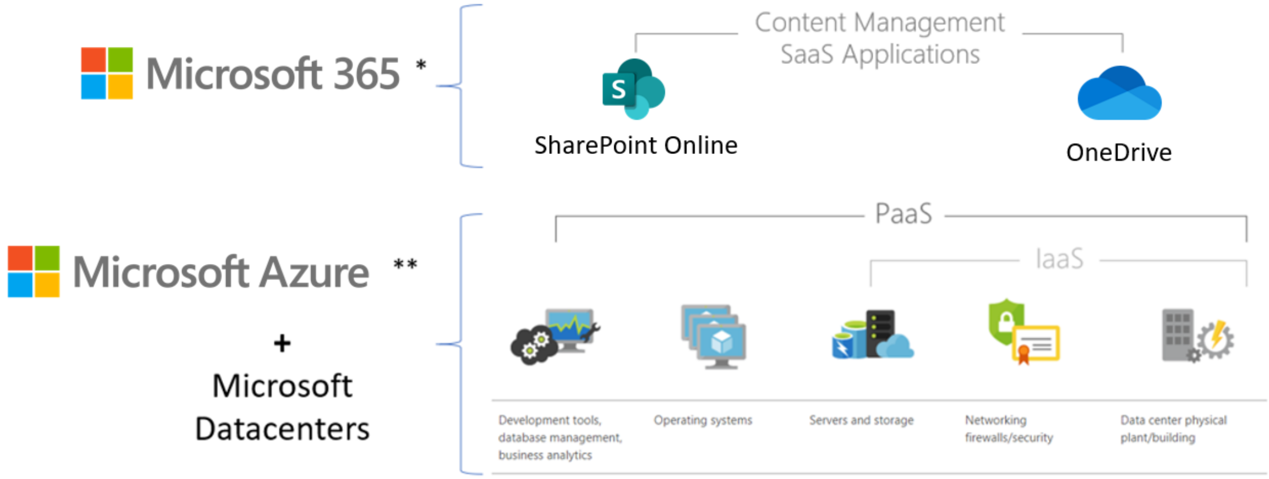
Microsoft 365 is a multi-tenant subscription-based software service hosted by Microsoft Corporation within Microsoft managed datacenters. Microsoft 365 services are designed to provide performance, scalability, security, management capabilities, and service levels required for mission-critical applications and systems used by business organizations.

The following services are provided to all Microsoft 365 customers:

- Email access and productivity tools
- Team communication and collaboration
- Document and file storage
- Documents viewed and edited in a Web browser

Although Microsoft 365 uses a limited set of Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services provided by Microsoft Azure (Azure) and Microsoft Datacenters considered subservice organizations within Microsoft. User administrative and compliance experiences are driven exclusively via the Microsoft 365 user interface and do not require independent access to and consumption of Azure user administrative experiences.

Microsoft Datacenters provide hosting and network support solutions for the Microsoft 365 environment. Microsoft Azure provides supporting services for the Microsoft 365 applications including authentication, virtual server hosting, and system data storage.


Microsoft 365 *
Content Management SaaS Applications
SharePoint Online
OneDrive
Microsoft Azure **
+
Microsoft Datacenters
PaaS
IaaS
Development tools, database management, business analytics
Operating systems
Servers and storage
Networking firewalls/security
Data center physical plant/building

Note: *While several applications may be included as part of a customer's Microsoft 365 subscription (i.e. Exchange Online, Skype for Business, Office Online, etc.), the topics discussed in this document focus on the content management functionality within SharePoint Online and OneDrive for Business.*

***Note: Microsoft Datacenters and Azure are treated as subservice organizations and are not within the scope of this document. For information about Microsoft Datacenters and Azure quality management, IT infrastructure qualification, and software development practices, refer to the Microsoft Azure GxP Guidelines (Ref. [14])*

2.1 Establishing trust

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:

Security

Protecting you from cyberthreats

Privacy

Giving you control over access to your data

Compliance

Unparalleled investment in meeting global standards

Microsoft's approach to securing our customers' files involves a security control framework of technologies, operational procedures, and policies that meet the latest global standards and can quickly adapt to security trends and industry-specific needs. Additionally, we provide a set of customer-managed tools that adapt to the organization and its security needs.

Microsoft focuses its investments in the following areas:

1. Platform security
   a. Infrastructure and processes of our datacenters
   b. Strong encryption technologies (at rest and in transit)
2. Secure access and sharing
   a. Restrict access of files to approved people, devices, applications, locations, and data classifications
   b. Enforce who can share files and with whom
3. Awareness and insights
   a. Understanding of how individuals are using SharePoint and OneDrive
   b. Analyze usage to measure return on investment
   c. Identify potentially suspicious activity
4. Information governance
   a. Classify what constitutes sensitive data and enforce how it can be used
   b. Protection in the event of litigation
   c. Retain business-critical files when people leave your organization
5. Compliance and trust
   a. Ensure that service operations are secure, compliant, trustworthy, and transparent

Visit the Trust Center to learn more about what Microsoft is doing to earn our customers' trust.

2.2 Microsoft 365 certifications and attestations

Microsoft 365 services employ a security framework that encompasses industry best practices and spans multiple standards, including the ISO 27000 family, NIST 800-171, and others. As part of our comprehensive compliance offering, Microsoft 365 regularly undergoes independent audits performed by qualified third-party accredited assessors for SOC, ISO, Health Information Trust Alliance (HITRUST) and the US Federal Risk and Authorization Management Program (FedRAMP). 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 assess controls similar to those required to meet regulatory requirements, such as US FDA 21 CFR Part 11 and EudraLex Volume 4 Annex 11.

The following table identifies some of the certifications and attestations that Microsoft 365 has achieved, 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	Auditor
SOC 1 Type II (SSAE 18)	Annually	Deloitte
SOC 2 Type II (SSAE18)	Annually	Deloitte
ISO/IEC 27001:2013	Annually	British Standards Institution (BSI)
ISO/IEC 27017:2015	Annually	British Standards Institution (BSI)
ISO/IEC 27018:2014	Annually	British Standards Institution (BSI)
HITRUST	Annually	Coalfire
FedRAMP (NIST SP 800-53 Rev. 4)	Annually	Coalfire

This guidance document aims to assist in the review of the compliance audit reports by outlining the interconnectivity of Microsoft 365 and its dependency services.

The latest certificates and audit reports are available to customers in the Service Trust Portal (STP). Also available is the **Microsoft 365 Compliance Offerings** document that provides an overview of Microsoft 365 compliance offerings intended to help customers meet their own compliance obligations across regulated industries and markets worldwide.

2.2.1 SOC 1 and SOC 2

Microsoft 365 online services are audited annually 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 different categories such as SOC 1 and SOC 2 which fall in-scope for Microsoft 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 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 Principles (TSP), which are composed of the following five (5) sections:

- The **security** of a service organization's system
- The **availability** of a service organization's system
- The **processing integrity** of a service organization's system
- The **confidentiality** of the information that the service organization's system processes or maintains for user entities
- The **privacy of personal information** that the service organization collects, uses, retains, discloses, and disposes of for user entities

During the SOC examination, the independent auditor performs a variety of verifications 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 “Section V: Supplemental Information Provided by Microsoft.”

The latest SOC 1 and SOC 2 audit reports are available to customers in the Service Trust Portal (STP).

Note: *As presented in a SOC 2 audit report, a positive outcome where all relevant criteria have been achieved is referred to as an "unqualified" opinion. 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 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 Portal (STP).

2.2.3 ISO/IEC 27017:2015

The ISO/IEC 27017:2015 standard is designed for organizations to use as a reference for selecting cloud services information security controls when implementing a cloud computing information security management system based on ISO/IEC 27002:2013. It can also be used by cloud service providers as a guidance document for implementing commonly accepted protection controls.

This international standard provides additional cloud-specific implementation guidance based on ISO/IEC 27002, and provides additional controls to address cloud-specific information security threats and risks referring to clauses 5 to 18 in ISO/IEC 27002: 2013 for controls, implementation guidance, and other information.

The latest ISO/IEC 27017 audit report is available to customers in the Service Trust Portal (STP).

2.2.4 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.

The latest ISO/IEC 27018 report is available to customers in the Service Trust Portal (STP).

2.2.5 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, GDPR, ISO 27001, 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 level that precedes it. An organization with the highest level, CSF-certified, meets all the CSF certification requirements.

Microsoft 365 is certified for the HITRUST CSF.

The latest HITRUST CSF Assessment Report is available to customers in the Service Trust Portal (STP).

Additional Resources:

- HITRUST CSF

2.2.6 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.

Microsoft stands apart from other cloud service providers by making the FedRAMP System Security Plan (SSP) available to all customers in the Service Trust Portal (STP).

Additional Resources:

- Microsoft 365 FedRAMP FAQ

2.3 Microsoft 365 Quality and Secure Development Lifecycle

Microsoft 365 has implemented internal processes and controls to quality principles which are incorporated into the development and operation of Microsoft 365 services. An overview of the relevant internal processes and controls is provided in this section.

2.3.1 Roles and responsibilities

Microsoft personnel responsible for the successful delivery and management of Microsoft 365 services are distributed across several groups that are responsible for service and support. Microsoft 365 Security and Compliance is managed by the Microsoft 365 Security, and Governance, Risk and Compliance (GRC) teams.

Quality responsibilities are embedded into each functional group, overall compliance oversight is managed by the GRC group.

The general responsibilities of each Microsoft 365 service group are as follows:

Access Security Team

- The Access Security Team maintains Active Directory (AD) services, authentication rules and user access.

Change Management Team

- The Change Management Team is comprised of development, testing and project management teams tasked with developing and maintaining Microsoft 365 applications and supporting services.

Backups and Replication Team

- The Backups and Replication Team is responsible for configuring and monitoring the replication of backup of specified internal and customer content.

Security and Availability Monitoring Team

- The Security and Availability Monitoring Team monitors the incidents that affect the security and availability of Microsoft 365 applications and supporting services.

The following are the centralized support teams which provide specialized functions for the Microsoft 365 services:

Enterprise Business Continuity Management (EBCM)

- The Enterprise Business Continuity Management group assists in analyzing continuity and disaster recovery requirements, documenting procedures, and conducting testing of established procedures.

M365 Security

- The M365 Security group manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning.

Governance, Risk, and Compliance (GRC)

- The GRC group identifies, documents, and advises teams in implementing controls to maintain M365's availability and security commitments to its customers.

Identity Management
(also known as Access Control team)

- The Identity Management group operates the IDM tool to provide access control automation for all teams (excluding Microsoft Teams).

Core Services Engineering and Operations (CSEO)

- The CSEO group provides the access control and authentication mechanism for Microsoft Teams via MyAccess.

Azure

- Azure function provides customer authentication infrastructure including Microsoft Online Directory Services, Microsoft Organization ID, and AAD.

Microsoft 365 Remote Access

- The Microsoft 365 Remote Access function provides internal users remote access control and authentication to the M365 environment.

2.3.2 Policies and standard operating procedures

Microsoft 365 adheres to Microsoft Corporation's Security Policy. This policy describes how the efficacy of security controls is evaluated and defines the accountability and responsibility for implementing security controls.

Microsoft 365 has also implemented the Microsoft 365 control framework. The framework uses NIST standard 800-53 for baseline control procedures and additional control measures are implemented to fulfill Microsoft's contractual and regulatory commitments. These activities are implemented by the Microsoft 365 groups responsible for the application and by the supporting service teams; the framework is managed by the Information Risk Management Council (IRMC).

Team-specific standard operating procedures (SOPs) have been developed to provide implementation details for carrying out specific operational tasks required for the management of Microsoft 365 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 "Procedures" section of the SOC 2 report available to customers in the Service Trust Portal (STP).

2.3.3 Microsoft personnel and contractor training

Microsoft has implemented a training program to ensure that personnel and contractors responsible for managing Microsoft 365 services are adequately trained on internal processes and are qualified to perform their job 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 related processes and controls.

2.3.4 Risk Management

The Microsoft 365 Risk Management approach is a combination of various processes and support tools through which Microsoft 365 achieves its compliance and risk management goals. The process focuses on identifying, assessing, and managing Microsoft 365 risks to meet contractual obligations and accreditations, to help prioritize Microsoft 365 trust efforts, to scale with the Microsoft 365 vision, to maintain customer trust, and to gain a competitive edge for Microsoft 365.

The Risk Management methodology has been designed in compliance with NIST SPs 800-30 and 800-37 and comprises the following four phases to accomplish a successful risk management process:

1. **Identify** – Threat, Vulnerability, and Risk identification provides the list of risks which exist in the environment and provides a basis for all other risk management activities
2. **Assess** – The risk assessment considers the potential impact of an information security risk to the business and its likelihood of occurrence; determine appropriate risk treatment plan to reduce risk to a desirable level
3. **Report** – Risk reports provide managers with the data they need to make effective business decisions and to comply with internal policies and industry regulations
4. **Monitor** – Risk groups perform testing and monitoring activities to evaluate whether processes, initiatives, functions, and/or activities are mitigating the risk as designed

An operational enterprise risk assessment of Microsoft 365 is performed on an annual basis by members of Operational Enterprise Risk Management (OERM) team. The Operational Enterprise Risk Management (OERM) Governance Committee includes representatives from the Microsoft 365 Risk Management Office and business leads that serves as their area's primary contact. This review consists of obtaining information from the Microsoft 365 Governance, Risk and Compliance (GRC) Working Group related to updates of the overall environment, as well as a discussion of risk issues identified during the assessment process. This review is documented in a report that is examined and approved by the corporate Vice President of the Office Product Group. The Microsoft 365 Risk Management Office also provides input to the annual report issued to the Microsoft Board of Directors. The assessment's findings are subsequently an input to the Microsoft 365 Planning Process. Additionally, the Microsoft 365 control framework is updated based on the outcome of the Microsoft 365 risk assessment.

2.3.5 Design and development of Microsoft 365 services

While the regulated company is responsible for demonstrating that a GxP regulated application is fit for its intended use, the development activities performed by the application supplier have traditionally been leveraged by the regulated company performing the validation. This model remains valid for cloud-based applications, such as Microsoft 365, that are used to manage regulated content. As a result, the regulated company will likely focus on the processes employed by Microsoft 365 to design and develop a quality product and ensure that these processes align with the regulated company's quality expectations.

Microsoft 365 development activities are aligned with the Microsoft 365 planning process. The vision and strategy for the Microsoft 365 product is defined by senior management annually. The plan is communicated to Microsoft 365 personnel so that it may be incorporated into design considerations in forthcoming product releases. Component planning meetings are held to allow for team leads from development and project management, to communicate their respective teams' commitments to security, availability, processing integrity and confidentiality. These commitments are also incorporated into the design considerations for implementation. The implementation process is carried out by the Microsoft 365 service teams with input from the Microsoft 365 Security team and the Microsoft 365 Governance, Risk and Compliance (GRC) team.

Microsoft's Security Development Lifecycle (SDL) process includes the formulation of development requirements related to security, availability, processing integrity and confidentiality to detect security related software bugs and to implement fixes to these bugs as part of the SDLC process. Moreover, software builds undergo quality and security testing prior to being deployed to pre-productions for integration testing.

Checks and processes exist within the various stages of the engineering release process to increase resiliency against data corruption, including:

- System Design
- Code organization and structure
- Code review
- Unit tests, integration tests, and system tests
- Trip wires tests/gates

Within Microsoft 365 production environments, peer replication between datacenters ensures that there are always multiple live copies of any data. Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer data. Microsoft maintains backups of Microsoft 365 information system documentation (including security-related documentation), using built-in replication in SharePoint Online and our internal code repository tool, Source Depot. System documentation is stored in SharePoint Online, and Source Depot contains system and application images. Both SharePoint Online and Source Depot use versioning and are replicated in near real time.

Microsoft 365 is designed using the principles of defense in depth. Cross-tenant protections are implemented at the application layer to ensure that customers cannot compromise Microsoft 365 applications to gain unauthorized access to the information of other tenants. Protections are also implemented at the network layer to prevent interception of network traffic and resource starvation attacks. Protections are additionally implemented at the operating system layer to prevent side channel attacks.

While Prevent Breach security processes, such as threat modeling, code reviews, and security testing are very useful as part of the Security Development Lifecycle, Assume Breach provides numerous advantages that help account for overall security by exercising and measuring reactive capabilities in the event of a breach. This is accomplished through ongoing war-games exercises and live site penetration testing of our security response plans with the goal of improving our detection and response capability. Microsoft regularly simulates real-world breaches, conducts continuous security monitoring, and practices security incident management to validate and improve the security of Microsoft 365.

On a semi-annual basis, data flow diagrams for each service showing Microsoft 365 system interactions and dependencies are updated by GRC personnel in collaboration with relevant subject matter experts. The diagrams provide Microsoft 365 personnel with system design information and aid in the resolution of issues related to system security, availability, processing integrity, and confidentiality.

2.3.6 Operations management

The ISPE guidance document, *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems* (Ref. [5]), outlines operational processes involved in maintaining the compliance of a computerized system. The following sections provide an overview of the processes implemented by Microsoft 365 to manage operations.

2.3.6.1 Handover

Microsoft 365 maintains multiple pre-production environments in which software testing is performed. These environments are maintained in accordance with the change management process outlined in Section 2.3.6.4 which ensures that relevant stakeholders are involved in the process and that these are implemented in a controlled manner. Three types of pre-production environments are available for testing purposes which are differentiated by the stakeholders who are granted access to them.

The different environment types are:

- DogFood: The work stream’s initial test environment in which select Microsoft employees and authorized customers test changes.
- MSIT: The release is tested by a larger subset of Microsoft employees within this environment.
- Slice in Production ("SIP"): The release is made available to targeted customers who provide feedback (approximately 5% of worldwide customers are enrolled).

2.3.6.2 Service management and performance monitoring

Microsoft continuously monitors and explicitly tests for weaknesses and vulnerabilities in tenant boundaries, including monitoring for intrusion, permission violation attempts, and resource starvation. We also use multiple internal systems to continuously monitor for inappropriate resource utilization, which if detected, triggers built-in throttling.

Microsoft 365 has internal monitoring systems that continuously monitor for any failure and drive automated recovery when failure is detected. Microsoft 365 systems analyze deviations in service behavior and initiate self-healing processes that are built into the system. Microsoft 365 also uses outside-in monitoring in which monitoring is performed from multiple locations both from trusted third-party services (for independent SLA verification) and our own datacenters to raise alerts. For diagnostics, we have extensive logging, auditing, and tracing. Granular tracing and monitoring helps us isolate issues and perform fast and effective root cause analysis.

Microsoft 365 utilizes monitoring tools to evaluate the status of services and provide automatic notifications of issues to technical personnel. Additionally, technical resources are available 24 hours a day, seven days a week to monitor the system and resolve issues. Microsoft’s Datacenters’ Global Networking Services (GNS) monitor network devices to detect and resolve issues and anomalies.

Monitoring activities focus on capacity, resiliency and availability. Reporting is then made available to Microsoft 365 senior management to allow for the review of the system's health.

Customer support is available to Microsoft 365 customers via the online customer portal and the customer service phone number.

2.3.6.3 Incident management

Incident response procedures are established to govern the detection, resolution and prevention of security incidents. The Security Incident Response (SIR) team is responsible for managing security logs created by monitoring tools to identify and resolve incidents. Incidents are captured and tracked via an incident tracking system.

A risk-based approach is used to prioritize reported incidents and processes are in place to govern the escalation of incidents deemed severe and/or high priority to appropriate stakeholders. Contingency plans are implemented when applicable based on the incident priority.

The Microsoft 365 Security team and the service teams work together on and take the same approach to security incidents, which is based on the NIST 800-61 response management phases:

- **Preparation** — Refers to the organizational preparation that is needed to be able to respond, including tools, processes, competencies, and readiness.
- **Detection & Analysis** — Refers to the activity to detect a security incident in a production environment and to analyze all events to confirm the authenticity of the security incident.
- **Containment, Eradication, Remediation** — Refers to the required and appropriate actions taken to contain the security incident based on the analysis done in the previous phase. Additional analysis may also be necessary in this phase to fully remediate the security incident.
- **Post-Incident Activity** — Refers to the post-mortem analysis performed after the remediation of a security incident. The operational actions performed during the process are reviewed to determine if any changes need to be made in the Preparation or Detection & Analysis phases

2.3.6.4 Change management

A change management process has been implemented to document and track system changes and software releases. Procedures have been established to govern the implementation of changes. The Change Management process is documented and tracked via ticketing systems. Within the ticketing systems, the key stakeholders for a given change are identified to ensure that changes are approved prior to implementation in the production environment. Moreover, testing is performed, and the test results are approved by stakeholders before releasing the change for implementation.

The Change Management process employs a risk-based approach to the implementation of proposed changes based on the type of change and its potential impact. The following change categories have been defined:

- **Auto-approval** — A set of preapproved low-risk standard changes
- **Functional (Peer) Approval** — Standard changes with a slightly higher level of risk
- **Change Advisory Board Approval** — Changes with the potential for high risk and high impact

- **Emergency Change Advisory Board Approval** — A risk that must be remediated timely, such as an out of-band security patch

The Change Advisory Board (CAB) and its members are chartered to formally "Approve" or "Deny" all changes prior to implementation. Configuration and code changes follow a common system development process which includes provisions for oversight and approval. The CAB convenes as needed to support changes to the environment.

If a quorum for the CAB exists, the change process begins with a Request for Change (RFC), which documents:

- What is being changed
- Where the change is to be implemented
- Why the change is needed
- Change deployment steps
- What is the impact of doing and not doing the requested change
- Change mitigation
- When is the change desired to be implemented
- Change rollback criteria and instructions

The ticketing tool or source control retain an audit history, showing what actions were taken and by whom, including approvals. Microsoft 365 service teams review the audit history as required by investigations and during annual independent security assessments.

Hardware and network changes, as well as configuration management are governed by processes outlined in the Microsoft Azure GxP guidelines (Ref. [14]).

2.3.6.5 Audits and review

Microsoft's Internal Audit (IA) function performs audits to independently review current processes. These audits assess whether management objectives are being met and provide a forum to propose process improvements.

The auditors communicate issues and recommendations for improvements to management and to the Audit Committee, the group to whom the auditors directly report. IA representatives perform periodic risk assessments; the outcomes of these assessments are reviewed by senior management.

Risk mitigation strategies and controls are reviewed on a periodic basis by individuals assigned the task of tracking implementing these controls.

2.3.6.6 Continuity management

2.3.6.6.1 Backup and restore

Procedures are in place to govern backup and restoration processes. Microsoft 365 customer content data is backed up via the Azure Blob Storage backup process, performed periodically. The backup process complements the content replication and geographical redundancies performed on customer data in accordance with Service Level Agreement (SLA) requirements.

Three types of backups have been implemented. These backup types are differentiated by the frequency at which they are performed, as described below.

- **Full backups** — All customer content data within a server or a content database is backed on a weekly basis and maintained for 30 days.
- **Differential Backups** — Additional data generated since the last full back-up or the last differential backup is backed up daily.
- **Transaction-Log Backups** — Occurring every 5 minutes, additional data generated within a 5-minute interval is backed up.

Customer content data is restored when requested by a customer in accordance with the SLA terms.

2.3.6.6.2 Business continuity/ disaster recovery planning

Microsoft 365's Business Continuity and Disaster Recovery Planning sets recovery time objectives to be met in the event of an unforeseen incident affecting the system. The recovery time objectives are testing by conducting failover exercises to verify the ability to recover the system within the targeted timeframe. The frequency at which failover exercises are performed are set based a determination of system criticality. Any issues detected as part of failover exercises are tracked and resolved.

The Enterprise Business Continuity Management support team assists Microsoft 365 teams in establishing and evaluating disaster recovery requirements and testing these requirements in accordance with applicable procedures.

Microsoft corporate has established an RTO for Office Services Infrastructure and the infrastructure team has a mitigation goal in which they mitigate the issue within the Office Services Infrastructure service itself within the mitigation window.

A disaster recover standard operating procedure exists, which includes a keystroke-level guide for rapid restoration of computing resources in the event of a datacenter level outage. The process describes how to re-route traffic to another datacenter (which has replicated data) to maintain operations in the short-term, while the original datacenter can be brought back online.

2.3.6.7 Security and system administration

The Microsoft 365 Information Security Policy provides the overarching security guidance for Microsoft 365. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Microsoft 365. The Security Policy covers the following topics according to the Microsoft 365 SOC 2 reporting:

- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Systems acquisitions, development and maintenance
- Supplier relationships
- Information security incident management
- Business continuity management

- Compliance

Protection mechanisms have been implemented to prevent the introduction of malware (viruses) into Microsoft 365. Anti-malware software detects and prevents various types of malicious software, including computer viruses, malware and worms. The software scans the environment and files at a predefined frequency and blocks any malicious software that is detected. The software also alerts relevant stakeholders who initiate the incident response process discussed in Section 2.3.6.3.

Microsoft 365 has implemented a server build-out process to deploy and configure new servers. The process is also used to rebuild existing servers. This process includes the installation of anti-malware signature files and definitions and it incorporates quality assurance reviews to ensure verify that the build-out process was successfully completed. Portions of SharePoint Online and OneDrive for Business services utilize Microsoft's Azure PaaS offerings for server build-out and management. Network management activities are governed by processes outlined in the Microsoft Azure GxP Guidelines (Ref. [14]).

Microsoft 365 environments rely on Active Directory (AD) infrastructure which provides centralized authentication and authorization for user access management. Identity manager tools are employed by the Identity Management team to manage Microsoft 365 user identities and credentials.

Requests to grant access to new users or to modify access granted to existing users is subject to management approval. The submission and approval of these requests is performed using an identify manager tool. The tool is also used to periodically review user access to detect inactive or expired accounts. When an employee leaves the company, Microsoft HR is responsible for initiating the process to terminate the employee’s access.

2.3.6.7.1 Security audit logs

The Microsoft 365 Security team has developed a general set of auditable events specific to the Microsoft 365 Support based on ongoing risk assessments of the system which incorporate identified vulnerabilities, business requirements, and Microsoft 365 Security standards. The Microsoft 365 Security team specifies each event that must be audited for all servers. The list of auditable events is maintained and reviewed at least annually by Microsoft 365 Security team. For application-specific events, reviews and updates are considered at service reviews, or in the planning phases of feature milestones.

Microsoft 365 generates audit records containing sufficient information to establish the type of event that occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any user/subject associated with the event. These events include:

- Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)
- Successful and unsuccessful logon attempts
- Privileged activities or other system level access
- Starting and ending time for user access to the system
- Concurrent logons from different workstations

- Successful and unsuccessful accesses to objects
- All program initiations
- All direct access to the information system
- All account creations, modifications, disabling, and terminations

2.3.6.8 Records management

Microsoft has implemented a documentation and records management procedure governs that complete lifecycle of system documents, from creation to approval, distribution, and withdrawal.

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.

Microsoft 365 information system documentation (including security-related documentation), is maintained in SharePoint Online and our internal code repository tool, Source Depot. Both SharePoint Online and Source Depot use versioning and are replicated in near real-time.

Access to system documentation is restricted to the respective Microsoft 365 teams based on their job roles. Documents are subject to levels of protection that are appropriate to their classification level.

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 processes, as well by external third-party auditors during the SOC audit and ISO certification processes.

3 Recommendations for implementing a Microsoft 365 GxP compliance framework

Achieving a compliant cloud-based solution requires well-defined controls and processes, with shared responsibilities between Microsoft and our customers. Microsoft has implemented a series of technical and procedural controls to help ensure the dependability (availability, reliability, security, integrity, accessibility, and maintainability) of Microsoft 365.

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 Microsoft 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 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 globe have published guidance documents related to this topic:

- U.S. 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 (Draft – August 2016)

Various GxP regulations, such as 21 CFR Part 11, 21 CFR Part 211, 21 CFR Part 212, EMA 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.

The integrity of customer data within Microsoft 365 is protected by a variety of technologies and processes. For example, Microsoft embeds advanced cryptographic technologies within Microsoft 365 to ensure data in transit and at rest is encrypted. 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 Microsoft 365.

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 customer is responsible for authorizing access, managing data governance and configuring settings related data integrity. The follow table describes the shared responsibilities between Microsoft 365 and the GxP customer as it relates to data integrity.

Entity	Data Integrity Responsibilities
GxP regulated customer	✓ Properly authorize users who are granted access to the resources and monitor continued appropriateness of access ✓ Configure and monitor Microsoft 365 audit log ✓ Enable library versioning settings as required ✓ Define data classification and retention rules ✓ Configure information rights management ✓ Enforce desired level of encryption for network sessions ✓ Establish proper controls over the use of system IDs and passwords ✓ Manage user password authentication mechanism ✓ Manage anonymous access and external sharing ✓ Secure the software and hardware used to access Microsoft 365 ✓ Conduct end-user training

	✓ Report any identified security, availability, processing integrity, and confidentiality issues ✓ Understand and adhere to the contents of service contracts, including commitments related to system security, availability, processing integrity, and confidentiality ✓ Manage Microsoft 365 data inputs, processing, storage and outputs for completeness, accuracy, and timeliness ✓ When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content and approving appropriate requests in a timely manner ✓ Establish the necessary configuration to support the regulated user's GxP processes in accordance with user and regulatory requirements ✓ Perform validation testing to demonstrate that the system is fit for its intended use
Microsoft 365	✓ Implement BitLocker disk-level encryption and per-file encryption of data at rest ✓ Implement transport Layer Security (TLS) encryption of data in transit ✓ Ensure tenant data isolation and logical segregation ✓ Review and analyze system level audit logs for indications of inappropriate or unusual activity, including indications of compromise ✓ Perform Microsoft 365 patch management ✓ Implement and manage data resiliency controls, including: o Data backup o RAID 10 disk mirroring and striping o SQL Database synchronous mirroring and asynchronous log shipping ✓ Perform routine logical security activities: o Update anti-malware software on Microsoft 365 servers o Port scanning and remediation o Perimeter vulnerability scanning o Operating system security patching o Network-level distributed denial-of-service (DDoS) detection and prevention ✓ Manage and maintain physical data center security and environmental controls ✓ Follow industry best practices for security, software development and system maintenance, including: o System Design o Code organization and structure o Code review o Unit tests, integration tests, and system tests o Trip wires tests/gates ✓ Perform documented testing to ensure conformance with system specifications

These activities combined with the Microsoft 365 technical capabilities described in the following sections combine to provide a foundation for control of data integrity, privacy, and security. Together with a well-defined computer system validation program, life sciences customers can demonstrate their GxP content is managed within Microsoft 365 with proper data integrity controls.

Additional Resources:

- ISPE, GAMP Good Practice Guide: Records & Data Integrity

3.1.1 Key Microsoft 365 features supporting data integrity

The following sections highlight various key features and capabilities of the Microsoft 365 platform that can be used by life science customers to help ensure integrity of their data.

3.1.1.1 Sensitivity labels

Microsoft 365 empowers people to collaborate on GxP documents and within their lifecycles, this can mean content transiting to and from external sources and collaborators in different systems. Content that leaves its home in the cloud can stress the control and security of the content.

Microsoft 365 has many features to help maintain this control in immediate and extended areas of collaboration, and one of them is *Sensitivity Labels* for global (public) cloud tenants.

Sensitivity Labels are part of the Microsoft Information Protection framework and they enable email and document-level classification, encryption, integrity and data-loss protection online by leveraging overarching safeguards like those from Azure Information Protection, Azure Rights Management, Intune, Cloud App Security and policies in Azure Portal. Once applied, Sensitivity Labels become integral to the document and persist as the document transits between people and environments. Sensitivity Labels can also be used to:

- Enforce protection settings through encryption, marks and data-loss prevention.
- Protect content across Microsoft 365 applications on different platforms.
- Prevent sensitive content from leaving an organization on devices running Windows using endpoint protection in Microsoft Intune. This prevents content from entering transit into other third-party applications, or removable storage.
- Content can be protected in third-party applications and services, even if they don't support Sensitivity Labels.
- Classify content by customizing the Sensitivity Labels into priorities, categories, and groups thereof (via sub-labels).
- Further protect content offline with temporary licenses.

Life sciences organizations that enable Sensitivity Labels for Office files in SharePoint Online and OneDrive may use them within their SharePoint Libraries and document storage spaces. Once a Library has been configured for highly confidential protection, Sensitivity Labels become available for automatic application to documents that enter the library, or as a manual application once the document is opened. The encryption and permissions will travel with documents even when downloaded.

Microsoft Information Rights Management can be leveraged to configure a Sensitivity Label to encrypt documents once applied to limit the access of the document to its owner, and co-authors can be configured for collaboration.

External users can become co-authors on documents with Sensitivity Labels that have been configured for encryption if they are given an Azure Active Directory account, as single users, or as members of an organization or Microsoft 365 group.

3.1.1.2 Retention labels

21 CFR Part 11 and Annex 11 require that records are protected, accurate and ready for retrieval throughout the records' retention period.

Microsoft 365 enables the application of ***Retention Labels*** for the purpose of declaring documents as records, enforcing retention polices and protections. Retention labels utilize Retention Policies that can be published to make labels available in specific locations (e.g. to items as an explicit label, and to libraries as a default label. Once a label is applied on content, the content will be automatically managed in accordance with the retention rules defined for that label.

In SharePoint Online, libraries and folders can be configured to automatically apply retention labels so that any document that enters the library or folder, is automatically labeled for retention; as a record.

Alternately, overarching Retention Policies can be defined (in the Microsoft 365 Security & Compliance Center) to apply a blanket retention rule on all contents of a specified SharePoint site.

3.1.1.3 Overarching site retention policies

Microsoft 365 offers a retention system known as Retention Policies. They exist to gather and preserve data from different content hierarchies in an overarching way, with or without direct user participation. Content that is required to be preserved is kept in a Preservation Hold Library where it cannot be deleted or altered in any way throughout its retention period. Retention Policies can be designed to cover a broad range of scenarios from specific types of data, to libraries and entire sites across a tenant.

If a more granular or manual approach is needed, a Retention Label can be defined that needs to be applied first, either automatically or manually.

A hierarchy of rules exists to help businesses manage the implementation of retention from policies to labels.

3.1.1.4 Record metadata

The metadata pertaining to creation of a record (by applying a retention label), i.e., time of applying the label and identifying the user performing the action is recorded by SharePoint Online as corresponding metadata entries in the 'Retention label applied' and 'Label applied by' columns of the source library. The metadata entries are not editable and remain linked to the record.

The metadata pertaining to modification of a record (by unlocking a labeled record a true copy of the latest version of the record is sent to the Preservation Hold Library), i.e., time of unlocking a labeled record and the user performing the action is recorded by SharePoint Online as metadata entries in the 'Preserved Date' and 'Modified By' columns of the Preservation Hold Library, corresponding to the copy of the latest version of the record. The copies of records in the Preservation Hold Library and related metadata cannot be edited or deleted throughout the retention period of the record.

3.1.1.5 Audit Log

As described in Section 2.3.6.7.1, Microsoft has implemented internal security controls to audit key events performed by Microsoft 365 internal teams responsible for managing and maintaining the Microsoft 365 environment.

The Audit Log feature in the Microsoft 365 Security & Compliance Center captures the complete history of activities performed on documents stored within SharePoint Online. The feature provides an audit log that records events such as when content is created, viewed, modified, and deleted. The audit log includes the username of the user who performed the associated action and the time and date when the event occurred.

Audit log entries are read-only (i.e. not alterable by end-users) and are stored in a secure database.

Depending on the license type, audit log retention policies can be defined to retain entries from the Audit Log for 90 days or for up to one year. When longer retention periods are required, audit log data can be extracted periodically using PowerShell or preferably using the Microsoft 365 Management API. The extracted audit log can be labeled a ‘record’ with retention labels to prevent alteration by end users. Audit log data can also be exported from the system and viewed in Microsoft Office Excel.

Customers can also use the Retention label and policy capabilities together with the Preservation hold library as a means of satisfying audit trail requirements for GxP records. If a retention label is used to label a document as a record, then every time a record is unlocked, a true copy of the latest version of the record is sent to the Preservation Hold Library. Every such version is stored as a separate file, along with its associated metadata, in the Preservation Hold Library and cannot be edited or deleted throughout its retention period.

3.1.1.6 Versioning

The versioning feature tracks and manages changes to documents and data over time in SharePoint lists and libraries. When enabled, new versions are added to an item's version history after changes are saved. The number of versions stored and the visibility of draft or minor versions can be configured for each list and library. Life sciences customer can use this feature to view and recover previous versions from the item's version history. This can be especially useful in under the following circumstances:

- Need to track history of changes made to a document throughout its lifecycle
- Need to restore a previous version due to an inadvertent document modification or document corruption
- Need to view and compare versions of documents without overwriting the current version

3.1.1.7 Library restore

Data recovery is essential for any system that manages GxP data. With cloud-based solutions, a special focus must be paid to the movement of data as it changes state, which includes that of intentional or accidental deletion. Solutions exist at the granular document level (like with version control), and also at the structural level, like that with document libraries.

The Restore this library feature of the modern experience SharePoint Online in Microsoft 365 exists to restore several documents within a library with the least amount of effort in situations of deletion, corruption or infection by malware.

Restore this library leverages the Recycle bin of SharePoint Online and version control so that full libraries, or its parts, can be restored to any day in the past 30 days of the library's history. When greater control is needed, selected individual or groups of activities can be reversed. If version control was enabled for the library, restoration activity can even be applied to the historical past of particular documents.

3.1.1.8 Site Designs and Site Scripts

Site designs and site scripts can be used to automate provisioning of new or existing modern SharePoint sites that use custom configurations. Site designs are like a template that provide reusable lists, columns, themes, layouts, pages, and custom actions, which can be used each time a new site is created and can also be applied to existing modern sites. Life sciences customers can use the site design functionality to apply a consistent and controlled configuration to each site used to support a controlled GxP business process.

3.1.1.9 Power Automate

Power Automate is a cloud-based workflow tool that is integrated with Microsoft 365 / SharePoint Online. It is used to automate repetitive tasks and as a business process automation tool and can be used to automate GxP processes where specific sequencing of events or activities are required.

One of the primary reasons life science organizations are using automated workflows to support GxP processes is to increase control and efficiency of GxP business processes and help manage the lifecycle of GxP records. With this comes the following ancillary benefits:

- Optimizes the creation of GxP records by allowing users to collaborate simultaneously while maintaining control over the record source
- Ensures business processes are followed in controlled and consistent manner
- Reduces human error by automating repetitive tasks
- Can be adapted as business needs change
- Leverages built-in capabilities of the Microsoft 365 platform to minimize costs and risks associated with system changes

The following table highlights some of the key functionality of Microsoft 365 / SharePoint Online which can be automated using Power Automate to support a variety of GxP processes.

Microsoft 365 Feature	How Power Automate can be used
User account creation in Azure AD	➔ Use Power Automate to manage the on-boarding/off-boarding process of employees and guest users
Sharing of content and permissions management	➔ Use Power Automate to control which content can be shared and the permissions granted to the content (Read/Contribute)

Document filing and metadata control	➔ Use Power Automate to move documents between designated libraries/folders and update document metadata throughout the document lifecycle process
Record protection and retention	➔ Use Power Automate to automatically set a retention label on a record rather than having to rely on the end-user to manually set it
Self-service site creation	➔ Use Power Automate to provision sites with predefined structures including libraries, lists, columns, content types, views and security groups, etc.

Life science organizations are encouraged to establish good design and governance practices to ensure their Power Automate workflows are design and maintained in controlled manner. These practices include the following:

- ✓ Establish good workflow design practices to ensure quality and consistency in terms of design and naming conventions
- ✓ GxP Power Automate workflows should be tested before using them in a production context
- ✓ When using multiple environment (e.g. development, test, staging, etc.) a process should be defined for packaging Power Automate workflows and moving them from one environment to another
- ✓ Implement procedures for monitoring, administering and making changes to GxP Power Automate workflows
- ✓ Ensure only authorized individual can make changes to GxP Power Automate workflows
- ✓ Ensure proper training and qualification of individuals involved in the development and administration of GxP Power Automate workflows
- ✓ Implement controlled processes to manage the versioning and backup of GxP Power Automate workflows
- ✓ Perform periodic reviews to ensure the change management process has been followed and that GxP Power Automate workflows remain in a validated state

3.1.1.10 Microsoft Compliance Score

Microsoft Compliance Score is a risk-based assessment tool, available to Microsoft 365 customers can be used for managing regulatory compliance within the shared responsibility model for Microsoft cloud services. Microsoft Compliance Score includes a dashboard that provides a summary of customer data protection and recommendations to improve data protection and compliance. Life sciences customers can use this feature to evaluate the effectiveness of these recommendations in their respective regulatory environments by creating an assessment template for applicable GxP regulations.

Note: *Recommendations found in Compliance Score should not be interpreted as a guarantee of compliance.*

3.1.2 Considerations for FDA 21 CFR Part 11 compliance

An application that supports GxP processes subject to FDA regulations should be assessed to determine 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 the risks associated with its intended use should determine the degree to which application is validated to ensure it can satisfy regulatory requirements and is fit for its intended use.

As a SaaS solution provider, Microsoft is responsible for protecting our customer's data and ensuring the quality of our software solutions and services. As a regulated user, our customers are responsible for configuring available features and functional capabilities to address business and regulatory requirements.

The following table highlights some of the Microsoft 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.

Regulatory requirements pertaining to electronic records	*Microsoft 365 records management features and capabilities
Generation of accurate and complete copies of records (that is, data and associated metadata) in both human readable and electronic form.	• Records may be copied from SharePoint using the built-in "Download" feature or by opening the library with Windows Explorer. • Associated metadata stored within library columns can be copied using the "Export to Excel" feature. • Additional metadata, such as the audit trail log can be copied from SharePoint by accessing the site audit report (provided in Excel) or via the Microsoft 365 Unified Audit Log using the "Export results" feature within the Security & Compliance Center.
Protection of records to enable their accurate and ready retrieval throughout the records retention period.	• Microsoft 365 record label functionality provides the ability to apply retention policies to protect records from modification or deletion throughout the record retention period. • SharePoint Version History capability provides the ability to view and restore previous versions of a record. • Microsoft Information Protection framework that allows Sensitivity Labels to be applied to email and documents in Microsoft 365 applications, Windows systems and SharePoint Online to classify, encrypt, rights manage and protect the content of individual pieces of information from loss and unauthorized access within.

Regulatory requirements pertaining to electronic records	*Microsoft 365 records management features and capabilities
User access controls to limit system access to authorized individuals.	• Microsoft 365 uses Azure Active Directory (Azure AD) to manage users and limit access to authorized individuals. With Azure AD, administrators can manage users and groups, enforce strong passwords, set up multi-factor authentication, and enable conditional access. • Microsoft 365 also allows integration with an on-premises Active Directory or other directory stores and identity systems such as Active Directory Federation Services (ADFS) or third-party secure token systems (STSs) to enable secure, token-based authentication to services. • Information Rights Management (IRM) and Azure Rights Management (RMS) features provide the ability to limit access to individual records.
Secure, computer-generated, time-stamped audit trails to independently record the date and time of user actions that create, modify, or delete electronic records.	• SharePoint automatically captures the name of the user and the data and time when a document is created or modified which can be displayed as metadata on each document. • Document libraries can be configured to capture each version of a document. • The Preservation Hold library can be configured to capture each version of a document record, along with its associated metadata. • Audit log functionality can be configured to monitor user actions within Microsoft 365.
Enforcement of permitted sequencing of steps and events (as necessary)	• Workflows can be created using SharePoint workflow or Power Automate (Formerly Flow) to automate various business process and enforce the permitted sequencing of steps as required.
Authority checks to ensure that only authorized individuals can use the system to perform permitted activities	• SharePoint security groups and user permissions can be specified to ensure users can only perform permitted activities based on their role or job function.
Data input validity verification (as necessary)	• Azure Active Directory Conditional Access provides the ability to establish device-based conditional access policies as required.

*__Note__: Some features/services may only be available for specific Microsoft 365 subscription plans. Customers are encouraged to select the appropriate plan that is tailored to their specific needs.

3.2 Microsoft 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 Microsoft 365:

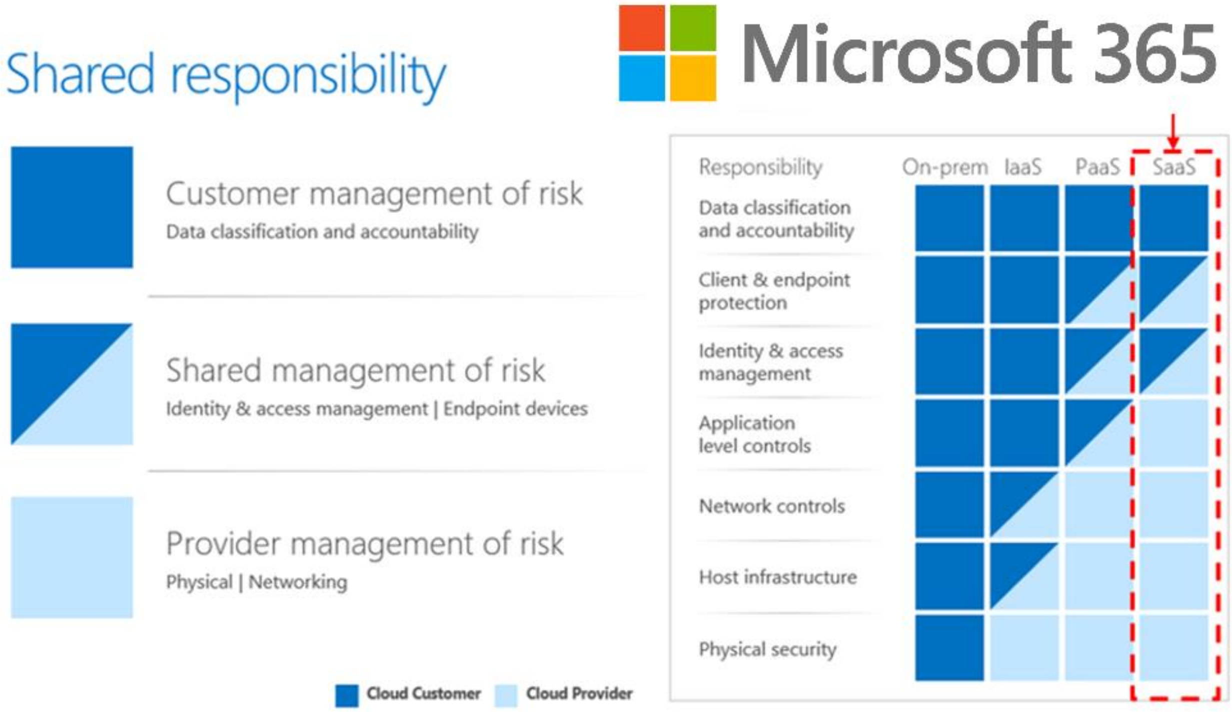
- Identify roles and responsibilities for ensuring data integrity based on the shared responsibility model
- Train personnel responsible for using and administering Microsoft 365
- Review and ensure adherence with service agreements
- Perform routine monitoring and evaluation of Microsoft 365 service 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 governance and compliance strategy to help Microsoft life sciences customers manage their GxP content in a compliant manner when using Microsoft 365. The proposed methodology is based upon proven practices used by Microsoft 365 customers and partners in life sciences.

3.2.1 Shared responsibilities

Due to the nature of the cloud environment, there is a shift in certain responsibilities that deal with the management of the underlying cloud infrastructure and software. While implementing the governance strategy, it is essential to understand how different cloud service models affect the ways responsibilities are shared between customer and the cloud service provider.

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



Shared responsibility

■ Customer management of risk
Data classification and accountability

◩ Shared management of risk
Identity & access management | Endpoint devices

□ Provider management of risk
Physical | Networking

■ Cloud Customer □ Cloud Provider

Microsoft 365

Responsibility	On-prem	IaaS	PaaS	SaaS
Data classification and accountability	■	■	■	■
Client & endpoint protection	■	■	◩	◩
Identity & access management	■	■	◩	◩
Application level controls	■	■	◩	□
Network controls	■	◩	□	□
Host infrastructure	■	◩	□	□
Physical security	■	□	□	□

Microsoft 365 is delivered as a SaaS solution where customers are responsible for establishing proper data classification, governance and rights management, managing client endpoints, as well as account and access management. Microsoft is responsible for all aspects surrounding physical infrastructure, network and application level controls, and shares responsibilities with respect to identity and access managing, as well and client and endpoint protection.

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, as well as the ISPE GAMP Good Practice Guide, *IT Infrastructure Control and Compliance* (Ref. [6]).

Microsoft 365 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 ISPE GAMP Good Practice Guide (Ref. [6]).

3.2.2.1 Service level agreements

Microsoft 365 service is 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 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 Online Services Terms 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.

Microsoft 365 support plans including Premier Support for Microsoft 365 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 ✓ Training management ✓ Documentation management ✓ Records lifecycle management ✓ Supplier management ✓ Periodic review	✓ Application security ✓ System administration and user access management ✓ Change management ✓ System configuration management ✓ Data backup and recovery ✓ 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 the Microsoft 365 applications. Additional training requirements may need to be defined for each controlled Microsoft 365 application.

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

Microsoft 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 Microsoft 365 engineering teams.

Additional Resources:

- Microsoft Virtual Academy – Microsoft Azure Courses
- Microsoft 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 and 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.

Microsoft 365 provides advanced data governance capabilities, including the ability to apply retention labels and policies to content. With labels, customer can classify data across organization for governance, and enforce retention rules based on that classification. With retention policies, customers can retain content so that it can't be permanently deleted before the end of the retention period. The retention period can be based on when the content was created, last modified, the label was applied or when specific type of event has occurred.

Customers are responsible for determining their recordkeeping requirements based on internal policies and regulatory requirements. Customer data stored within the customer's Microsoft 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 Terms (OST) agreement. Microsoft commitments regarding the protection of customer data retained within the Microsoft 365 platform are also described in the OST.

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" (Ref. [12]):

> *"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, Microsoft 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 Microsoft 365 has implemented. The analysis also maps to a specific control ID as referenced within the latest SOC 2 report for Microsoft 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 Microsoft 365 admin console 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. Microsoft 365 includes a security model that enables separation of administration based on roles. Customers can configure Azure Active Directory (AAD) and role-based access control (RBAC) to facilitate segregation of duties and least privilege.

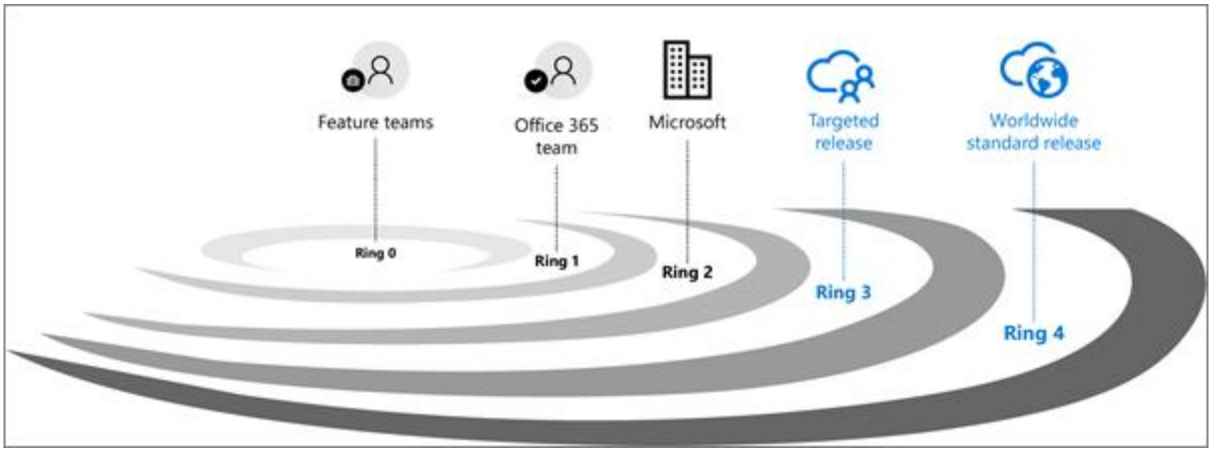
Customers should develop a permissions strategy to keep the environment manageable and secure. An effective permissions strategy will enhance the manageability and performance of the system, ensure compliance with the organization’s data governance policies, and minimize the cost of maintenance.

3.2.3.2.3 Change management

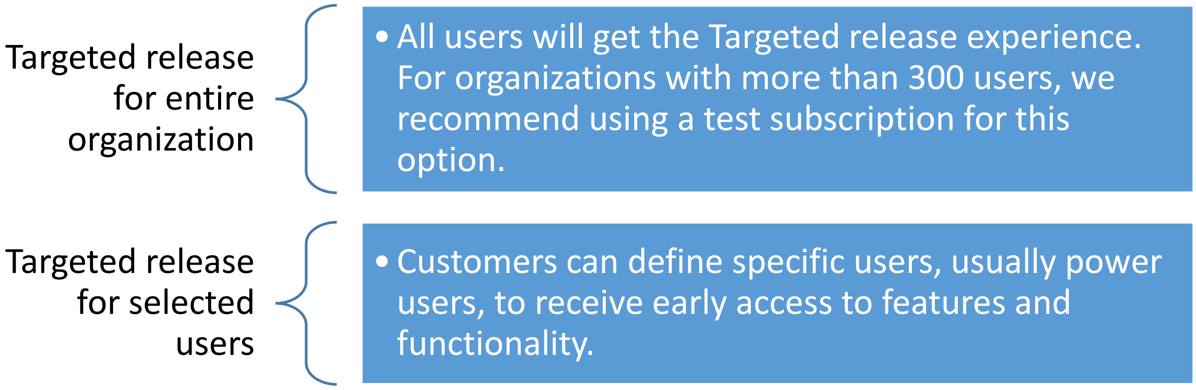
A formal process should be in place for change management that will ensure that application changes are implemented in a controlled manner. This process must also establish the framework for proposing, reviewing, and approving changes to a system.

As part of their Microsoft 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.

Microsoft engineering teams have implemented robust processes around change management as it relates to implementing software, hardware, and network changes. Any new release is first tested and validated by the feature team, then by the entire Microsoft 365 feature team, followed by entire Microsoft. After internal testing and validation, the next step is a Targeted release (formerly known as First release) to customers who have selected to opt in. At each release ring, Microsoft collects feedback and further validates quality by monitoring key usage metrics. This series of progressive validation is in place to make sure the worldwide-release is as robust as possible. The releases are pictured in the following figure:



Customers can choose whether the targeted release will be applied for the entire organization or for selected users.



Targeted release for entire organization

- All users will get the Targeted release experience. For organizations with more than 300 users, we recommend using a test subscription for this option.

Targeted release for selected users

- Customers can define specific users, usually power users, to receive early access to features and functionality.

Targeted release allows administrators, change managers, or anyone else responsible for Microsoft 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.

Customers who need to develop and test Microsoft 365 solutions in a separate environment can use the Microsoft 365 Developer Program to create a sandbox subscription. This environment can be set to receive updates on the targeted release ring, allowing users to test certain new features prior to them being released on the standard release ring.

For significant updates, Office customers are initially notified of upcoming changes by the Microsoft 365 public roadmap. As an update gets closer to rolling out, it is communicated through the Microsoft 365 Message Center. 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.

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 Microsoft 365 Portal provides the ability to administer the configuration of certain settings within a customer’s Microsoft 365 subscription. Additional content management configuration settings are available within SharePoint Online site settings. Information about the configuration settings, can be viewed within the portal. Alternatively, customers may create automated scripts to manage the configuration of Microsoft 365 resources using the Microsoft 365 PowerShell.

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 Microsoft 365 and can use the best practices described below to select the appropriate process for each situation.

For the daily use of SharePoint Online, three main functions have an impact on the backup and restore abilities of SharePoint: **User Level Recycle Bin**, **Site Collection Recycle Bin**, and **Version Control**.

First, is the **User Level Recycle Bin**. This recycle bin catches all the files a user deletes and retains them for a default time of 90 days. When a user deletes a file in his recycle bin, it goes to the Site collection Recycle bin.

Next and at a higher level, we have the **Site Collection Recycle Bin**, or the *second stage recycle bin*. The Site Collection Recycle Bin holds all the files that users delete from their recycle bin for the remaining of the 90 days. This recycle bin also holds the Sites and Libraries that administrators have deleted. Sites and files can be recovered through the SharePoint Online Administration center recycle bin page.

When the modern experience of SharePoint Online is available, Libraries can be restored specifically using the *Restore this library* feature within SharePoint Settings.

Third, an essential feature of SharePoint Online is the ability to apply **Version Control** within document libraries. Version Control provides the ability to view and restore a previous version of a document. This is not a default option and should be configured in the repository. With version control enabled, the *Restore this library* feature becomes capable of utilizing version control to further empower its restoration capabilities.

SharePoint Online uses a hot standby system that includes paired geographically separate datacenters within the same customer data location region configured as active/active. The SharePoint Online team conducts weekly full backups and backs up the transaction logs every 5 minutes (see **Section 2.3.6.6** for additional details). In the unlikely event that a complete recovery from backup is required, customers can contact Microsoft support personnel to request recovery from backup.

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 Microsoft 365 platform as part of their operations and maintenance strategy.

The Microsoft 365 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 Microsoft 365 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.

Support tickets can be raised with Microsoft support personnel directly within the Microsoft 365 portal which provides an efficient way of communicating and tracking the status of an incident until it is resolved.

3.3 GxP Use Cases

As a highly configurable content management platform, Microsoft 365 may be configured to support a wide range GxP activities. Many of these use cases will result in the generation of electronic records which the customer may choose to manage within Microsoft 365. Some examples of these types of GxP records include:

- Standard Operating Procedures (SOPs)
- Training records
- Clinical trial documents (eTMF)
- Incident and CAPA records
- Change control records
- System specifications (User Requirements, Functional/Configuration/Design Specifications, etc.)
- Validation documents (Validation Plan, Validation Protocol, Test Scripts, Validation Summary Report, etc.)

3.4 Considerations for implementing a risk-based validation strategy

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.

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]

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

[1] ISPE, GAMP Good Practice Guide: IT Infrastructure Control and Compliance (Ref. [6])

Section 2.2, help to ensure the people, processes, and technology that make up the Microsoft 365 operating environment work together to maintain a state of control and compliance.

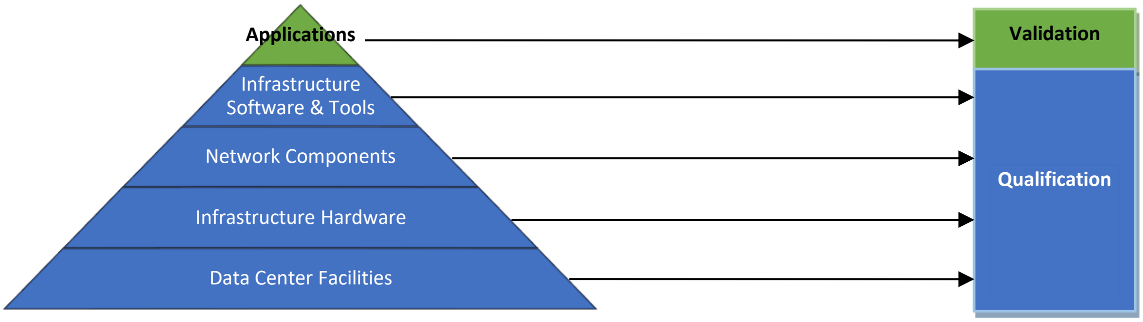


Figure 1 – Qualification of Infrastructure vs. Validation of Applications

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 Microsoft 365.

The ISPE's *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems* (Ref. [5]) 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*."

3.4.1 GAMP 5 Software Category

The ISPE's *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems* (Ref. [5]) 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 Microsoft 365 functionality for GxP-regulated processes (i.e. as a document repository), Microsoft 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 Microsoft 365. Such custom-development should be treated as a GAMP 5 Software **Category 5** – Custom Application and tested appropriately. Because Microsoft 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:

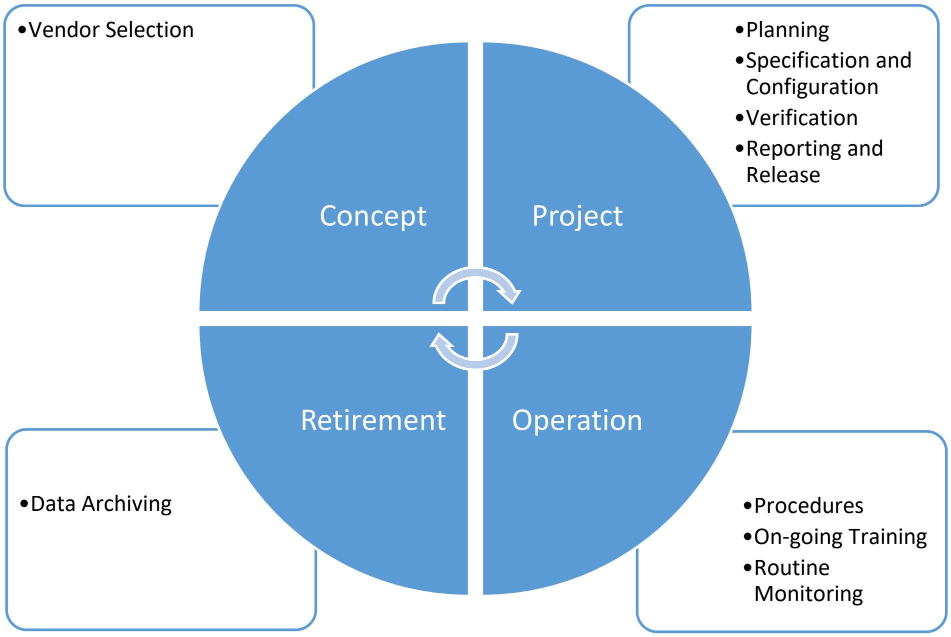
- **Process Owner**: The Process Owner acts as a subject matter expert for the business processes carried out within the system and is responsible for ensuring the system is fit for its intended use and operated in accordance with appropriate procedures (SOPs). The Process Owner represents the user group 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 Microsoft 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 the ensuring the Microsoft 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. [5]) 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

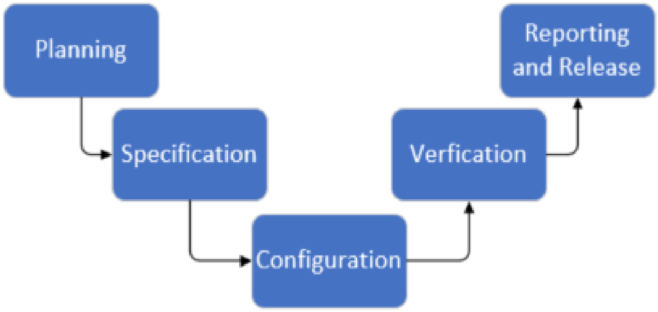
3.4.3.1 Concept

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 Microsoft 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 Microsoft 365. Planned activities should be scaled according to:

- The outcome of an initial risk analysis, in which the intended use of Microsoft 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. [7]), 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. SharePoint Online (SaaS) versus SharePoint 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 leverage the Microsoft 365 multi-geo capabilities when planning for data location and residency requirements. Multi-Geo in SharePoint Online and Groups enables global organizations to control the country or region where shared resources like SharePoint Team Sites, Office 365 Groups content are stored at-rest.

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 Microsoft 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 Microsoft 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 Microsoft 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 Microsoft 365 features that may be used to support GxP regulated activities (see Section 3.1.1), for example:

- Site collection features needed for records management
- Functionality pertaining to audit logging and document versioning
- Information management policies and functionality pertaining to record retention.
- System access and security controls
- Data encryption

Configuration specifications should be documented to establish the wireframe that will ensure Microsoft 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:

- Microsoft 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 labels and policies
- SharePoint Online administration settings, including the identification of relevant site collections
- Site Collection settings, including required site collection features, record declaration settings, and the identification of relevant sites and libraries.

A landscape diagram may prove to be beneficial in understanding the design, which may impact subsequent risk assessments and the definition of test strategies. The landscape diagram may be appended to the Configuration specifications or managed as a separate document.

Individuals responsible for designing the Microsoft 365 landscape should consider the following factors which may affect configuration decisions:

- The need for data isolation across functional departments/business units
- Service limits, quotas, and constraints. To help make design decisions, Microsoft routinely updates its list of SharePoint Online limits as new services are added or enhanced within Microsoft 365
- The need for separate Microsoft 365 tenants to achieve segregation of development, test, staging, and production environments
- The need for Multi-Geo capabilities in order to meet data residency requirements
- Options for scaling applications in Microsoft 365

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 Microsoft 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 Microsoft 365 admin center and SharePoint 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 Microsoft 365 is configured in accordance with documented specifications. Verifications should focus on key security and content management settings with GxP impact. Verification of the following configuration settings are typically performed:

- Configuration of site and list settings and enablement of key features having GxP impact
- Configuration of libraries, lists, columns and content types
- SharePoint Group permissions and inheritance
- Records management and content organizer settings

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, Microsoft 365 will be used and maintained in a controlled manner.

By using the Microsoft 365 platform, 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. Test cases covering the following scenarios are relevant:

- System security (logical security): Verifications to ensure that only authorized and authenticated users can access SharePoint Online
- User access controls: Verifications of the behavior of SharePoint groups and permissions
- Auditing: Verifications of functionality associated with document versioning and audit trail entries for the creation, modification, and deletion of records
- Records retention: Verification of functionality associated with record declaration, record labels and/or overarching site retention policies.

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 Microsoft 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 Microsoft 365 will meet stated requirements for electronic records management and additional business process needs.
✓ **Configuration specifications**	The Configuration specifications capture how Microsoft 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 Microsoft 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 Microsoft 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 in 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 Microsoft 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 Microsoft 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 Microsoft 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.

When repatriating data, customers may choose to use an "on-premise" SharePoint Server instance to store exported content or export all files and folders, maintaining the folder structure originally in the SharePoint site.

4 Conclusion

By combining state-of-the-art technology and industry standards, Microsoft 365 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 Microsoft 365 meets its specifications and is maintained in a state of control and compliance. Microsoft 365 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 sciences customers while defining their validation and governance strategies to ensure the integrity of their GxP content.

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
April 2019	Initial release
April 2020	Updated to incorporate new Microsoft 365 features and functionality.

6 References

6.1 Industry guidance and standards

Ref. [1] NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Ref. [2] PIC/S PI-011-3 Good Practices for Computerised Systems in Regulated "GXP" Environments, September 2007.

Ref. [3] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

Ref. [4] ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Ref. [5] ISPE, GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems, 2008.

Ref. [6] ISPE, GAMP Good Practice Guide: IT Infrastructure Control and Compliance (Second Edition), 2017.

Ref. [7] ISPE, GAMP Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition), 2012.

Ref. [8] ISPE, GAMP Good Practice Guide: Records & Data Integrity, 2017.

6.2 Regulations and regulatory guidance

Ref. [9] U.S. FDA, Code of Federal Regulations, Title 21 Part 11, Electronic Records; Electronic Signatures

Ref. [10] U.S. FDA, Guidance for Industry - Part 11, Electronic Records; Electronic Signatures — Scope and Application, August 2003.

Ref. [11] U.S. FDA, Data Integrity and Compliance with CGMP - Guidance for Industry (Draft Guidance), April 2016.

Ref. [12] U.S. FDA, Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11-- Questions and Answers (Draft Guidance), June 2017.

Ref. [13] 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

6.3 Microsoft resources and reference material

Microsoft publishes a variety of content for customers, partners, auditors, and regulators around security, compliance, privacy, and related areas. Below are links to other content in our Risk Assurance Documentation library.

Name	Abstract
Auditing and Reporting in Microsoft Cloud Services	Describes the auditing and reporting features in Microsoft 365 and Azure Active Directory available to customers. Also details the various audit data that is available to customers via the Microsoft 365 Security & Compliance Center, remote PowerShell, and the Management Activity

Name	Abstract
	API. Also describes the internal logging data that is available to Microsoft 365 engineers for detection, analysis, and troubleshooting.
Protect user and device access	Describes the Conditional Access (CA) features in Microsoft 365 and Microsoft Enterprise Mobility + Security, and how they are designed with built-in data security and protection to keep company data safe, while empowering users to be productive on the devices they love. It also provides guidance on how to address common concerns around data access and data protection using Microsoft 365 features.
Encryption in the Microsoft Cloud	Provides an overview of the various encryption technologies that are used throughout Microsoft 365, including features deployed and managed by Microsoft and features managed by customers.
Data Resiliency in Microsoft 365	Describes how Microsoft prevents customer data from becoming lost or corrupt in Exchange Online, SharePoint Online, and Skype for Business, and how Microsoft 365 protects customer data from malware and ransomware.
Defend Against Denial-of-Service Attacks in Microsoft 365	Discusses different types of Denial of Service attacks and how Microsoft defends Microsoft 365, Azure, and their networks against attacks.
Microsoft Cloud - Financial Services Compliance Program	Describes how the core contract amendments and the Microsoft Regulatory Compliance Program work together to support financial services customers in meeting their regulatory obligations as they relate to the use of cloud services.
Center for Financial Industry Information Systems (FISC)	Explains how Microsoft addresses the risks and requirements described in the FISC Revised Guidelines, and it describes features, controls, and contractual commitments that customers can use to meet the requirements in the Revised Guidelines.
Administrative Access Controls in Microsoft 365	Provides details on Microsoft's approach to administrative access and the controls that are in place to safeguard the services and processes in Microsoft 365. For purposes of this document, Microsoft 365 services include Exchange Online, Exchange Online Protection, SharePoint Online, and Skype for Business. Additional information about some Yammer Enterprise access controls is also included in this document.
Microsoft 365 Customer Security Considerations	Provides organizations with quick access to the security and compliance features in Microsoft 365 and considerations for using them.

Name	Abstract
Microsoft 365 Mapping of CSA Cloud Control Matrix 3.0.1	Provides a detailed overview of how Microsoft 365 maps to the security, privacy, compliance, and risk management controls defined in version 3.0.1-11-24-2015 of the Cloud Security Alliance's Cloud Control Matrix.
Microsoft 365 Risk Management Lifecycle	Provides an overview of how Microsoft 365 identifies, evaluates, and manages identified risks.
Security Incident Management in Microsoft 365	Describes how Microsoft handles security incidents in Microsoft 365.
Privacy in Microsoft Cloud Services	Describes Microsoft's privacy principles and internal privacy standards that guide the collection and use of customer and partner information at Microsoft and give employees a clear framework to help ensure that we manage data responsibly.
Tenant Isolation in Microsoft 365	Describes how Microsoft implements logical isolation of tenant data within Microsoft 365 environment.

6.3.1 Additional resources and reference material

Ref. [14] Microsoft Azure GxP Guidelines, April 2018

Ref. [15] Microsoft 365 mapping of CSA Security, Compliance and Privacy Cloud Control Matrix requirements

Ref. [16] Microsoft EU-U.S. Privacy Shield

Ref. [17] EU General Data Protection Regulation (GDPR)

Ref. [18] Microsoft 365 Compliance Offerings

7 Appendices

Appendix A: Glossary

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

Appendix C: Shared Responsibilities pertaining to U.S. FDA 21 CFR Part 11

Appendix D: Shared Responsibilities pertaining to EudraLex Volume 4 Annex 11

Appendix A. Glossary, Abbreviations and Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants
CFR	Code of Federal Regulations
CV	Curriculum vitae
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
OST	Online Services Terms
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
STP	Service Trust Portal
TSP	Trust services principles

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

The ISPE GAMP Good Practice Guide, *IT Infrastructure Control and Compliance* (Ref. [6]), recommends establishing mutual expectations of services delivery in a formal Service Level Agreement (SLA) or Quality Agreement.

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	For each Microsoft 365 subscription, a global administrator is assigned and is considered the customer's primary contact. By default, the person who purchased the Microsoft 365 subscription becomes a global administrator. Contact information for global administrator is maintained directly within the Microsoft 365 Admin Center. The customer's global administrator can manage his company's profile (including organization name, address, phone, and technical contact) directly within the Microsoft 365 Admin Center. Microsoft Account Managers typically act as the primary point of contact between Microsoft and its customers. The Online Services Data Protection Addendum (DPA) also contains a section on "How to Contact Microsoft," which provides instructions for contacting Microsoft.
Duration of validity and circumstances triggering reviews	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. As stated in the SOC 2 audit report (see Trust Criteria A1.1), Microsoft 365 management performs monthly reviews to evaluate capacity and availability.

Typical SLA/Quality Agreement Content	Coverage
Prerequisites and customer deliverables or involvement	Because of the generic nature of the Microsoft 365 online service offering, there are no specific prerequisites, customer deliverables, or involvement required in the delivery of the services to the customer.
Scope and nature of the required services	A detailed description of the Microsoft 365 Services offering is available in Microsoft 365 Services section of the Product Terms.
Metrics in the form of KPIs	Online Services SLAs contain service specific terms with relevant service performance metrics in the form of monthly uptime percentages. Microsoft monitors SLA performance and notifies customers if there is a lapse. Microsoft publishes information concerning the current Microsoft 365 service health on the online dashboard. Built-in diagnostic tools also allow administrators to monitor the customer's Microsoft 365 service health.
Records demonstrating fulfillment of specified service levels	Per the Online Services Data Protection Addendum (DPA), Microsoft maintains several logs and records related to security and data protection commitments: • Event logging: Microsoft logs, or enables customers 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.

Typical SLA/Quality Agreement Content	Coverage
	• 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. As described in Section 2.3.6.8 above, 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. Per the Online Services Data Protection Addendum (DPA), to the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Microsoft, its Affiliates, and its Subprocessors available.
Pricing arrangements, including penalties in case of shortcomings	Pricing arrangements for enterprise customers are stipulated in the Enterprise Agreement. 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.
Reports, scope, frequency, distribution	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.
Audit provisions, including preparedness to facilitate inspections from regulatory authorities or other regulators	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: • Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually. • 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.

Typical SLA/Quality Agreement Content	Coverage
	Each audit will result in the generation of an audit report that will clearly disclose any material findings by the auditor. Microsoft will promptly respond and when required remediate issues raised in any Microsoft audit report to the satisfaction of the auditor. Microsoft provides customers access to 3rd party audit reports, subject to non-disclosure and distribution limitations. Within its Security Policy, Microsoft defines technical and organizational measures to protect customer data. Microsoft will make that policy available to customers. Microsoft implements and maintains customer data security measures that comply with the Microsoft Security Policy and with the following control standards and frameworks: • ISO 27001 • ISO 27002 • ISO 27018 • SSAE 18 SOC 1 Type II • AT 101 SOC 2 Type II Microsoft may add additional standards but will not eliminate the above-listed standards or frameworks unless no longer used in the industry and it is replaced with an applicable successor. Customers may contact their Microsoft Account Managers for support requests should additional information be requested by a regulatory authority.
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	Microsoft responsibilities, controls, and practices concerning the following quality related activities are described as Security Measures within the Online Services Data Protection Addendum (DPA): • 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

Typical SLA/Quality Agreement Content	Coverage
	Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to customer data.
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)	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. 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.

Appendix C. Shared Responsibilities pertaining to U.S. FDA 21 CFR Part 11

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 evaluated as part of the most recent SOC 2 report for Microsoft 365. The Trust Criteria pertain to trust service principles and criteria that are met by control activities provided by Microsoft 365.

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
Subpart B — Electronic Records	
Sec. 11.10 Controls for closed systems.	
11.10 *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:*	
11.10 (a) *Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*	***Customer responsibilities*** - Produce Software Requirements and define data flow (as applicable) - Perform and document the qualification/validation activities surrounding the company's intended use of Microsoft 365. ***Microsoft responsibilities*** - Provide a qualified computing environment and ensure that the supporting hardware is also qualified. (Refer to Microsoft Azure GxP Guidelines). - Ensure that software has been developed, tested and maintained following a formal Software Development Lifecycle (SDLC) and Change Management process. (**Refer to SOC 2 Report Controls: CC7.1, CC7.2, CC7.3, and CC7.4)**. - Provide users with information surrounding upgrades and changes to Microsoft 365 services. (**Refer to SOC 2 Report Controls: CC2.2, CC2.3, and CC3.1)**

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
11.10 (b) *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.*	***Customer responsibilities*** - Manage stored records for completeness and accuracy. - Manage inputs and data uploads to Microsoft 365 for completeness, accuracy, and timeliness. - Ensure through verification that the transfer of data from any applications integrated with Microsoft 365 services does not impact data integrity. - Ensure that the Microsoft 365 services are validated to respond to this requirement. ***Microsoft responsibilities*** - Respect SLA terms for system availability and maintenance. (**Refer to SOC 2 Report Controls: A1.1, A.1.2, CC2.2, CC2.3 and CC7.2)**
11.10 (c) *Protection of records to enable their accurate and ready retrieval throughout the records retention period.*	***Customer responsibilities*** - Ensure that appropriate security controls are in place. - Ensure that backup infrastructure and policies are in place and have been tested. - Ensure that record retention policies have been defined. - Ensure that mechanisms for Disaster Recovery and Business Continuity are in place and tested, should any issue arise with the Microsoft 365 services subscribed to. - Data repatriation plan is in place and tested. ***Microsoft responsibilities*** - Ensure that security policies are in place. **(Refer to SOC 2 Report Controls: C1.1, C1.2 and CC5.3.)** - Respect SLA terms for system availability and maintenance. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)** - Ensure that controls are in place to oversee service of data backup or mirroring. (**Refer to SOC 2 Report Controls: A1.2, A1.3 and PI1.3)**

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
11.10 (d) *Limiting system access to authorized individuals.*	***Customer responsibilities*** - Ensure that appropriate Logical security policies are established, and training has been documented. - Ensure that appropriate System Administration practices are followed for Microsoft 365 services requiring such management activities. ***Microsoft responsibilities*** - Ensure that both Physical and Logical Security policies are in place and followed. **(For Logical Security considerations, refer to SOC 2 Report Controls: CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7 and CC6.8).** Note: Microsoft Datacenters are responsible for maintaining controls over physical access to facilities supporting Microsoft 365 that house backup storage media. (Refer to Microsoft Azure GxP Guidelines).
11.10 (e) *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.*	***Customer responsibilities*** - Ensure that appropriate security controls are in place. - Ensure that record retention policies have been defined. - Ensure that mechanisms for Disaster Recovery and Business Continuity are in place and tested, should any issue arise with the Microsoft 365 services subscribed to. - Data repatriation plan is in place and tested. - Ensure that audit trails have been properly defined and verified. ***Microsoft responsibilities*** - Ensure that security policies are in place. **(Refer to SOC 2 Report Controls: C1.1, C1.2, CC1.1, CC1.2, CC1.3, CC1.4, CC2.1, CC3.2, CC3.3, CC5.1, CC5.2, CC5.3, CC7.4 and CC7.5)** - Respect SLA terms for system availability and maintenance. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)** - Ensure that controls are in place to oversee service of data backup or mirroring. (**Refer to SOC 2 Report Controls: A1.2, A1.3 and PI1.3)**
11.10 (f) *Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.*	***Customer responsibilities*** - 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). ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
11.10 (g) *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.*	***Customer responsibilities*** - Ensure that appropriate Logical security policies are established, and training has been documented. - Ensure appropriate System Administration practices are followed for Microsoft 365 services requiring such management activities. ***Microsoft responsibilities*** - Ensure that both Physical and Logical Security policies are in place and followed. (**For Logical Security considerations, refer to SOC 2 Report Controls: CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6 and CC6.7).**. Note: Microsoft Datacenters are responsible for maintaining controls over physical access to facilities supporting Microsoft 365 that house backup storage media. (Refer to Microsoft Azure GxP Guidelines).
11.10 (h) *Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.*	***Customer responsibilities*** - Ensure that Microsoft 365 services subscribed to have been assessed to this requirement as defined in applicable Software Requirements and data flow documents. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
11.10 (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.*	***Customer responsibilities*** - 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 (i.e. training records, job descriptions, CV). ***Microsoft responsibilities*** - Training procedures have been established to evaluate the competency of personnel based on their job function. (**Refer to SOC 2 Report Controls: CC2.2, CC2.3 and CC7.2.).**
11.10 (j) *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.*	***Customer responsibilities*** - Not applicable - Microsoft software will not be used to apply electronic signatures at this time. ***Microsoft responsibilities*** - Not applicable – Microsoft software will not be used to apply electronic signatures at this time.

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
11.10 (k) ***Use of appropriate controls over systems documentation including:***	***Customer responsibilities*** - Documents under the scope of these requirements include procedures, requirements, specifications, and validation documents. ***Microsoft responsibilities*** - Documents under the scope of these requirements include system descriptions, procedures, and technical specifications.
11.10 (k)(1) *Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.*	***Customer responsibilities*** - Ensure that procedural controls are in place to appropriately manage the distribution, access and use of system documentation. ***Microsoft responsibilities*** - Ensure that procedural controls are in place to appropriately manage the distribution, access and use of system documentation produced for M365 environment(s) operations and maintenance. (**Refer to SOC 2 Report Controls: CC6.8, CC7.1 and CC8.1)**
11.10 (k)(2) *Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Documentation management controls (procedures) are in place for specifications. - Revision history of documents may contain the audit trail of changes made to documentation. **(Refer to SOC 2 Report Controls: CC6.8, CC7.1 and CC8.1.)**.
Sec. 11.30 Controls for Open Systems	

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
11.30 *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.*	***Customer responsibilities*** - Configure encryption and access controls to ensure that the integrity of data is maintained. - Define data segregation model to be used. - Ensure that Microsoft 365 services subscribed to have been assessed to this requirement as defined in applicable Software Requirements and data flow documents. ***Microsoft responsibilities*** - A series of procedural and technical controls are in place to ensure the protection and confidentiality of customer data. (**Refer to SOC 2 Report Controls: C1.1, CC2.3, CC6.1, CC6.6, CC6.7, A1.1, PI1.3, PI1.4 and PI1.5)** - Internal communication where customer data is transmitted/involved is secured using SSL or equivalent mechanisms and travels within secured tunnel.
Sec. 11.50 Signature manifestations	
11.50 (a) *Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:* ***11.50 (a) (1)*** ***The printed name of the signer;*** ***11.50 (a) (2)*** ***The date and time when the signature was executed; and*** ***11.50 (a) (3)*** ***The meaning (such as review, approval, responsibility, or authorship) associated with the signature.*** ***11.50 (b)*** *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).*	***Customer responsibilities*** - Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements. ***Microsoft responsibilities*** - Not applicable - this requirement applies exclusively to the regulated use of the GxP application.
Sec. 11.70 Signature/record linking	
11.70 *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.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Subpart C — Electronic Signatures	
Sec. 11.100 General requirements	

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
11.100 (a) *Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
11.100 (b) *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.*	***Customer responsibilities*** - Ensure procedure controls are in place to govern the assignment of electronic signatures. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
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.* ***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.* ***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.*	***Customer responsibilities*** - Ensure that a letter of intent 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Sec. 11.200 Electronic signature components and controls	
11.200 (a) ***Electronic signatures that are not based upon biometrics shall:***	

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
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.* ***11.200 (a) (2)*** *Be used only by their genuine owners; and* ***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.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
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.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Sec. 11.300 Controls for identification codes/passwords.	
11.300 ***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:***	
11.300 (a) *Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

U.S. FDA 21 CFR Part 11	Customer / Microsoft shared responsibilities
11.300 (b) *Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
11.300 (c) *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.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
11.300 (d) *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.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
11.300 (e) *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.*	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.

Appendix D. Shared Responsibilities pertaining to EudraLex Volume 4 Annex 11

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 table shows how Microsoft and customer responsibilities are shared. In addition, for each Microsoft responsibility, the corresponding controls are traced to the Microsoft SOC 2 Report.

EU Volume 4 Annex 11	Customer / Microsoft shared 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.	***Customer responsibilities*** - Document the assessment of risks related to patient safety, data integrity and product quality as part of the validation activities surrounding the use of Microsoft 365 services. - Following the assessment of risks described above define/implement the necessary controls to ensure the integrity of data. ***Microsoft responsibilities*** - Risk management is incorporated into processes surrounding the development and maintenance of Microsoft 365 services. **(Refer to SOC 2 Report Controls: CC3.1, CC3.2, CC3.3, CC3.4, CC9.1 and CC9.2**) - Respect SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)**
2. Personnel	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Ensure that appropriate Training policies are established, and that training and personnel qualifications are documented (i.e. training records, job description, CV). - Ensure that appropriate Logical security policies are established, and training has been documented. ***Microsoft responsibilities*** - Training procedures have been established to evaluate the competency of personnel based on their job function. (**Refer to SOC 2 Report Controls: CC1.1, CC1.2, CC1.3, CC1.4, CC1.5, CC2.1, CC2.2, CC2.3, CC3.1, CC3.2, CC3.3, CC4.1, CC5.1, CC5.2, CC5.3, CC7.1, CC7.4, CC7.5, PI1.1, PI1.2, PI1.3 and PI1.4)** - Physical and Logical Security policies are in place to limit access to authorized individuals based on the individual's job duties. **(For Logical Security considerations, refer to SOC 2 Report Controls: CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6 and CC6.7)** Note: Microsoft Datacenters are responsible for maintaining controls over physical access to facilities supporting Microsoft 365 (Refer to Microsoft Azure GxP Guidelines) Moreover, Microsoft Datacenters are responsible for maintaining controls related to protection of the network environment. (Refer to Microsoft Azure GxP Guidelines).
3. Suppliers and Service Providers	
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.	***Customer responsibilities*** - Ensure that formal agreements are implemented with suppliers that clearly define the roles and responsibilities of each party. ***Microsoft responsibilities*** - 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 Report Controls: CC2.3, CC3.2, CC3.3, CC3.4, CC7.2 and CC9.2)** - Formal agreements are implemented between Microsoft and its customers that include statements of responsibilities.
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.	***Customer responsibilities*** - Ensure that the supplier assessment process is documented and provides rationale to support the method implemented to qualify a selected supplier. ***Microsoft responsibilities*** - Risks related to external parties are assessed and addressed. (**Refer to SOC 2 Report Controls: CC9.2)**

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	***Customer responsibilities*** - Ensure that supplier/vendor provided documentation is reviewed/verified during validation activities to ensure that this requirement is met. ***Microsoft responsibilities*** - Microsoft continuously publishes and updates content on the Microsoft 365 Documentation site and within the Service Trust Portal (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 Microsoft 365 training website.
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.	***Customer responsibilities*** - Review the most recent Microsoft 365 ISO certificates 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. ***Microsoft responsibilities*** - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Portal (STP). **(Refer to SOC 2 Report Controls: CC1.2, CC1.3, CC2.1, CC3.1, CC3.2, CC3.4, CC4.1, CC4.2 and CC5.3)**
Project Phase	
4. Validation	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Implement a formal computer system validation policy or procedure that conforms to the specified requirements. - Perform and document the validation of Microsoft 365 services based on a risk assessment. ***Microsoft responsibilities*** - Procedures and controls are in place to ensure the Microsoft 365 platform is developed and tested in accordance with industry best practices and standards (for example, ISO/IEC 27001) to ensure quality and security as well as consistent and reliable performance. (**Refer to SOC 2 Report Controls CC7.1, CC7.2, CC7.3, and CC7.4)** - Risk management is incorporated into processes around the development and maintenance of the Microsoft 365 platform. (**Refer to SOC 2 Report Controls: CC3.1, CC3.2, CC3.3, CC3.4, CC9.1 and CC9.2)**
4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	***Customer responsibilities*** - Implement formal change control and deviation management processes in conjunction with validation activities surrounding the intended use of Microsoft 365 services. ***Microsoft responsibilities*** - A formal change management process is defined governing how changes are made to the Microsoft 365 platform (including products, services, and supporting hardware). (**Refer to SOC 2 Report Controls: CC2.2, CC2.3 and CC3.1)**
4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. 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.	***Customer responsibilities*** - 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 ***Microsoft responsibilities*** - Microsoft maintains an inventory of key information assets. - Controls are in place to ensure the Microsoft 365 platform (including products, services, and supporting hardware) is maintained in a state of control and compliance. (**Refer to SOC 2 Report Controls: CC7.1, CC7.2, CC7.3 and CC7.4)**

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Implementation and use of a formal Software Development Lifecycle policy or procedure which meets these requirements. ***Microsoft responsibilities*** - Microsoft 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 Report Controls: CC7.1, CC7.2, CC7.3, and CC7.4)** - Formal risk assessments are performed on a regular basis **Refer to SOC 2 Report Controls: CC3.1, CC3.2, CC3.3, CC3.4, CC9.1 and CC9.2)**
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.	***Customer responsibilities*** - Review the most recent Microsoft 365 ISO certificates 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. ***Microsoft responsibilities*** - Microsoft regularly undergoes independent audits performed by qualified third-party accredited assessors for ISO (27001, 27018), SOC (1, 2), HITRUST, and FedRAMP. - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Portal (STP) **(Refer to SOC 2 Report Controls: CC1.2, CC1.3, CC2.1, CC3.1, CC3.2, CC3.4, CC4.1, CC4.2 and CC5.3)**
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.	***Customer responsibilities*** - Document validation testing activities in accordance with established processes. - Establish controls to ensure the assessment of quality and performance metrics throughout the GxP computerized system's lifecycle. ***Microsoft responsibilities*** - Microsoft's development teams follow defined processes for verifying newly developed products and features, as well as for product changes and enhancements. (**Refer to SOC 2 Report Controls: CC2.2, CC2.3, and CC3.1)** - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Portal (STP). **(Refer to SOC 2 Report Controls: CC1.2, CC1.3, CC2.1, CC3.1, CC3.2, CC3.4, CC4.1, CC4.2 and CC5.3)**

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Ensure the implementation and use of a formal computer system validation policy or procedure that meets these requirements. - Document validation testing activities in accordance with established processes. ***Microsoft responsibilities*** - Microsoft's development teams follow defined processes for verifying newly developed products and features, as well as for product changes and enhancements. (**Refer to SOC 2 Report Controls: CC7.1, CC7.2, CC7.3, and CC7.4)** - Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Portal (STP). (**Refer to SOC 2 Report Controls: CC1.2, CC1.3, CC2.1, CC3.1, CC3.2, CC3.4, CC4.1, CC4.2 and CC5.3)**
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.	***Customer responsibilities*** - Establish data migration plan and testing strategy to ensure data integrity is maintained during the migration process. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
Operational Phase	
5. Data	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Perform and document validation activities surrounding the deployment of applications/systems using Microsoft 365 services. - 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. - Ensure that audit trails have been properly defined and verified. - Ensure through verification that the transfer of data from applications/systems to Microsoft 365 services (which may store data) does not impact data integrity. - Ensure that appropriate security controls are defined to govern Microsoft 365 access along with permissions related to data. - Ensure that backup infrastructure and policies are in place and have been tested for Microsoft 365 related data. - Ensure that record retention policies have been defined. - Ensure that mechanisms for Disaster Recovery and Business Continuity are in place and tested, should any issue arise with Microsoft 365 services. - Implement periodic review of assigned access rights. - Verify GxP system only permits authorized actions to be taken with respect to regulated content. ***Microsoft responsibilities*** - Encryption and access controls have been implemented to ensure that the integrity of data is maintained. (**Refer to SOC 2 Report Controls: CC2.3, CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, A1.1, PI1.3, PI1.4 and PI1.5)**
6. Accuracy Checks	
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.	***Customer responsibilities*** - Establish procedural controls to enforce review of manually entered data or implement automated accuracy check mechanisms as part of the GxP system design and configuration. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
7. Data Storage	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Ensure that appropriate security controls are defined to govern Microsoft 365 access along with permissions related to data. - Ensure that record retention policies have been defined. - Ensure that appropriate Logical security policies are established, and training has been documented. - Ensure that audit trails have been properly defined and verified. - Ensure appropriate System Administration practices are followed. - Ensure appropriate governance of System Administration activities surrounding the management of Microsoft 365 services. - Ensure that encryption and access controls are in place to ensure that the integrity of data is maintained. ***Microsoft responsibilities*** - Security controls to protect Microsoft 365 services and infrastructure are in place. **(Refer to SOC 2 Report Controls: C1.1, C1.2 and CC5.3)** - 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 Report Controls: CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6 and CC6.7)** - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)** - Controls are in place to oversee the service of data backup or mirroring. (**Refer to SOC 2 Report Controls: CC2.3, CC6.1, CC6.6, A1.1, PI1.3, PI1.4 and PI1.5)**

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Ensure that mechanisms for Disaster Recovery and Business Continuity are in place and tested, should any issue arise with Microsoft 365 services. - Implement and test data repatriation plan(s). - Ensure that backup infrastructure and policies are in place and have been tested for Microsoft 365 services related data. ***Microsoft responsibilities*** - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity. **(Refer to SOC 2 Report Controls: CC2.3, CC6.1, CC6.6, A1.1, PI1.3, PI1.4 and PI1.5)** - Physical and logical security policies are in place and followed. (**For Logical Security considerations, refer to SOC 2 Report Controls: CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7 and CC6.8)** - 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. Note: Microsoft Datacenters are responsible for maintaining controls over physical access to facilities supporting Microsoft 365 (Refer to Microsoft Azure GxP Guidelines) Moreover, Microsoft Datacenters are responsible for maintaining controls related to protection of the network environment. (Refer to Microsoft Azure GxP Guidelines).
8. Printouts	
8.1 It should be possible to obtain clear printed copies of electronically stored data.	***Customer responsibilities*** - Ensure through verification that the transfer of data from Microsoft 365 services (which may store data) does not affect data integrity. - Verify that Microsoft 365 Services conforms to the specified regulatory requirement. ***Microsoft responsibilities*** - Respect SLA terms for data/service availability and maintenance. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)**

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Ensure through verification that the transfer of data from Microsoft 365 services (which may store data) does not affect data integrity. - Verify that Microsoft 365 Services conforms to the specified regulatory requirement. ***Microsoft responsibilities*** - Respect SLA terms for data/service availability and maintenance. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)**
9. Audit Trails	
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.	***Customer responsibilities*** - Ensure that appropriate security controls are defined to govern Microsoft 365 access along with permissions related to data. - Ensure that backup infrastructure and policies are in place and have been tested for data maintained within Microsoft 365. - Ensure that record retention policies have been defined. - Ensure that mechanisms for Disaster Recovery and Business Continuity are in place and tested, should any issue arise with Microsoft 365 services. - Implement and test data repatriation plan(s). - Ensure that audit trails have been properly defined and verified. - Ensure that documentation management controls are in place (i.e. procedure). ***Microsoft responsibilities*** - Respect SLA terms for data/service availability and maintenance. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)**
10. Change and Configuration Management	
Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	***Customer responsibilities*** - Ensure that a formal change management process is in place to govern any configuration changes to the Microsoft 365 services. - Ensure appropriate governance of System Administration activities surrounding the management of Microsoft 365 Services. ***Microsoft responsibilities*** - A formal change management process is in place. **(Refer to SOC 2 Report Controls: CC8.1)** - Microsoft notifies customers of potential changes and events that may affect security or availability of the services. (**Refer to SOC 2 Report Controls: CC2.2, CC2.3, and CC3.1)**
11. Periodic evaluation	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Ensure that procedural controls are in place to periodically review the state of Microsoft 365 services to meet this requirement. ***Microsoft responsibilities*** - Controls are in place to periodically review the state of Microsoft 365 services to ensure their configuration is aligned with the baseline configuration. **(Refer to SOC 2 Report Controls: CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, CC5.3, CC7.3, CC8.1 and CC9.2)**
12. Security	
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. 12.2 The extent of security controls depends on the criticality of the computerised system. 12.3 Creation, change, and cancellation of access authorisations should be recorded. 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.	***Customer responsibilities*** - Ensure that appropriate security controls are defined to govern Microsoft 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 the management of Microsoft 365 services. - Ensure that audit trails have been properly defined and verified. - Ensure procedure controls are in place to help meet this requirement. ***Microsoft responsibilities*** - Security policies to protect Microsoft 365 services and infrastructure are in place. **(Refer to SOC 2 Report Controls: C1.1, C1.2 and CC5.3)** - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity. **(Refer to SOC 2 Report Controls: A1.1, A.1.2, CC2.2, CC2.3 and CC7.2)** - Physical and logical security policies are in place and followed. **(For Logical Security considerations, refer to SOC 2 Report Controls: CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6 and CC6.7)** Note: Microsoft Datacenters are responsible for maintaining controls over physical access to facilities supporting Microsoft 365 that house backup storage media. (Refer to Microsoft Azure GxP Guidelines).
13. Incident Management	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Ensure procedure controls are in place to manage system incidents and perform root cause analysis to identify corrective and preventive actions. ***Microsoft responsibilities*** - 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 Report Controls: CC2.2, CC3.2, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, A1.1 and A1.2)**
14. Electronic Signature	
Electronic records may be signed electronically. Electronic signatures are expected to: 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.	***Customer responsibilities*** - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
15. Batch Release	
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.	***Customer responsibilities*** - Perform and document validation activities for applications/systems using Microsoft 365 services. - 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. ***Microsoft responsibilities*** - Not applicable – this requirement applies exclusively to the regulated use of the GxP application.
16. Business Continuity	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - 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). ***Microsoft responsibilities*** - Ensure that mechanisms for disaster recovery and business continuity are in place and tested, should any issue arise with Microsoft 365 services. (**Refer to SOC 2 Report Controls: CC7.2, CC9.1, A1.2 and A1.3)** - Ensure that backup infrastructure and policies are in place and have been tested. **(Refer to SOC 2 Report Controls: A1.2 and A1.3)** Note: Microsoft Datacenters are responsible for maintaining controls over physical movement of data. (Refer to Microsoft Azure GxP Guidelines). - Implement and test data repatriation plan(s). - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)**
17. Archiving	

EU Volume 4 Annex 11	Customer / Microsoft shared responsibilities
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.	***Customer responsibilities*** - Implement appropriate security controls that govern access to Microsoft 365) including permissions related to 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. - Implement and test data repatriation plan(s). ***Microsoft responsibilities*** - Security controls to protect Microsoft 365 services and infrastructure are in place. **(Refer to SOC 2 Report Controls: C1.1, C1.2 and CC5.3)** - 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 Report Controls: CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6 and CC6.7)** - SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity. **(Refer to SOC 2 Report Controls: A1.1, A1.2, CC2.2, CC2.3 and CC7.2)** - Controls are in place to oversee the service of data backup or mirroring. **(Refer to SOC 2 Report Controls: A1.2, A1.3 and PI1.3)**