

**DISCLAIMER**

© 2017 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. In addition, for your convenience, this document references one or more Microsoft agreements and summarizes portions of such agreements. 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 legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You bear the risk of using it.

**Acknowledgements**

**Authors:** Katie Look, Michael Zwetkow (Montrium), Paul Slater

**Reviewers:**

Microsoft: Benny Vermachelen, Christof Wascher, Derek Harris, Frank Simorjay, Gabor Fari, Stevan Vidich, Tom Schinder

Industry: Christopher Bullock (Johnson & Johnson), Jeffrey Feist (Merck) Judith Samardelis (AstraZeneca Pharmaceuticals), Luca Emili (Promeditec), Markus Roemer (comes compliance services), Meredith Sewell (Allergan), Robert Streit (Johnson & Johnson), Sion Wyn (Conformity Ltd.), Steven Jeffrey (GlaxoSmithKline), Wolfgang Schumacher (SPC – Schumacher Pharma Consult, formerly F. Hoffmann-La Roche Ltd.)

## Foreword

Over the past few years, life sciences organizations have begun to consider cloud computing as a major part of their overall IT strategy. Microsoft partners and customers in the life sciences industry are beginning to embrace cloud as an engine of digital transformation—one that can shorten the time to market, and that has the potential to drive whole new categories of products and services.

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.

As a company that manages millions of servers, Microsoft has a deep understanding of standardized policies and procedures, and how to ensure predictable outcomes and manage risk at extreme scale. 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 guidelines document is a key step toward that goal. Although the ultimate responsibility for validating GxP applications remains with our customers and partners, no matter where those applications are hosted, this guide should help demonstrate that you can develop and operate GxP applications on Microsoft Azure with confidence and remain compliant while using Microsoft cloud services.

We look forward to working with you to help you achieve your digital transformation initiatives using Azure, the Microsoft hyperscale cloud platform.

Paul Slater – Worldwide Industry Strategist, Pharmaceuticals

**Microsoft Corporation**

**December 2017**

## Executive summary

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

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

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

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

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

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

## Authors

The production of this GxP guidelines document was driven by the Microsoft Azure Health and Life Sciences Team, and was developed in collaboration with several functional team members whose responsibilities include compliance, engineering, legal, life sciences, technology, strategy, and account management. We collaborated with our longstanding life sciences industry partner, [Montrium](#), to review internal Microsoft Azure 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 more than 150 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 qualified Azure-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.....  | 2  |
| Executive summary.....                                     | 3  |
| Authors.....   | 4  |
| 1 Introduction .....                                       | 8  |
| 1.1 Purpose.....   | 8  |
| 1.2 Audience and scope.....                                | 9  |
| 1.3 Key terms and definitions.....                         | 9  |
| 1.3.1 GxP .....  | 9  |
| 1.3.2 GxP regulations .....                                | 9  |
| 1.3.3 GxP computerized system.....                         | 10 |
| 1.3.4 Customer .....                                       | 10 |
| 1.3.5 Microsoft Azure and the Azure platform .....         | 10 |
| 1.3.6 IaaS.....  | 10 |
| 1.3.7 PaaS.....  | 10 |
| 2 Overview of Microsoft Azure .....                        | 10 |
| 2.1 Azure products and services.....                       | 11 |
| 2.2 Microsoft Online Services.....                         | 12 |
| 2.3 Azure Government .....                                 | 12 |
| 2.4 Azure certifications and attestations .....            | 13 |
| 2.4.1 SOC 1 & SOC 2 .....                                  | 13 |
| 2.4.2 CSA Security, Trust & Assurance Registry (STAR)..... | 14 |
| 2.4.3 FedRAMP .....  | 14 |
| 2.4.4 ISO/IEC 27001:2013 .....                             | 15 |
| 2.4.5 ISO/IEC 27018:2014 .....                             | 15 |
| 2.4.6 ISO 9001:2015 .....                                  | 16 |
| 2.4.7 ISO/IEC 20000-1:2011 .....                           | 16 |
| 2.4.8 HITRUST.....   | 16 |
| 2.5 Azure Quality Management System.....                   | 17 |
| 2.5.1 Roles and responsibilities.....                      | 17 |
| 2.5.2 Policies and standard operating procedures .....     | 19 |
| 2.5.3 Microsoft personnel and contractor training .....    | 20 |

|        |   |    |
|--------|---|----|
| 2.5.4  | Documented information .....  | 20 |
| 2.5.5  | Design and development of Azure products and services.....  | 21 |
| 2.5.6  | Operations management .....   | 25 |
| 2.5.7  | Performance evaluation.....   | 31 |
| 2.5.8  | Improvement .....   | 32 |
| 3      | Recommendations to consider for satisfying GxP requirements .....                                     | 32 |
| 3.1    | Implementing a cloud strategy and governance model.....   | 33 |
| 3.1.1  | Shared responsibilities .....   | 34 |
| 3.1.2  | Computerized systems compliance policies and procedures .....   | 35 |
| 3.1.3  | Personnel training .....  | 36 |
| 3.1.4  | Supplier evaluation .....   | 37 |
| 3.1.5  | Service agreements.....   | 38 |
| 3.1.6  | Data integrity .....  | 39 |
| 3.1.7  | Operations, maintenance, and monitoring.....  | 41 |
| 3.2    | Qualification and validation considerations for cloud-based GxP applications.....                     | 44 |
| 3.2.1  | GAMP categories.....  | 45 |
| 3.2.2  | Qualification considerations of infrastructure components and services (Platform qualification) ..... | 46 |
| 3.2.3  | Validation considerations for PaaS-based GxP applications.....  | 52 |
| 3.3    | GxP-relevant products and service features within Azure .....   | 54 |
| 3.3.1  | High availability .....   | 54 |
| 3.3.2  | Local and geographic redundancy .....   | 55 |
| 3.3.3  | Ability to specify geographic location of data.....   | 55 |
| 3.3.4  | Customer data isolation .....   | 55 |
| 3.3.5  | Encryption of data in transit and at rest .....   | 55 |
| 3.3.6  | Azure Key Vault .....   | 56 |
| 3.3.7  | Azure Rights Management Services.....   | 56 |
| 3.3.8  | Azure Resource Manager .....  | 56 |
| 3.3.9  | Virtual machine scale sets.....   | 57 |
| 3.3.10 | Azure Active Directory and Azure AD Connect .....   | 57 |
| 3.3.11 | Azure Backup service and recovery .....   | 57 |
| 3.3.12 | Azure Automation .....  | 57 |
| 3.3.13 | Azure Logic Apps .....  | 58 |

|             |  |    |
|-------------|--|----|
| 3.3.14      | Azure Roadmap and updates .....  | 58 |
| 3.3.15      | Cloud monitoring .....   | 58 |
| 3.3.16      | Azure Metadata Service - Scheduled Events (Preview) .....  | 58 |
| 3.3.17      | EU GDPR compliance .....   | 59 |
| 4           | Conclusion .....   | 59 |
| 5           | Document Revision .....  | 60 |
| 6           | References .....   | 61 |
| 6.1         | Industry guidance and standards .....  | 61 |
| 6.2         | Regulations and regulatory guidance .....  | 61 |
| 6.3         | Microsoft resources and reference material.....  | 62 |
| 6.3.1       | Compliance and quality.....  | 62 |
| 6.3.2       | Technical .....  | 62 |
| 6.4         | Other references .....   | 63 |
| 7           | Appendices.....  | 63 |
| Appendix A. | Glossary, Abbreviations and Acronyms .....   | 64 |
| Appendix B. | Coverage of SLA / Quality Agreement Requirements with Microsoft Azure Agreements<br>65             |    |
| Appendix C. | US FDA 21 CFR Part 11 Electronic Records; Electronic Signatures - Shared<br>Responsibilities ..... | 69 |
| Appendix D. | EudraLex Volume 4 Annex 11 Computerised Systems - Shared Responsibilities .....                    | 78 |

## 1 Introduction

### 1.1 Purpose

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

Microsoft's goal is to provide life sciences organizations with a comprehensive toolset for using Azure 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 cloud services as the basis for their GxP validated applications. We also collaborated with Montrium to review our internal quality and development practices, while collaborating with industry subject matter experts and regulatory agencies to identify critical elements that have GxP relevance. Together, we defined recommendations for organizations seeking to use Azure-based GxP applications.

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

- Increased visibility into crucial areas of internal Azure quality management, IT infrastructure qualification, and software development practices
- Recommendations for customer GxP compliance readiness, including an approach for establishing qualified environments using Azure IaaS (infrastructure as a service) and PaaS (platform as a service) to support cloud-based GxP applications or workloads
- Description of GxP-relevant tools and features within Azure
- 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 Azure and its customers. We have implemented a series of technical and procedural controls to help ensure the dependability (accessibility, availability, reliability, safety, integrity, and maintainability) of Microsoft systems and services. Of equal importance are the activities performed by Microsoft customers in protecting the security and privacy of their data.

This guidelines document begins with an initial focus on internal Azure quality and development practices, followed by a customer focus consisting of our recommendations to help life sciences industry customers successfully implement their GxP applications in Azure.



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

<sup>1</sup>Section 2 includes details about internal Microsoft systems, controls, and processes.

<sup>2</sup>Section 3 includes recommendations for customers implementing GxP applications within Azure.

## 1.2 Audience and scope

Life sciences organizations as well as IT solution providers using the Azure platform to host GxP-regulated computerized systems or workloads can benefit from the information contained in this guidelines document. The life sciences industry consists of a wide array of organizations operating in various segments, including pharmaceuticals, biotechnology, medical device clinical research, and veterinary medicine.

The Azure platform may be used across these industry segments to run a variety of business applications that support GxP activities. The specific GxP activities performed within the customer's Azure environment are not addressed in this guidelines document, as the customer (regulated user) is responsible for defining the requirements and validating the GxP computerized system installed within Azure.

The Azure products and services within the scope of this document include the Azure Core Services, Microsoft Online Services, and Azure Government, are identified in Sections 2.1, 2.2 and 2.3

## 1.3 Key terms and definitions

### 1.3.1 GxP

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

### 1.3.2 GxP regulations

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

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

- Prescription Drug Marketing Act (PDMA)

### 1.3.3 GxP computerized system

A GxP computerized system is a computerized system that is subject to GxP regulations as defined earlier. Throughout this guidelines document, the terms GxP computerized system, GxP system, and GxP application are used interchangeably.

### 1.3.4 Customer

Within the context of this guidelines document, the customer is any person or organization using or managing a GxP computerized system hosted on the Azure platform.

### 1.3.5 Microsoft Azure and the Azure platform

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

### 1.3.6 IaaS

The IaaS service model includes the infrastructure resources from the facilities to the hardware platforms and the hypervisor that supports the customer's computer resources—that is, virtual machines and containers. IaaS capability provides the customer with the ability to provision processing, storage, networks, and other fundamental computing resources on which the customer can deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (for example, host firewalls).

### 1.3.7 PaaS

The PaaS service model provides an additional layer of integration with application development frameworks, middleware capabilities, and functions such as databases, messaging, and queuing. PaaS allows developers to build and deploy applications on the platform. PaaS also provides the customer with the capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure, which might include network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

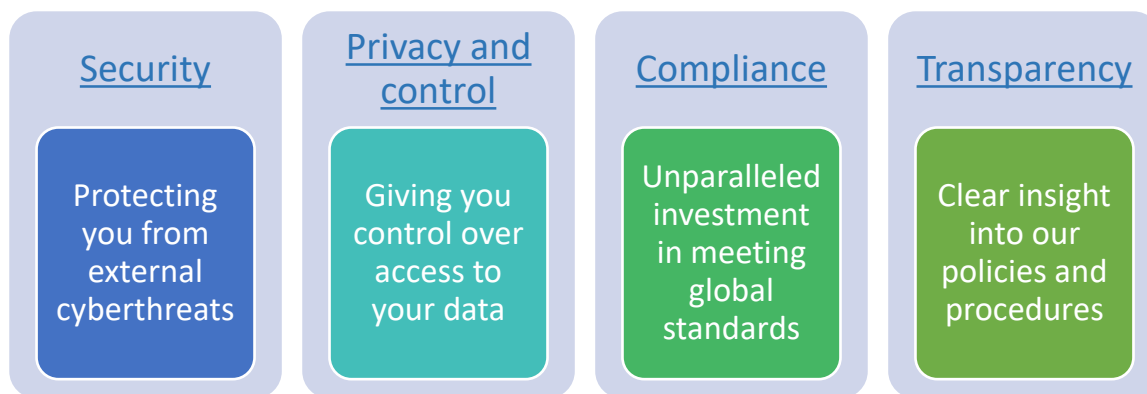
## 2 Overview of Microsoft Azure


[Microsoft Azure](#) is a multi-tenant public cloud computing platform for building, deploying, and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both infrastructure as a service (IaaS) and platform as a service (PaaS) cloud service models and enables hybrid solutions that integrate cloud services with customers' on-premises resources.

Azure consists of a growing collection of integrated cloud services, including analytics, computing, database, mobile, networking, storage, and web. Microsoft has applied state-of-the-art technology and processes across all cloud services to maintain consistent and reliable access, security, and privacy and have incorporated capabilities for compliance with a wide range of regulations and privacy mandates.

The Azure platform is supported by a growing network of more than 100 Microsoft-managed [datacenters](#) containing millions of servers and is currently available in 140 countries, including 42 regions. Our experience delivering consumer and enterprise cloud services at a global scale dates to 1994, when MSN was launched. Since then, the Microsoft cloud infrastructure has grown to more than one billion customers and 200 million organizations.

At Microsoft, trust is a focal point for services delivery, contractual commitments, and industry accreditation, which is why we established the [Trusted Cloud initiative](#). This set of requirements, guidelines, and controlled processes ensures we deliver our cloud services with the highest standards regarding engineering, legal, and compliance support. The Trusted Cloud initiative is divided into four key pillars:



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

## 2.1 Azure products and services

Azure consists of the following products and services (see the [Microsoft Azure Compliance Offerings](#) white paper):

- **Compute:** Batch, Cloud Services, Functions, Service Fabric, Virtual Machines (including SQL VM), Virtual Machine Scale Sets
- **Containers:** Azure Container Registry, Azure Container Service
- **Networking:** Application Gateway, Azure DNS, Azure Network Watcher, ExpressRoute, Load Balancer, Traffic Manager, Virtual Network, VPN Gateway
- **Storage:** Backup, Cool Storage, Data Lake Store, Import/Export, Premium Storage, Site Recovery, Storage (blobs, disks, files, queues, tables), StorSimple
- **Web + Mobile:** App Service (including API Apps, Mobile Apps, and Web Apps), Azure Search, Media Services

- **Databases:** Azure Cosmos DB, Azure Database for MySQL, Azure Database for PostgreSQL, Redis Cache, SQL Database, SQL Data Warehouse, SQL Server Stretch Database
- **Data + Analytics:** Azure Analysis Services, Data Lake Analytics, HDInsight, Machine Learning, Stream Analytics
- **Internet of Things:** Event Hubs, Internet of Things (IoT) Hub, Notification Hubs
- **Enterprise Integration:** API Management, Data Catalog, Logic Apps, Service Bus
- **Security + Identity:** Azure Active Directory (Free, Basic), Azure Active Directory (Premium) Azure Active Directory B2C, Azure Active Directory Domain Services, Azure Information Protection (including Azure Rights Management), Key Vault, Multi-Factor Authentication, Security Center
- **Developer Tools:** Application Insights, Azure DevTest Labs
- **Monitoring + Management:** Automation, Azure Advisor, Azure Monitor, Azure Resource Manager, Log Analytics, Microsoft Azure Portal, Scheduler

## 2.2 Microsoft Online Services

Additional Microsoft Online Services (covered by the Azure Service Organization Controls (SOC) 2 audit report, see Section [2.4.1](#)) consist of the following products and services:

- [Microsoft Cloud App Security](#)
- [Microsoft Flow](#)
- [Microsoft Graph](#)
- [Microsoft Intune](#)
- [Microsoft Power BI](#)
- [Microsoft PowerApps](#)
- [Microsoft Stream](#)

## 2.3 Azure Government

[Azure Government](#) is a separate Azure cloud that is offered exclusively to governmental organizations and consists of the following products and services:

- **Compute:** Batch, Cloud Services, Service Fabric, Virtual Machines (including SQL VM), Virtual Machine Scale Sets
- **Networking:** Application Gateway, ExpressRoute, Load Balancer, Traffic Manager, Virtual Network, VPN Gateway
- **Storage:** Backup, Cool Storage, Import/Export, Premium Storage, Site Recovery, Storage (blobs, disks, files, queues, tables), StorSimple
- **Web + Mobile:** App Service (including API Apps, Mobile Apps, and Web Apps), Media Services
- **Databases:** Redis Cache, SQL Database, SQL Data Warehouse, SQL Server Stretch Database
- **Data + Analytics:** HDInsight
- **Internet of Things:** Event Hubs, Notification Hubs
- **Enterprise Integration:** Service Bus
- **Security + Identity:** Azure Active Directory (Free, Basic), Azure Information Protection (including Azure Rights Management), Key Vault

- **Monitoring + Management:** Automation, Azure Resource Manager, Log Analytics, Microsoft Azure Portal, Scheduler
- Azure Supporting Infrastructure Services
- Microsoft Power BI

## 2.4 Azure certifications and attestations

The Azure platform and its underlying physical environments employ a security framework that encompasses industry best practices and spans multiple standards, including the ISO 27000 family of standards, NIST 800, and others. As part of our comprehensive [compliance offering](#), Microsoft Azure regularly undergoes independent audits performed by qualified third-party accredited assessors for ISO (27001, 27017, 27018 & 9001), SOC (1, 2, 3), Health Information Trust Alliance (HITRUST), [US Federal Risk and Authorization Management Program \(FedRAMP\)](#), and Payment Card Industry (PCI).

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

The following table identifies the certifications and attestations that Microsoft Azure 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   |
|--|-----------------|---|
| <b>SOC 1 Type II</b>                   | Quarterly       | <a href="#">Deloitte</a>                            |
| <b>SOC 2 Type II</b>                   | Quarterly       | <a href="#">Deloitte</a>                            |
| <b>FedRAMP (NIST SP 800-53 Rev. 4)</b> | Annually        | <a href="#">Kratos SecureInfo</a>                   |
| <b>ISO/IEC 27001:2013</b>              | Semi-annually   | <a href="#">British Standards Institution (BSI)</a> |
| <b>ISO/IEC 27018:2014</b>              | Semi-annually   | <a href="#">British Standards Institution (BSI)</a> |
| <b>ISO 9001:2015</b>                   | Annually        | <a href="#">Coalfire ISO</a>                        |
| <b>ISO/IEC 20000-1:2011</b>            | Annually        | <a href="#">Coalfire ISO</a>                        |
| <b>HITRUST</b>                         | Annually        | <a href="#">Coalfire</a>                            |



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

**Additional Resources:**

- [Overview of Microsoft Azure Compliance](#)

### 2.4.1 SOC 1 & SOC 2

The Azure platform is audited quarterly according to the [Service Organization Controls \(SOC\)](#) framework developed by the American Institute of Certified Public Accountants (AICPA). Service audits based on the SOC framework fall into two categories—SOC 1 and SOC 2—that apply to in-scope Azure 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). 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 tests to confirm the effectiveness of the controls supporting the trust services criteria, the results of which are included in the SOC audit reports. Any exceptions identified in the audit are addressed by management in the last section of the audit report “Section V: Supplemental Information Provided by Microsoft Azure.”



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

**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. Microsoft SOC 2 audit reports are available to customers on the Trust Center site.

#### 2.4.2 CSA Security, Trust & Assurance Registry (STAR)

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

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



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


- [Microsoft Azure Cloud Controls Matrix \(CCM\)](#)
- [Microsoft Azure Responses to CSA Consensus Assessments Initiative \(CAI\) Questionnaire](#)

#### 2.4.3 FedRAMP

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

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


Microsoft Azure was the first public cloud with infrastructure and platform to earn a Provisional Authority to Operate (P-ATO) from the Joint Authorization Board (JAB). Microsoft also stands apart from other cloud service providers in that we make the FedRAMP System Security Plan (SSP) available to all our customers in the [Service Trust Platform \(STP\)](#).

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

#### 2.4.4 ISO/IEC 27001:2013

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

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

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

**Additional Resources:**


- [13 Effective Security Controls for ISO 27001 Compliance when using Microsoft Azure](#)

#### 2.4.5 ISO/IEC 27018:2014

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

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

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

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

#### 2.4.6 ISO 9001:2015

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

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

- Customer focus
- Leadership commitment to quality objectives
- Employee engagement in the quality goals set by leadership
- Process-driven approach to achieve quality objectives
- Continuous improvement
- Evidence-based decision making
- Customer and partner relationship management

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



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

**Additional Resources:**

- [ISO Quality Management Principles](#)

#### 2.4.7 ISO/IEC 20000-1:2011

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

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



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

**Additional Resources:**

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

#### 2.4.8 HITRUST

The Health Information Trust Alliance (HITRUST) is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework (CSF), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner. The CSF builds on HIPAA and the HITECH Act



and incorporates healthcare-specific security, privacy, and other regulatory requirements from existing frameworks such as the PCI DSS, ISO 27001, and MARS-E.

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

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



The latest Azure HITRUST Letter of Certification is available to customers in the [Service Trust Platform \(STP\)](#).

**Additional Resources:**

- [HITRUST CSF Version 9](#)

## 2.5 Azure Quality Management System

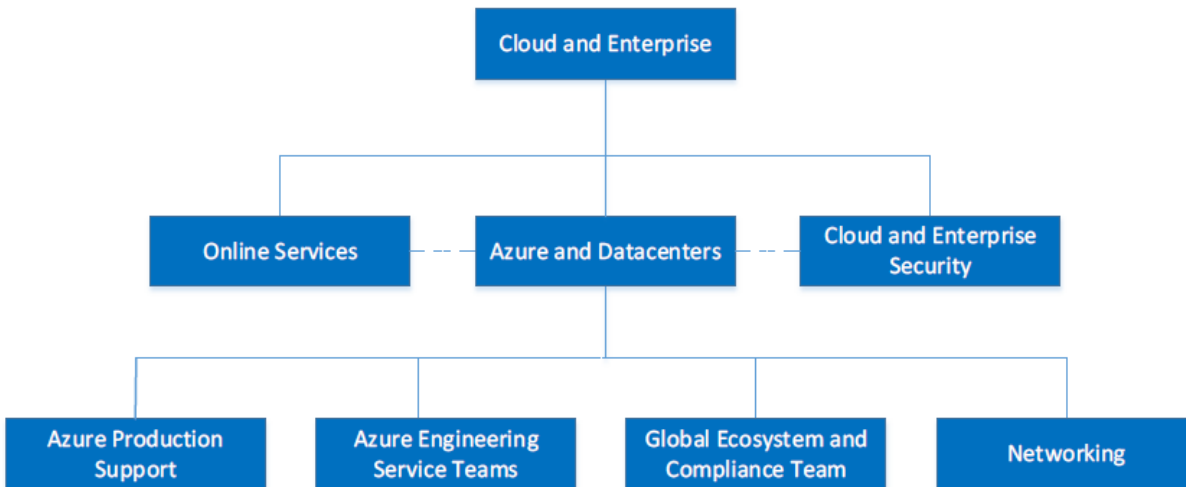
The Global Ecosystem and Compliance Team has established a Quality Manual that identifies the primary objectives of the Microsoft Azure Quality Management System (QMS), which is aligned with the ISO 9001:2015 standard. The Azure QMS governs the core quality practices that deal with the delivery and management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

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

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

### 2.5.1 Roles and responsibilities

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



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

#### *2.5.1.1 Online Services Teams*

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

#### *2.5.1.2 Cloud and Enterprise Security Team*

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

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

#### *2.5.1.3 Azure Production Support Team*

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

- **Azure Live Site:** Monitors and supports the Azure platform; proactively addresses potential platform issues; and reacts to incidents and support requests
- **Azure Deployment Engineering:** Builds out new capacity for the Azure platform and deploys platform and product releases through the release pipeline

- **Azure Customer Support:** Provides support to individual customers and multinational enterprises from basic break-fix support to rapid response support for mission-critical applications

#### 2.5.1.4 *Azure Engineering Service Teams*

---

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

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

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

#### 2.5.1.5 *Global Ecosystem and Compliance Team*

---

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

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

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

#### 2.5.1.6 *Networking Team*

---

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

- Network configuration and access management
- Network problem management
- Network capacity management

### 2.5.2 *Policies and standard operating procedures*

Policies and processes that accompany the Information Security program provide a framework to assess risks to the Azure environment, develop mitigation strategies, and implement security controls.

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



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

### 2.5.3 Microsoft personnel and contractor training

Microsoft Azure has implemented a training program to ensure that personnel and contractors responsible for the Azure platform 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 EMA's 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 Principle - CC1.3. This trust principle stipulates, "The entity has established procedures to evaluate that the competency of personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system...have the qualifications and resources to fulfill their responsibilities." Microsoft adheres to this SOC 2 trust principle and is regularly audited by independent third-party assessors to assess the effectiveness of the related processes and controls.

### 2.5.4 Documented information

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

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

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

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

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

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

### 2.5.5 Design and development of Azure products and services

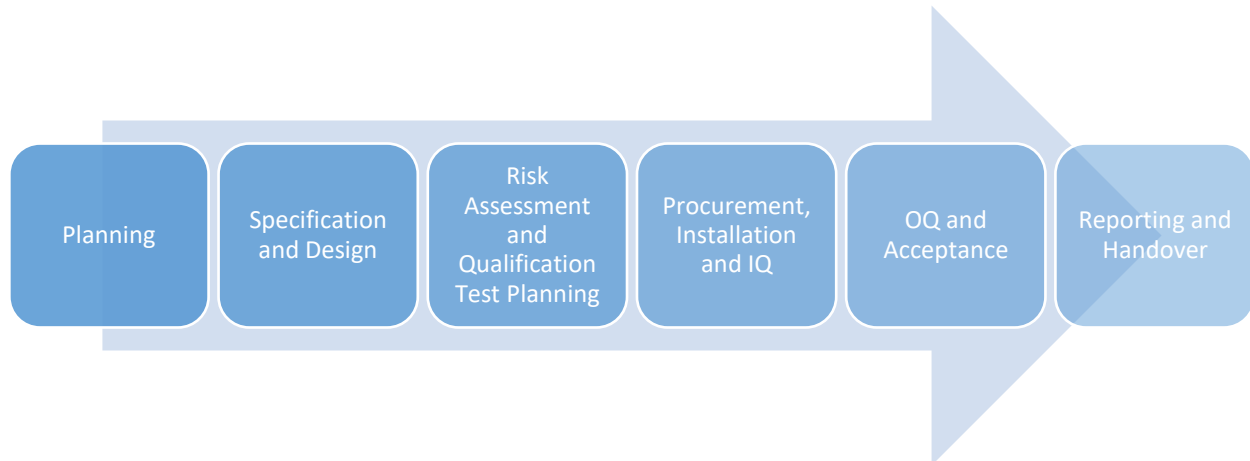
Traditionally, the regulated company has been responsible for all aspects of their IT infrastructure, such as physical security, environmental controls, and server and network management. In contrast, with the cloud service model, the regulated company must rely on cloud vendors to properly manage the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

Microsoft understands that IT infrastructure qualification is an essential aspect of GxP computerized system compliance for the life sciences industry. The ISPE *GAMP Good Practice Guide for IT Infrastructure Control and Compliance (Second edition)* defines qualification as “a process of demonstrating the ability of an entity to fulfill specified requirements. In the context of an IT Infrastructure, this means demonstrating the ability of components such as servers, clients, and peripherals to fulfill the specified requirements for the various platforms regardless of whether they are specific or of a generic nature.” (Ref. [9]). According to the GAMP guidance, the following critical elements should be considered during IT infrastructure qualification:

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

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

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



#### *2.5.5.1 Planning*

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

#### *2.5.5.2 Specification and design*

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

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

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

Microsoft [Operational Security Assurance](#) (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Security Development

Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. OSA defines the aspects of these domains by first establishing baseline requirements that each service should meet or exceed. These baseline requirements are then used to establish a test plan that can be used to validate a service's security during an assessment.

The three key processes of OSA are:

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

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

Physical network diagrams are maintained for all Azure datacenters, with general data flows that provide functional level detail on load balancers, routers, firewalls, and other network infrastructure. Diagrams are stored in a secured location with access restricted to the appropriated individuals.

#### [2.5.5.3 Risk assessment and qualification test planning](#)

---

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

The Risk Management Program consists of six processes:

1. **Establish context:** Setting the context or scope of the risk assessment includes establishing many characteristics before beginning the assessment to ensure appropriate data is collected and evaluated. The type of details captured while determining the assessment context include: the geographical locations of the information assets and equipment; how information is exchanged internally and with external parties; and what legal, regulatory, policy, and contractual requirements apply given the locations involved.
2. **Identify critical assets:** After the risk assessment context has been established, asset owners evaluate which assets are critical and which are not in a process that often reuses analyses conducted for asset management or business continuity planning efforts. The assets considered include:
  - a) **Primary assets:** Business processes, activities, and information
  - b) **Supporting assets:** Hardware, software, network devices, personnel, and facilities

3. **Identify risks:** Workshops or interviews are used to solicit input from asset owners and business managers in teams that support the given scope of the assessment. Also, operational data is evaluated to identify risks.
4. **Assess risks:** The potential business impact and the likelihood of occurrence are investigated in this phase, which also includes looking for and estimating the effectiveness of potential controls that are used to reduce or eliminate the impact of risks.
5. **Report and review risks:** Provide management with the data to make effective business decisions. This phase includes risk determination, including whether to take measures to avoid, reduce, transfer, or accept risks.
6. **Treat and manage risks:** This phase involves identifying accountable risk owners and applying risk treatment plans to those risks that management decided to reduce, transfer, or avoid in the previous phase. Possible treatments include authorizing special projects intended to address those risks.

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

#### *2.5.5.4 Procurement, installation, and IQ*

---

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

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

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

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

The Technical Security Services Team develops security configuration standards for systems in the physical environment that are consistent with industry-accepted hardening standards. These



configurations are documented in system baselines and are reviewed annually, and relevant configuration changes are communicated to affected teams.

#### [2.5.5.5 OQ and acceptance](#)

---

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

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

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

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

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

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

#### [2.5.5.6 Reporting and handover](#)

---

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

### [2.5.6 Operations management](#)

The following sections provide an overview of Microsoft processes and controls corresponding to the topics as recommended within *GAMP Guidance for IT Infrastructure Control and Compliance* (Ref. [9]).

### 2.5.6.1 *Change management*

---

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

The change management process governs the following activities:

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

The Azure teams have implemented a centralized ticketing tool to document changes and their approvals. Change records are kept in accordance with a corporate retention policy.

#### 2.5.6.1.1 *Software and configuration changes*

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

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

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

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

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

#### 2.5.6.1.2 Hardware changes

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

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

#### 2.5.6.1.3 Network changes

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

#### 2.5.6.2 Configuration management

---

Technical standards and baselines have been established and communicated for operating system deployments. Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions and deviations from the baseline in the production environment. Operating system and component teams review and update configuration settings and baseline configurations at least annually.

#### 2.5.6.3 Information security and access management

---

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

The Azure platform is specially designed and architected to prevent the possibility of production data being moved or replicated outside of the Azure cloud environment. These controls include:

- Physical and logical network boundaries with strictly enforced change control policies
- Segregation of duties requiring a business need to access an environment
- Highly restricted physical and logical access to the cloud environment
- Strict controls based on [SDL](#) and [Operational Security Assurance](#) (OSA) that define coding practices, quality testing, and code promotion

- Ongoing security, privacy, and secure coding practices awareness and training
- Continuous logging and audit of system access
- Regular compliance audits to ensure control effectiveness

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

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

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

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

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

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

#### [2.5.6.4 Server management](#)

---

Server management relates to the ability to manage information stored on servers. This function is accomplished through the implementation of various processes to ensure servers are secured (see Section 2.5.6.3) that data is adequately backed up (see Section 2.5.6.9) and sufficient monitoring is performed (see Section 2.5.6.11).

#### 2.5.6.5 Client management

---

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

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

#### 2.5.6.6 Network management

---

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

#### 2.5.6.7 Incident and problem management

---

An incident management framework has been established with defined processes, roles, and responsibilities for the detection, escalation of, and response to incidents. Incident management teams perform 365x24x7 monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. Events, thresholds, and metrics have been defined and configured to detect incidents and alert the appropriate Azure teams. The Azure logging and monitoring infrastructure encompasses the entire Azure platform and does not vary by tenant. Detected incidents are isolated or contained most effectively depending on the nature of the event. Incidents that require a change would then go into the standard change process (which can include emergency changes). Incident records are kept in accordance with a corporate retention policy.

Microsoft Azure has developed robust processes to facilitate a coordinated response to a security incident if one was to occur. A security incident may include, among other things, unauthorized access resulting in loss, disclosure, or alteration of data. Security incident response plans and collection of evidence adheres to ISO/IEC 27001 standards. Azure has also established processes for evidence collection and preservation for troubleshooting incidents and analyzing their root cause. In addition, Azure has established procedures to receive, generate, and disseminate security alerts from external organizations as necessary. The [Security Incident Response Lifecycle](#) consists of the activities described in the following table:

| Phase               | Activity description   |
|---------------------|--|
| <b>1 – Detect</b>   | First indication of an event investigation.  |
| <b>2 - Assess</b>   | An on-call incident response team member assesses the impact and severity of the event. Based on the evidence, the assessment may or may not result in further escalation to the security response team. |
| <b>3 - Diagnose</b> | Security response experts conduct the technical or forensic investigation and identify containment, mitigation, and workaround strategies.   |

|                               |   |
|-------------------------------|---|
|                               | If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, parallel execution of the Customer Incident Notification process begins in parallel.  |
| <b>4 - Stabilize, Recover</b> | The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining affected systems may occur immediately and in parallel with the diagnosis. Longer term mitigations may be planned that occur after the immediate risk has passed. |
| <b>5 - Close/ Post Mortem</b> | The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the incident.   |

*2.5.6.8 Help Desk*

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

*2.5.6.9 Backup, restoration, and archiving*

The backup, restoration, and archiving process defines activities for initiating, applying, monitoring, restoring, and testing the backup process for servers and data. The Data Protection Team has implemented a secure backup system infrastructure to provide secure backup, retention, and restoration of data in the Microsoft Online Services environment.

*2.5.6.10 Disaster recovery*

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

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

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

*2.5.6.11 Performance monitoring*

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

The following operational processes are in place:

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

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

Proactive monitoring continuously measures the performance of critical subsystems of the Microsoft Azure services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event that can be visualized either within the customer's Azure Management Portal – [Service Issues Dashboard](#) or on the [Azure Status Dashboard](#).

#### *2.5.6.12 Supplier management*

---

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

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

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

#### *2.5.6.13 System retirement*

---

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

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

### *2.5.7 Performance evaluation*

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

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

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

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

#### 2.5.8 Improvement

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

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

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

### 3 Recommendations to consider for satisfying GxP requirements

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

By using the Azure platform, the customer is effectively outsourcing the management and operations of the physical infrastructure (that is, datacenter, network, and hosts) to Microsoft. However, as per the GAMP guidance (Ref. [9]), *“the regulated company remains responsible for the regulatory compliance of*



*their IT operations regardless of whether they choose to outsource/offshore some or all of their IT Infrastructure processes to external service provider(s). Compliance oversight and approvals cannot be delegated to the outsource partner.”* It is therefore essential for the regulated user(s) to determine the appropriate validation strategy of their GxP application(s) hosted on the Azure platform.

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

### 3.1 Implementing a cloud strategy and governance model

An important step to achieve and maintain compliance of cloud-based GxP systems is establishing a comprehensive cloud strategy and governance model. Customers should consider integrating the following activities into their operations to help achieve successful governance of their cloud-based applications:

- Identify clear roles and responsibilities for cloud environment based on shared responsibility model
- Establish governance policies and procedures that are aligned to the cloud model
- Train personnel responsible for managing and maintaining cloud-based solutions
- Manage supplier relationships with all third-party service providers and review service agreements
- Identify cloud resources and services using a standardized naming convention to support system inventory and documentation
- Plan validation of cloud-based GxP applications with key stakeholders and subject matter experts
- Implement data backup and restoration processes and perform routine testing
- Ensure integrity of data is maintained when data is at rest and in transit by taking advantage of cryptography and security best practices
- Perform routine monitoring to verify service quality
- Establish continuous improvement activities
- Integrate best practices associated with the following pillars of software quality:
  - **Scalability:** The ability of a system to handle increased load
  - **Availability:** The proportion of time that a system is functional and working
  - **Resiliency:** The ability of a system to recover from failures and continue to function
  - **Management:** Operations processes that keep a system running in production
  - **Security:** Protecting applications and data from threats



#### Additional Resources:

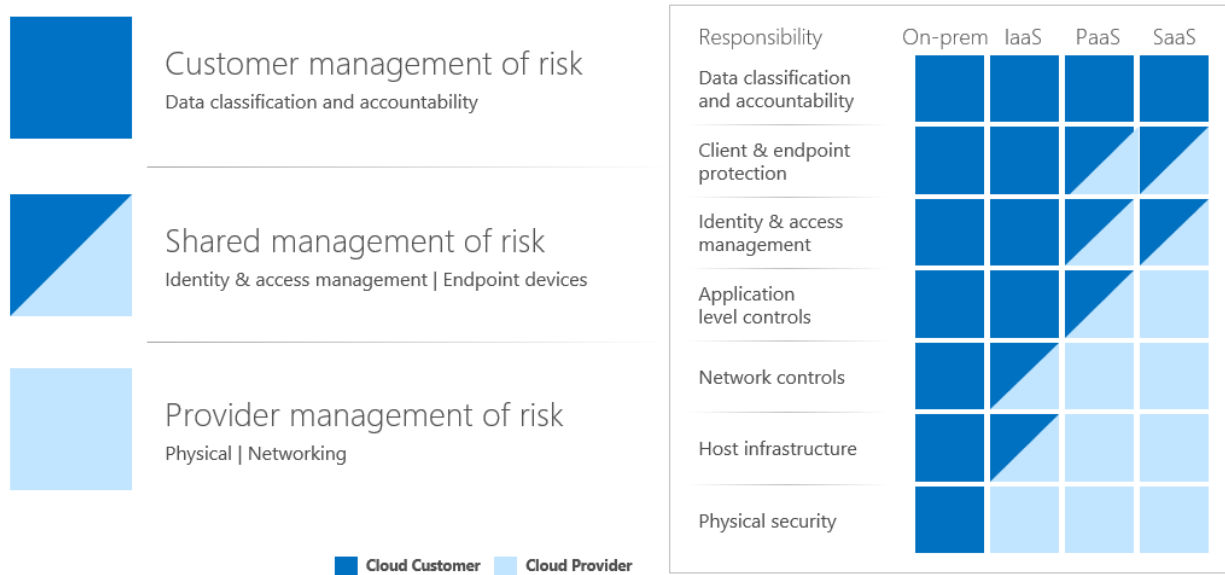
- [ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, 2011](#)

## 3.1.1 Shared responsibilities

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

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

### Shared responsibility



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

The following table describes potential roles and responsibilities that customers may consider when defining their cloud governance responsibilities.

| Role                        | Responsibilities include   |
|-----------------------------|--|
| <b>Cloud Platform Owner</b> | <ul style="list-style-type: none"> <li>Define cloud platform requirements</li> <li>Implement cloud governance strategy</li> <li>Ensure governance processes are followed and service level agreements are met</li> <li>Review impacts and approve changes to cloud platform</li> <li>Conduct periodic reviews to ensure qualified state of cloud environment is maintained</li> <li>Manage budgeting and purchasing of cloud resources and services</li> </ul> |

| Role                                | Responsibilities include   |
|-------------------------------------|--|
| <b>Cloud Platform Administrator</b> | <ul style="list-style-type: none"> <li>• Maintain logical security of cloud platform resources</li> <li>• Implement platform changes in accordance with procedures and specifications</li> <li>• Manage cloud platform users and access to cloud resources</li> <li>• Provide technical support and incident/problem management</li> <li>• Maintain and test backup and recovery processes</li> <li>• Review audit logs and security reports</li> <li>• Monitor status of cloud services and respond to alerts</li> <li>• Manage patches and updates to cloud resources</li> </ul> |



**Additional Resources:**

- Additional information and considerations regarding shared responsibilities can be found in the [Azure - Cloud Security Diagnostic Tool 2016](#)

### 3.1.2 Computerized systems compliance policies and procedures

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

#### 3.1.2.1 Quality governance processes

| Procedure topic                        | Purpose  |
|--|--|
| <b>Training management</b>             | Defines an internal training program to ensure personnel have the competencies required to access and work within the application running on the controlled cloud platform. Additional training requirements may need to be defined for each controlled application within the cloud platform.   |
| <b>Documentation management</b>        | Establishes 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).                           |
| <b>Records retention and archiving</b> | Ensures that all records are managed in conformance with applicable regulations and requirements.  |
| <b>Supplier management</b>             | Defines a formal process to ensure that cloud service providers are identified, assessed, selected, and managed in a formal and controlled manner.   |
| <b>Periodic review</b>                 | Defines 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. |


3.1.2.2 Operational (IT) governance processes

| Procedure topic                              | Purpose   |
|--|---|
| <b>System security</b>                       | Describes the logical security measures for cloud applications systems to protect against unauthorized access to cloud platform administrative console and regulated application components.  |
| <b>Change and configuration management</b>   | Defines a formal process 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. Ensures that all updates to baseline items (configuration items) are controlled and traceable. |
| <b>System monitoring</b>                     | Describes the tools used to monitor the cloud application(s) to ensure consistent availability and performance.   |
| <b>System administration and maintenance</b> | Provides instruction for the technical management and engineering practices to be used in the operation and maintenance of cloud application(s).  |
| <b>User access management</b>                | Describes the management of administrative accounts that enable access or changes to system data. User access management also establishes clear standards for issuing accounts, creating passwords, and managing accounts.  |
| <b>Backup and recovery</b>                   | Defines the strategy for data backup, recovery in the event of disruption, and intentional/unintentional destruction or corruption of data or disaster.   |
| <b>Incident and problem management</b>       | Defines a formal process to ensure that issues are raised, recorded, investigated, and resolved in a formal and controlled manner.  |

3.1.3 Personnel training

Customer personnel may require additional training based on their job function to ensure they have the qualifications needed to develop, deploy, and maintain cloud-based applications within Azure. Application architects, platform owners/administrators, and GxP system owners/administrators who have the responsibility of designing, securing, and managing the controlled environments and maintaining the validated state of the GxP applications may require more in-depth training for the cloud services at their disposal.

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

 **Additional Resources:**

- [Microsoft Virtual Academy – Microsoft Azure Courses](#)

### 3.1.4 Supplier evaluation

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. [21]):

*“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 2.4, Microsoft Azure regularly undergoes independent audits performed by qualified third-party accredited assessors with regard to several ISO, SOC, HITRUST, FedRAMP, and PCI certifications 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 and is aligned with the CSA STAR program criteria (see Section 2.4.2). 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 guidelines 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 Azure has implemented. The analysis also maps to a specific control ID as referenced within the latest SOC 2 report for Microsoft Azure. Because 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.



#### Additional Resources:

- The Cloud Security Alliance (CSA) [Consensus Assessments Initiative Questionnaire \(CAIQ\) v3.0.1](#) provides a comprehensive set of questions that customers can use to evaluate the depth / breadth of cloud vendors’ security, privacy, and compliance processes. Microsoft Azure team has compiled detailed responses to the items in the assessment questionnaire, which is available for [download](#).

- The following features are capabilities customers can review to ensure that the Azure platform is managed securely. Links have been provided for further drill-down on how Microsoft addresses customer trust questions in four areas: **Secure Platform**, **Privacy & Controls**, **Compliance**, and **Transparency**.

| <a href="#">Secure Platform</a>  | <a href="#">Privacy &amp; Controls</a>            | <a href="#">Compliance</a>                                     | <a href="#">Transparency</a>  |
|--|---|--|---|
| <a href="#">Security Development Cycle</a>   | <a href="#">Manage your data all the time</a>     | <a href="#">Trust Center</a>                                   | <a href="#">How Microsoft secures customer data in Azure services</a>     |
| <a href="#">Mandatory security training, background checks</a>                       | <a href="#">Control on data location</a>          | <a href="#">Common Controls Hub</a>                            | <a href="#">How Microsoft manages data location in Azure services</a>     |
| <a href="#">Penetration testing, intrusion detection, DDoS, Audits &amp; logging</a> | <a href="#">Provide data access on your terms</a> | <a href="#">The Cloud Services Due Diligence Checklist</a>     | <a href="#">Who in Microsoft can access your data on what terms</a>       |
| <a href="#">State of art datacenter, Secure Network</a>                              | <a href="#">Responding to law enforcement</a>     | <a href="#">Compliance by service, location &amp; industry</a> | <a href="#">How Microsoft secures customer data in Azure services</a>     |
| <a href="#">Security incident response, Shared Responsibility</a>                    | <a href="#">Stringent privacy standards</a>       |  | <a href="#">Review certification for Azure services, Transparency hub</a> |

### 3.1.5 Service agreements

GxP regulated users of cloud-based systems are expected to have service agreements in place with their service providers, as described in the FDA’s draft [Guidance for Industry](#) (Ref. [21]), as well as the recently released *GAMP Guidance for IT Infrastructure Control and Compliance (Second Edition)* (Ref. [9]).

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

Customers may also refer to [Appendix B](#) for a mapping of the contractual agreements we establish with our customers against the recommended content for service level agreements and quality agreements, as recommended within the GAMP guidance (Ref. [21]).

#### 3.1.5.1 Service level agreements

Each Azure product 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.

#### 3.1.5.2 Online Services Terms

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

- Privacy
- Security
- Asset management
- Human resources security
- Physical and environmental security
- Location of customer data at rest
- Data recovery procedures
- Encryption of data
- Data retention
- Physical access to facilities

- IT security access controls
- Environmental controls
- Security incident notification
- Managing system risks
- Business continuity
- Acceptable use policy
- Compliance with laws
- Retirement of services

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

#### [3.1.5.3 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.

#### [3.1.5.4 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.

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

### 3.1.6 Data integrity

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 draft guidance related to this topic:

- [FDA - Data Integrity and Compliance with CGMP - Guidance for Industry \(April 2016\)](#)
- [MHRA - GxP Data Integrity Definitions and Guidance for Industry \(Draft - July 2016\)](#)
- [WHO - Guidance on Good Data and Record Management Practices \(September 2015\)](#)
- [PIC/S \(PI 041-1\): Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments \(Draft – August 2016\)](#)

Several industry and government 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 Azure is protected by a variety of technologies and processes, including various forms of encryption. Multiple encryption methods, protocols, and algorithms are used to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure (see section 3.3.4 for additional details).

It is a shared responsibility between Azure and Microsoft customers to implement sufficient mechanisms to meet these obligations. Specifically, Microsoft provides a secure, compliant platform for services, applications, and data; customers must design and configure their cloud environment to ensure the [security, confidentiality and integrity](#) of their information assets. Microsoft embeds advanced cryptographic technologies within the Azure platform, which customers can use to ensure data in transit and at rest is encrypted. The customer is responsible for ensuring the GxP computerized systems deployed on the Azure platform are configured to employ encryption mechanisms and to manage encryption keys.

Microsoft customers control the following data protection features within the Azure platform:

- [Cryptography for storing data, in applications, and on the network](#) (encryption and decryption)
- [Key management](#) (provisioning, lifecycle management, security/protection)
- [Authentication, authorization, and access control](#)

These capabilities 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 applications have been designed with proper data integrity controls.

#### *[3.1.6.1 Considerations for GxP applications with FDA 21 CFR Part 11 regulatory impact](#)*

---

Any application that supports GxP processes subject to FDA regulations should be assessed by the customer as to whether it generates or manages (that is, creates, modifies, maintains, archives, retrieves, or distributes) electronic records based on FDA 21 CFR Part 11 [regulations](#) and [guidance](#). The outcome of the assessment and intended use of the application should determine which of the following features and functional capabilities will be incorporated into the application design and validated to ensure proper functionality and data integrity:

- Generation of accurate and complete copies of records (that is, data and associated metadata) in both human readable and electronic form
- Protection of records to enable their accurate and ready retrieval throughout the records retention period
- User access controls to limit system access to authorized individuals
- Secure, computer-generated, time-stamped audit trails to independently record the date and time of user actions that create, modify, or delete electronic records
- Enforcement of permitted sequencing of steps and events (as necessary)
- Data input validity verification (as necessary)
- Encryption of data at rest and in transit

If the GxP application is designed to provide the ability to apply legally binding electronic signatures on electronic records, the verification should also ensure the following functionalities are correctly incorporated into the design of the application:

- Electronic signature manifestations that include:
  - The printed name of the signer
  - The date and time when the signature was executed



- The meaning (such as review, approval, responsibility, or authorship) associated with the signature
- Electronic signature and record linking to ensure records cannot be falsified by ordinary means
- User identification and password controls:
  - Ensuring uniqueness of each combined identification code and password
  - Transaction safeguards to prevent unauthorized use of passwords and/or identification codes
  - Ability to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit

**Additional Resources:**

- [ISPE, GAMP Guide: Records & Data Integrity](#)
- [Introduction to Azure Security](#)
- [Azure Security Best and Encryption Best Practices](#)
- [Encryption in the Microsoft Cloud](#) (available in the Service Trust Portal under Trust Documents → FAQ and White Papers)

### 3.1.7 Operations, maintenance, and monitoring

#### 3.1.7.1 Segregation of duties

---

Customer personnel who are responsible for operations and maintenance activities, such as system administrators, architects, developers, testers, 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](#).

Customers can configure [Azure Active Directory \(AAD\)](#) and [role-based access control \(RBAC\)](#) within Azure Resource Manager to facilitate segregation of duties and least privilege.

**Additional Resources:**

- [Azure Identity Management and access control security best practices](#)
- [Getting started with Microsoft Azure security](#)
- [Azure Security Technical Capabilities](#)

#### 3.1.7.2 Change management

---

Customers may need to adapt their processes with regard to change management to better align with the cloud model. With the cloud model, changes may be performed to the underlying platform infrastructure that are not under customer control. However, this does not imply that changes are out of control. As described in Section 2.5.6.1, Azure engineering teams have implemented robust processes around change management as it relates to implementing software, hardware, and network changes. Azure notifies customers of potential changes and events that may affect security or availability of the services through an online [Service Dashboard](#). The [Online Services Terms](#) also describe 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.

Customers have significant control over their change management strategy when determining which deployment model to use and how their environment is architected. For example, customers who use virtual machines deployed in the IaaS model have complete control over the changes that occur within the virtual machine. By taking advantage of Azure's [High Availability](#) and [Region pairs](#), customers can design their environments to minimize the risks associated with unplanned hardware maintenance events, unexpected hardware faults, and planned maintenance events.

The [Scheduled Events](#) service provides customers with the ability to receive notifications from Azure when planned maintenance activities may affect customers' virtual machines and provides the ability to schedule maintenance windows. (Note: This service as of December 2017 is in Preview. See Section 3.3.16 for additional details.)

With PaaS-based applications, customers are encouraged to use modern change management techniques that involve making changes to their applications that are smaller in scope and impact, but with greater frequency. Change management mechanisms focus on change facilitation driven by the product release pipeline in which mitigation and risk controls, such as automated deployments, automated testing, and mandatory approvals, are engineered into the change operations.

**Additional Resources:**

- [Manage the availability of Windows virtual machines in Azure](#)
- [Modern Service Management for Azure](#)

### *3.1.7.3 System configuration and inventory management*

---

The Azure Management Portal provides an efficient way of managing all the IaaS and PaaS resources within a customer's subscription. Information about each resource, including its configuration, can be viewed directly within the portal. Alternatively, customers may create automated scripts to extract information about deployed resources in Azure using data from the [Azure management APIs](#).

Platform administrators may also use the [resource lock feature](#) to lock a subscription, resource group, or resource to prevent other users in the organization from accidentally deleting or modifying critical resources.

**Additional Resources:**

- [Azure Resource Manager Overview](#)
- [Using Azure Management APIs to get data about your deployed resources](#)


### *3.1.7.4 Data backup, restore, and disaster recovery*

---

Customers must define their data backup strategy based on their data recovery requirements and system architecture. The [Azure Backup](#) and [Recovery Services](#) can be configured to help customers achieve their application-specific backup goals (see Section 3.3.11).

A well-documented plan for application [disaster recovery](#) should be established and tested to ensure recovery from any failure that may affect system availability. Customers should choose a multi-site disaster recovery architecture for any mission-critical applications using as much automation as possible.

Customers should identify a specific owner of the disaster recovery plan who is responsible for maintaining the plan and ensuring its effectiveness. Operations staff should be trained to execute the plan and perform regular disaster simulations to validate and improve the plan.

 **Additional Resources:**

- [Disaster recovery for Azure applications](#)
- [Designing resilient applications for Azure](#)
- [Availability Checklist](#)

*3.1.7.5 Monitoring and logging*

Customers can make use of the numerous monitoring capabilities and services embedded in the Azure platform as part of their operations and maintenance strategy. The following table describes the Azure tools and services that can help customers monitor, audit, and log the state of their cloud environment(s):

|   |  |
|---|--|
| <a href="#">Azure Roadmap</a> and <a href="#">Azure Updates</a> | Keep up-to-date with new features and pending changes to Azure components and services (see Section 3.3.14 for additional details).  |
| <a href="#">Azure Monitor</a>                                   | <ul style="list-style-type: none"> <li>• <a href="#">View activity logs</a> that provide insight into change events taken on the resources in the subscription, allowing customers to determine the what, who, and when for any write operations.</li> <li>• Monitor system performance and use monitoring data to trigger alerts or processes (see Section 3.3.15 for additional details).</li> </ul> |
| <a href="#">Azure Logic Apps</a>                                | Develop workflows that perform automated regression testing (see Section 3.3.13 for additional details).   |
| <a href="#">Azure Automation</a>                                | Use <a href="#">update management</a> to manage updates and patches for virtual machines (see Section 3.3.12 for additional details).  |

*3.1.7.6 Data retention*

Customers are responsible for determining their recordkeeping requirements based on internal policies and regulatory requirements. Customer data stored within the customer’s IaaS and PaaS 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 with regard to the protection of customer data retained within the Azure platform are also described in the OST.

Special consideration may be needed to handle the data generated by Azure activity logs, monitoring tools, and security reports, which retain collected data for various [retention periods](#). The data collected and the period it is retained within the Azure reporting tools depends on the type of report and subscription or service edition selected, as well as when the logging service is enabled. For example, Azure Active Directory reporting consists of the following components:

- [Security Reports](#)
  - **Risky sign-ins:** A risky sign-in is an indicator for a sign-in attempt that might have been performed by someone who is not the legitimate owner of a user account.
  - **Users flagged for risk:** A risky user is an indicator for a user account that might have been compromised.
- [Activity Reports](#)
  - **Sign-in activities:** Information about the usage of managed applications and user sign-in activities.
  - **Audit logs:** System activity information about users and group management, managed applications, and directory activities.

In addition to the Azure Management Portal user interface, Azure Active Directory reporting provides [programmatic access](#) to the reporting data through a set of REST-based APIs. These APIs can be called from a variety of programming languages and tools to automatically extract report data. The exported data may be stored within Azure Storage or any other data repository (for example, Event Hubs) for as long as is deemed necessary. A good practice is to use a storage account or Event Hubs namespace that is not in the same subscription as the one emitting logs to provide additional protection.

**Additional Resources:**

- [Security management in Azure](#)
- [Overview of Azure Monitor](#)

### 3.2 Qualification and validation considerations for cloud-based GxP applications

As with on-premises GxP applications, the approach to validation of a cloud-based GxP application should be based on a *“justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity.”* (Ref. [18]). The regulated user should determine the appropriate validation strategy, considering risk, intended use, and regulatory compliance requirements associated with the GxP application.

The ISPE’s *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems* (Ref. [8]) defines computerized system validation as, *“achieving and maintaining compliance with applicable GxP regulations and fitness for intended use by:*

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

The underlying infrastructure platform supporting the GxP application should also be verified or qualified to demonstrate proper configuration and to ensure a state of control and compliance is maintained.

As described in Section 2.5, the Azure teams have 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 Azure ISO and SOC certification and attestation processes, as described in Section 2.4, help to ensure the people, processes, and technology that make up the Azure environment work together to maintain a state of control and compliance.

### 3.2.1 GAMP categories

The ISPE GAMP 5 guidance provides recommendations on how to analyze and categorize software and hardware components of a GxP system so that these categories can be used along with a risk assessment and supplier assessment to determine a suitable system lifecycle strategy.

The Azure platform may be considered as a combination of the following GAMP 5 software and hardware categories:

- Hardware Category 1 – Standard Hardware Components: Standard hardware components that are not custom-built.
- Hardware Category 2 – Custom-Built Hardware Components: Custom-built hardware components, designed to address specific business needs.
- Software Category 1 – Infrastructure Software: Infrastructure software components linked together within a unified environment that allows the installation and management of applications and services. This category contains two types of software:
  - Established or commercially available layered software (for example, operating systems, database managers, programming languages, and so on)
  - Infrastructure software tools (for example, network monitoring software, batch job scheduling tools, security software, antivirus, and configuration management tools)

An IaaS-based GxP application installed within a customer's virtualized environment could be considered a Category 3 (Non-Configured Product), Category 4 (Configured Product), or Category 5 (Custom Application), depending on the novelty and complexity of the application.

GxP applications built by customers using Azure PaaS cloud services to support regulated GxP processes would typically be considered Category 5 (Custom Application).

Because the Azure platform is not purposely built for any specific GxP application, the regulated user (customer) should verify that the underlying platform components are appropriately designed or configured to meet the requirements of the application.

The following sections discuss various activities and deliverables that GxP-regulated customers may adapt during their cloud-based GxP application qualification and validation efforts. 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. Customers should choose the appropriate development methodology (for example [Waterfall](#) or [Agile](#)), that best suits their project needs and results in an application that meets the necessary quality objectives and is fit for its intended use. In all cases, 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: IT Infrastructure Control and Compliance \(Second Edition\)](#)
- [PIC/S - Good Practices for Computerised Systems in Regulated “GxP” Environments](#)

### 3.2.2 Qualification considerations of infrastructure components and services (Platform qualification)

The infrastructure qualification lifecycle, as defined within the *GAMP Good Practice Guide for IT Infrastructure Control and Compliance* (Ref. [9]), provides a starting point from which life sciences customers may adapt their approach to qualifying the virtual infrastructure components and resources used to support their GxP application(s).

#### 3.2.2.1 Planning

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

##### Recommended deliverable(s):

- **Qualification plan:** The qualification plan defines the project scope, risk rationale, and the qualification approach. The qualification approach will likely depend on whether the infrastructure platform requirements are independent of any specific applications or whether they are mainly derived from application specifications on a case-by-case basis.

The qualification plan should also list the deliverables to be produced, roles and responsibilities, and overall project acceptance criteria.

#### 3.2.2.2 Specification and design

Specification documentation for platform components, including requirements specifications, architecture diagrams, and technical design specifications, should be developed and maintained by the system owners and/or platform administrators and maintained as quality records.

##### 3.2.2.2.1 Requirements specifications considerations:

Infrastructure requirements gathered through collaboration with various application stakeholders, platform owners/administrators, and business application owners are crucial for defining a system’s resource needs. In addition, any regulatory requirements that may have an impact on the architecture supporting the GxP application should also be identified.

The following factors should be considered when establishing the requirements of the underlying platform architecture to help ensure a successful implementation:

- Security and privacy
- Capacity

- Performance
- Availability
- Backup and recovery
- Maintenance (patching)
- Monitoring (auditing and logging)
- Regulations

Customers should be aware of local legislation with regard to 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 when enforcement begins May 25, 2018. GDPR-related assurances are provided in our [contractual commitments](#) (see Section 3.3.17 for additional information).

#### 3.2.2.2.2 Technical design considerations:

System architects and individuals responsible for driving infrastructure design decisions should consider the following factors during the planning, specification, and design phase:

- Ensure data is secured by configuring available [encryption](#) features within Azure for data at rest and in transit.
- Use [high availability](#) architecture to reduce impact of planned and unplanned maintenance.
- Decide in which [geographical location](#) the system will reside.
- Use Azure [logging and auditing](#) mechanisms to capture critical events and define [log archiving rules](#) based on data retention requirements.
- Establish data [backup and recovery](#) strategy based on recovery time objectives (RTO) and recovery point objectives (RPO).
- Decide whether separate development, test, staging, and production environments will be needed and establish proper architecture to ensure [data isolation](#).
- Understand options for [scaling up or scaling out](#).
- Determine whether [data partitioning](#) will be required.
- Be aware of the service limits, quotas, and constraints when implementing a cloud-based solution to ensure appropriate design and architecture decisions are made. To help make these design decisions, Microsoft routinely updates its [list of cloud service limits](#) as new services are added or enhanced within the Azure platform.

Customers may take advantage of the [Azure Reference Architectures](#), which include recommended practices along with considerations for scalability, availability, manageability, and security.

#### Recommended deliverable(s):

- **Requirements specification:** The requirements specification defines how a system should function to satisfy business needs and comply with applicable regulations.

- **System architecture / network diagram:** The system architecture / network diagram provides an overview of the system architecture, including all virtual infrastructure components of the customer's Azure environment. It forms the baseline against which the system design and configuration parameters will be established.
- **Technical design specification:** The technical design specification explains how the virtual infrastructure components are built and/or configured according to the requirements. Customers may need to include the specifications for the following infrastructure components (as required):
  - Azure Active Directory and Multi-Factor Authentication
  - Virtual networks and addressing
  - Virtual and local gateways
  - Storage accounts
  - Virtual machines
  - Load balancer and endpoints
  - Backup and recovery services
  - VPN gateway configuration

**Additional Resources:**

- [Availability Checklist](#)
- [DevOps Checklist](#)
- [Resiliency Checklist](#)
- [Scalability Checklist](#)
- [Solution architecture: Dev-Test deployment for testing IaaS solutions](#)
- [Design principles for Azure applications](#)
- [EU General Data Protection Regulation \(GDPR\) Compliance with Azure FAQ](#)

### 3.2.2.3 Risk assessment and qualification test planning

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 ISPE GAMP 5 framework provides guidance on how to conduct risk assessments to identify potential hazards and prioritize risk mitigation activities.

To help build resiliency into a system, customers may perform a failure mode analysis (FMEA) to identify possible failure points in the system. A standard FMEA process consists of the following activities:

1. Identify all critical components in the system. Include external dependencies, such as identity providers, third-party services, and so on.
2. For each component, identify potential failures that could occur. A single component may have more than one failure mode.
3. Rate each failure mode according to its overall risk. Consider these factors:
  - What is the likelihood of the failure?
  - How detectable is the failure?



- What is the impact on the application with regard to availability, data loss, and business disruption?
4. For each failure mode, determine how the application will respond and recover.

According to the *GAMP Good Practice Guide for IT Infrastructure Control and Compliance (Second edition)* (Ref. [9]), the following controls may be appropriate to mitigate any identified risks:

- Testing
- Redesign, including incorporation of high availability options
- The deployment of various automatic performance, diagnostic, alarm, and security monitoring tools, which greatly reduces the likelihood of undetected harm
- Updated or new policies, guidelines, and instructions
- Extra education or training
- Supplier assessments and management
- Contractual agreements (for example, SLAs)
- Identification of new or updated roles and responsibilities
- Provision of extra staff, facilities, tools, and office space
- Provision of an alternate XaaS supplier
- Data replication, storage redundancy, and mirroring
- Design reviews
- Procedures
- Clustering at the operating system or application level

The outcome of the risk assessment should help customers focus the scope of qualification testing.

#### Recommended Deliverable(s):

- **Risk assessment:** The risk assessment identifies potential hazards and risks associated with hosting GxP applications in the cloud. The risk assessment also describes mitigation strategies designed to reduce the overall risk level.



#### Additional Resources:

- [Azure - Cloud Security Diagnostic Tool 2016](#) (available in the Service Trust Platform (STP) under Trust Documents → Compliance Guides)
- [Microsoft Cloud - NIST Risk Assessment Checklist](#) (available in the Service Trust Platform (STP) under Trust Documents → Compliance Guides)
- [Microsoft Cloud Security for Enterprise Architects](#)

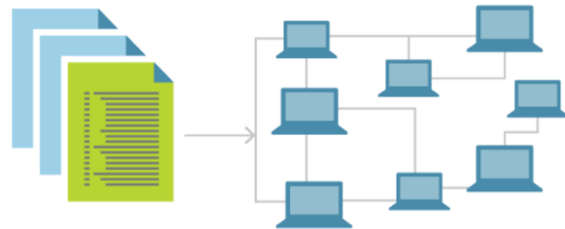
#### 3.2.2.4 *Deployment and qualification testing*

With traditional on-premises installations, the infrastructure procurement and installation process can be laborious and time-consuming, often causing significant project delays if not planned well in advance. These processes are more straightforward to manage when dealing with cloud-based technology, where components and services can be deployed and provisioned in a matter of minutes as opposed to weeks or months.

Customers can provision the IaaS resources they need, such as virtual machines (VM), storage accounts, and virtual network components, on demand. A series of predefined virtual machines are available in the Azure marketplace, which can be rapidly deployed and configured to meet specific requirements. Alternatively, customers can create their own [VM Images](#) to deploy VMs with preloaded applications and configurations in a consistent and repeatable manner. Together with the building-block approach to qualification as defined by GAMP, life sciences customers can create reusable building blocks for deploying infrastructure components with increased consistency and efficiency versus traditional one-off qualification methodologies.

A key benefit of using [Azure Resource Manager](#) is the ability to codify virtual infrastructure components, including networks, virtual machines, load balancers, and connection topology, using what is commonly referred to as [Infrastructure as Code](#) (IaC). IaC is a process of managing and provisioning computing infrastructure in a descriptive model by setting the configuration using definition files instead of traditional interactive configuration tools. The advantages of using IaC include the ability to:

- Consistently achieve standardized provisioning or deployment
- Rapidly accelerate provisioning or deployment
- Build reusable code for repeatable or similar provisioning or deployment
- Build extensible code for incorporating additional items



After adequately verifying the controlled IaC configurations files, these system infrastructure templates can be rapidly deployed creating as many prequalified instances as needed. With proper IaC management, customers can improve uniformity between their development, test, and production environments whose configurations tend to drift over time in traditional deployment models. A good practice for customers developing their own GxP application(s) is to store the infrastructure as code with the source code of the application to ensure the application is version controlled along with the infrastructure upon which it depends. Using this technique, development teams can also test applications in production-like environments early in the development cycle.

To facilitate the deployment and maintenance of certain Azure Resource Manager templates, customers may use [Azure Building Blocks](#). With Azure Building Blocks, developers only need to specify parameter settings for the resources they wish to deploy. These parameter settings are then merged with best practice defaults when deployed.

Azure Resource Manager provides visibility into the status of the [deployment operations](#), either directly within the Azure Management Portal or via automated scripts using [PowerShell](#), [Azure CLI](#), or [REST](#). Infrastructure build processes may be fully automated and designed to automatically flag and log errors or problems that may have occurred. This capability can significantly reduce the time required to implement and qualify infrastructure components while increasing overall quality by ensuring resources are deployed in a consistent state.

After infrastructure resources are deployed and configured, customers can proceed with the deployment and configuration verification, or installation qualification (IQ), to ensure key configuration settings match the documented specification. Scripts can also be used to collect information about deployed resources in Azure using data from the [Azure management APIs](#), and convert the information into a report-friendly format such as a CSV file or another format suitable for reporting.

Based on the output of the risk assessment, customers may also perform functional tests, or operational qualification (OQ), against predefined acceptance criteria to verify that critical infrastructure components function as expected.

**Recommended deliverable(s):**

- **Configuration verification/installation qualification (IQ):** The goal of configuration verification is to produce documented evidence that the customer's Azure platform components are installed and configured according to specifications.
- **Functional verification/operational qualification (OQ):** The goal of the functional verification is to produce objective and documented evidence that the configured platform components function according to specifications.
- **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 qualification testing, procedural controls, audits/assessments, and contractual agreements that serve to ensure the requirements are satisfied. The traceability matrix can be developed as a standalone document or embedded into other deliverables, such as risk assessments, test scripts, and system specifications.

**Additional Resources:**

- [Azure Resource Manager Overview](#)
- [Best practices for creating Azure Resource Manager templates](#)
- [Using Azure Management APIs to get data about your deployed resources](#)
- [Azure Management API IaaS VM Inventory Sample Scripts](#)

### 3.2.2.5 Reporting and handover

Upon completion of the verification activities, the test results should be summarized and the overall acceptance criteria confirmed within a summary report. Infrastructure owners and administrators should follow established governance policies and procedures as defined in Section 3.1.2 to maintain the qualified state of their cloud environment.

Successful completion of the infrastructure qualification activities is typically the stage gate to begin GxP application validation activities, which should be based on the regulated user's validation processes.

**Recommended deliverable(s):**

- **Qualification summary report:** The qualification summary report summarizes the entire qualification effort and confirms that all deliverables required by the approved qualification

plan have are complete. The qualification summary report would include a summary of testing results obtained during IQ and OQ test execution.

### 3.2.3 Validation considerations for PaaS-based GxP applications

Customers should perform a risk assessment to determine the extent to which their GxP applications built using PaaS services need to be validated. Custom-developed GxP applications are typically classified as Category 5 (Custom Applications) under ISPE GAMP 5 and may require additional testing based on the complexity and risk of the application.

Azure PaaS services such as [Azure Cloud Services](#) and [Azure App Service \(Web Apps\)](#) provide application developers a framework they can build upon to develop their GxP applications while simplifying development, testing, and deployment. Applications built using the [PaaS](#) model inherit cloud characteristics, such as scalability and high availability, by taking advantage of built-in automated server maintenance and auto-scaling of compute resources. In the PaaS model, customers are no longer responsible for maintenance of infrastructure components, including operating system patching, because Microsoft Azure automatically performs updates to the underlying platform components and services.

Azure teams have established robust procedures to evaluate, test, and implement patches to Azure service components. Risks associated with the fact that customers do not control the update process can be mitigated by following Azure [resiliency](#) design and architecture recommendations. Customers can also use the [Paired Region](#) feature, which ensures system updates are rolled out to paired regions sequentially to minimize downtime, the effect of bugs, and logical failures in the rare event of a faulty update.

Development of PaaS-based GxP applications should follow a robust security model and quality practices throughout the various lifecycle phases, including planning, development, deployment, and monitoring. Application developers may choose to follow an [Agile](#) development methodology, which when coupled with the [DevOps](#) practice helps to ensure operations and development personnel participate together throughout the entire service lifecycle, from design through the development process to production support.

The FDA recognized the use of Agile development methodology in the context of medical device development when it added the Association for the Advancement of Medical Instrumentation (AAMI)'s TIR45:2012, "[Guidance on the use of Agile practices in the development of medical device software](#)" to its list of [recognized standards](#). AAMI's guidance provides recommendations for compliance with FDA regulations, guidance documents, as well as international standards when using Agile practices to develop medical device software. The guidance also provides a thorough analysis of how to satisfy the expectations surrounding documentation throughout the product lifecycle stages.

One of the key characteristics of the Agile and DevOps methodologies is [test-driven development](#) in which automated tests are written before the functionality that is to be tested. These automated tests drive the design of software and help to ensure the application satisfies the requirements. The result of

using this practice is a comprehensive set of test scripts that can be run at any time to provide feedback that the application is still functioning as intended.

Azure [DevTest Labs](#) is a service that developers can use to simplify testing through rapid provisioning and deprovisioning of test resources. Test environments can be created using templates and reusable artifacts to closely match the production environment.

For larger, more complex applications that require a rapid release velocity and need to be highly scalable, the [Azure Service Fabric](#) and [Azure Container Service](#) offer clear advantages when compared to traditional on-premises application deployment.

Microsoft offers a wide range of tools and services to support DevOps work for continuous integration (CI) and delivery (CD). The following infrastructure automation tools are supported within Azure:

- VM configuration automation
  - Tools include [Ansible](#), [Chef](#), and [Puppet](#)
  - Tools specific to VM customization include [cloud-init](#) for Linux VMs, [PowerShell Desired State Configuration \(DSC\)](#), and the [Azure Custom Script Extension](#) for all Azure VMs
- Infrastructure management automation
  - Tools include [Packer](#) to automate custom VM image builds, and [Terraform](#) to automate the infrastructure build process
  - [Azure Automation](#) can perform actions across the customers Azure and on-premises infrastructure
- Application deployment and delivery automation
  - Examples include [Visual Studio Team Services](#) and [Jenkins](#)

The scripts used during the automated DevOps processes can also serve as a form of documentation. The information they contain about system, server, and software configuration can serve as a detailed design for the controlled environment. When combined with the deployment status logs, which form time-stamped records of individual deployments, these artifacts can be used as part of the GxP application qualification test reports to show historical deployment statistics.

Continuous [monitoring and diagnostics](#) is another crucial part of maintaining quality-of-service targets for PaaS-based applications. Built-in diagnostic logs provide the ability to monitor key performance metrics and helps with application troubleshooting by using [Azure Cloud Services](#) and [Azure App Service](#). Customers can use [Azure Monitor](#) to gain insights into how well a system is functioning. Common scenarios for collecting monitoring data include:

- Ensuring that the system remains healthy and in a state of control
- Tracking the availability of the system and its component elements
- Maintaining performance to ensure that the throughput of the system does not degrade unexpectedly as the volume of work increases
- Confirming that the system meets any service level agreements (SLAs) established with customers
- Protecting the privacy and security of the system, users, and their data
- Tracking the operations that are performed for auditing or regulatory purposes

- Monitoring the day-to-day usage of the system and spotting trends that might lead to problems if they're not addressed
- Tracking issues that occur, from initial report through to analysis of possible causes, rectification, consequent software updates, and deployment
- Tracing operations and debugging software releases

**Additional Resources:**

- [Securing PaaS deployments](#)
- [Overview of Azure Monitor](#)
- [Collect and consume log data from your Azure resources](#)
- [Solution architecture: Dev-Test deployment for testing PaaS solutions](#)
- [Run a web application in multiple regions](#)

### 3.3 GxP-relevant products and service features within Azure

#### 3.3.1 High availability

High availability is an important feature of the Azure platform, because it could be used as part of the customer's risk-based qualification strategy for mitigating risks that deal with the management of underlying infrastructure hardware.

Microsoft defines a highly available application as one that absorbs fluctuations in availability, load, and temporary failures in the dependent services and hardware. The application continues to operate at an acceptable user and systemic response level as defined by business requirements or application service level agreements. Depending on the service model being used, IaaS or PaaS, Azure offers several features via the Azure Fabric Controller to provide high availability of its services.

When using one of the Azure IaaS/PaaS cloud services, the Fabric Controller verifies the status of the hardware and software of the host and guest machine instances. When it detects a failure, it enforces SLAs by automatically relocating the compute instances. When multiple role instances are deployed, Azure relocates these instances to different fault domains, which are essentially different hardware racks in the same data center. Fault domains reduce the probability that a localized hardware failure will interrupt the service of an application.

To achieve high availability with virtual machines (VMs) that are provisioned as part of the Azure IaaS service model, the VMs must be configured to use availability sets. Within an availability set, Azure positions the virtual machines in a way that prevents localized hardware faults and maintenance activities from bringing down all the machines in that group. Putting two or more VMs in availability sets guarantees that the VMs are spread across multiple racks in the Azure datacenters, which means they will have redundant power supplies, switches, and servers. Grouping VMs in availability sets also provides the Azure Fabric Controller with the information it needs to intelligently update the host operating system that the guest VMs are running on so that they are not updated at the same time.

When a system is configured for high availability, the Azure Fabric Controller effectively renders the hardware into a commodity and minimizes the risk associated with physical machine failure whether it is caused by faulty hardware, improper installation, or as result of a change to infrastructure.

### 3.3.2 Local and geographic redundancy

Azure Storage provides data redundancy to minimize disruptions to the availability of customer data. Data redundancy is achieved through fragmentation of data into extents, which are copied onto multiple nodes within a region. This approach minimizes the impact of isolated storage node failures and loss of data. Azure Storage maintains three replicas of customer data in blobs, tables, queues, files, and disks across three separate fault domains in the primary region. Customers can choose to enable geo-redundant storage, in which case three additional replicas of that same data will be kept across separate fault domains in the paired region within the same geography. Examples of Azure Regions are North Central US, South Central US, North Europe, and West Europe. These regions are separated by several hundred kilometers. Geo-replication provides additional data durability in case of a region-wide disaster.

Azure SQL Databases have a minimum of three replicas of each database – one primary and two secondary replicas. If any component fails on the primary replica, Azure SQL Database detects the failure and fails over to the secondary replica. In case of a physical loss of the replica, Azure SQL Database creates a new replica automatically.

All critical platform metadata is backed up to an alternate region, several hundred kilometers from the primary copy. Backup methods vary by service and include Azure Storage geo-replication, Azure SQL Database geo-replication, service-specific backup processes, and backup to tape.

### 3.3.3 Ability to specify geographic location of data

Azure provides customers the ability to choose from a wide range of datacenters and their respective locations. A datacenter can be chosen based on [location](#), [compliance needs](#), [service availability](#), [data residency and sovereignty](#), and [pricing](#).

Depending on the location of the customer, certain regulations may apply with regard to data protection or patient data privacy. These regulations may require the data to be secured in a datacenter that complies with these high standards.

### 3.3.4 Customer data isolation

Microsoft works continuously to ensure that the multi-tenant architecture of Microsoft Azure supports security, confidentiality, privacy, integrity, and availability standards. The Azure platform is designed to support multiple levels of [data isolation](#) to protect against both malicious and non-malicious users, which include:

- [Tenant level isolation](#)
- [Compute isolation](#)
- [Storage isolation](#)
- [SQL Azure Database isolation](#)
- [Networking isolation](#)

### 3.3.5 Encryption of data in transit and at rest

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

For data in transit, Azure uses industry-standard secure transport protocols, such as TLS/SSL, between user devices and Microsoft datacenters. Encryption can be enabled for traffic between a customer's virtual machines (VMs) and the users. With Azure Virtual Networks, the industry-standard IPsec protocol can be used to encrypt traffic between corporate VPN gateway and Azure, as well as between the VMs located on the Virtual Network.

For data at rest, Azure offers encryption options such as AES-256, which provides the flexibility to choose the data storage scenario that best meets customer needs. When enabled, [Azure Storage automatically encrypts](#) data before persisting to storage and decrypts before retrieval. [Azure Disk Encryption](#) allows IaaS virtual machine disks to be encrypted using industry-standard encryption technology to address organizational security and compliance requirements.

### 3.3.6 Azure Key Vault

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

### 3.3.7 Azure Rights Management Services

[Azure Rights Management Services \(RMS\)](#) is a comprehensive toolkit that includes an SDK for developers, ready-to-use applications for information workers, and management tools for IT administrators. RMS enables an organization to:

- Encrypt and decrypt data
- Manage, distribute, and track the distribution of encryption keys
- Enforce who can receive keys, and what they can do with the decrypted data

Data must often be shared across applications, computers, devices, users, and organizations, and often flows from sender to receiver in multiple hops. In the RMS model, encryption and access policies travel with the data.

### 3.3.8 Azure Resource Manager

The [Azure Resource Manager](#) provides the ability to deploy, manage, and monitor all the resources within a solution and provides access to the activity logs. It also provides the ability to deploy and manage Azure Resource Management templates to help ensure that resources are deployed consistently.

Azure Resource Manager natively integrates role-based access control (RBAC) into the management platform and provides fine-grained access control to all services in a resource group. Using RBAC, customers can enable segregation of duties and self-service management of cloud resources for project teams while retaining central control over security-sensitive infrastructure.

Resource Manager also logs all operations that create, modify, or delete a resource. Customers can use activity logs to find an error when troubleshooting or to monitor how a user within the organization modified a resource.



### 3.3.9 Virtual machine scale sets

[Virtual machine scale sets](#) are an Azure compute resource that provides the ability to deploy and manage a set of identical VMs. With all VMs configured the same, scale sets are designed to support auto-scaling, and no pre-provisioning of VMs is required. For applications that need to scale compute resources out and in, scale operations are implicitly balanced across fault and update domains.

Customers can use Azure virtual machine scale sets to ensure their GxP applications always have sufficient computing resources available to support capacity and performance requirements. This availability is crucial to ensuring the applications operate consistently and reliably.

### 3.3.10 Azure Active Directory and Azure AD Connect

[Azure Active Directory](#) provides identity management and access control for cloud applications. These functions simplify user access to cloud applications, where customers can synchronize user accounts with on-premises identities and enable single sign-on. Azure provides the ability to require [multi-factor authentication](#) as a means of further enhancing security around user access to the platform infrastructure, services, and data.

Limiting system access to authorized individuals is an essential requirement for GxP-regulated applications. Using Azure Active Directory facilitates user access management and multi-factor authentication provides an extra control against misuse by unauthorized access.

### 3.3.11 Azure Backup service and recovery

[Azure Backup](#) is the Azure-based service used to back up and restore data in the Microsoft cloud. Azure Backup can replace existing on-premises or off-site backup solutions with a cloud-based solution. Azure Backup offers multiple components that can be downloaded and deployed on the appropriate computer, server, or in the cloud. The specific component, or agent, that is deployed depends on what to protect. All Azure Backup components can be used to back up data to a Recovery Services vault in Azure.

When backing up an Azure VM, Azure Backup relies on encryption of the virtual machine. For example, if the VM is encrypted using Azure Disk Encryption, or some other encryption technology, Azure Backup uses that encryption to secure the data. All the data that is backed up from Azure Backup Agent or Azure Backup Server is compressed and encrypted before being transferred over a secure HTTPS link. Data sent to Azure Backup remains encrypted at rest.

Ensuring proper data protection through verified backup and recovery processes is a crucial aspect of GxP regulations. With the proper use of Azure Backup, the integrity and accuracy of backup data can be established. Nevertheless, it is vital for the customer to establish the specific backup strategy and perform periodic monitoring and recovery testing to satisfy disaster recovery requirements, as well as data integrity requirements with regard to data retention.

### 3.3.12 Azure Automation

[Azure Automation](#) uses Windows PowerShell scripts and workflows, known as [runbooks](#), to help the user automate the creation, deployment, monitoring, and maintenance of Azure resources and partner applications. The Azure Automation Runbook Gallery provides the user with samples, utilities, and scenario runbooks.

Azure Automation provides the ability to automatically deploy and maintain a predefined system configuration.

### 3.3.13 Azure Logic Apps

The [Logic Apps](#) service offers a way to simplify and implement scalable integrations and workflows in the cloud. The service provides a visual designer to model and automate a process as a series of steps known as a workflow. There are many connectors across the cloud and on-premises to quickly integrate across services and protocols. A logic app begins with a trigger and after firing can begin many combinations of actions, conversions, and condition logic.

Azure Logic Apps can create workflows, which control, for example, the creation of users and can implement necessary controls or action coupled to this creation. If a specific workflow has been validated and is kept under control by the customer, it can help to ensure a compliant state of the user base.

### 3.3.14 Azure Roadmap and updates

The [Azure Roadmap](#) service provides visibility into new features being developed for the Azure platform. Customers can subscribe their RSS feed to receive automatic notifications to always be informed of pending updates. Product updates are announced on the Azure Roadmap and are rolled out frequently to ensure the state-of-the-art security of Azure and provide the user with an improved product. Administrators of GxP-regulated application can use the Azure Roadmap to assess feature updates and determine their potential impact.

### 3.3.15 Cloud monitoring

The following cloud services provide the ability to [monitor](#), analyze, and receive alerts about critical system operating and performance parameters:

- [Azure Status](#): Provides the current Azure health status and a summary of past incidents
- [Application Insights](#): Enables application performance management and interactive data analytics
- [Log Analytics \(Operations Management Suite\)](#): Enables the routing of Activity and Diagnostic Logs to Log Analytics. Operations Management Suite allows metric, log, and other alert types.
- [Azure Monitor](#): Enables alerts based on both metric values and activity log events, which can also be managed using the Azure Monitor REST API.

### 3.3.16 Azure Metadata Service - Scheduled Events (Preview)<sup>1</sup>

[Scheduled Events](#) is a sub-service that provides users with advanced information regarding upcoming events that may affect their Azure Virtual Machines. Scheduled Events provides Azure Virtual Machines with sufficient time to perform preventive tasks to minimize the effect of such events. The [use cases](#) for scheduled events include:

---

<sup>1</sup> Azure Metadata Service – As of the initial publication of this paper, Scheduled Events is under “Preview Release.” Previews are not included in the SLA for the corresponding Online Service, however this is included herein because the Scheduled Events service is due for General Availability release in the coming months.

- **Proactive failover:** Instead of waiting for the application, load balancer, or traffic manager to sense that something went wrong, the system can proactively failover to another node. In some cases, knowing that a VM will be running soon can help the application logic to start, accumulate, and log changes rather than failover a partition/replica.
- **Drain a node:** Instead of failing running jobs, the system can block the VM from accepting new jobs and allow it to drain those already started.
- **Log and audit:** Knowing that the VM was interrupted by Azure can simplify root cause analysis of detection availability issues.
- **Notify and correlate:** Send notification to the system administrator or monitoring software and correlate the scheduled event with other signals.

### 3.3.17 EU GDPR compliance

The [European Union's General Data Protection regulation \(GDPR\)](#) is a privacy regulation that goes into effect on May 25, 2018. The GDPR regulation 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.

Key requirements of the GDPR include:

- Identifying what data you have, and controlling who has access to it
- Protecting personal data in your systems, as well as the ability to review and report on compliance

Microsoft designed Azure with industry-leading security measures and privacy policies to safeguard data in the cloud, including the categories of personal data identified by the GDPR.

Microsoft is the first global cloud services provider to publicly offer contractual commitments to its customers that provide key GDPR-related assurances about our services. Our contractual commitments relate to helping customers accomplish the following actions:

- Respond to requests to correct, amend, or delete personal data
- Detect and report personal data breaches
- Demonstrate their compliance with the GDPR

## 4 Conclusion

By combining state-of-the-art technology and industry standards, Microsoft Azure 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 Azure development, security, and quality practices help to ensure that the Azure platform meets its specifications and is maintained in a state of control and compliance. Azure maintains secure, consistent, and reliable performance through a series of tried and tested access, security, and privacy controls. These processes and controls are audited and verified on a continuous basis by qualified third-party accredited assessors.

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

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

## 5 Document Revision

| Date                 | Description     |
|----------------------|-----------------|
| <b>December 2017</b> | Initial release |

## 6 References

### 6.1 Industry guidance and standards

- Ref. [1] [ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, 2011](#)
- Ref. [2] [NIST Cloud Computing Standards Roadmap](#)
- Ref. [3] [PIC / S PI 011-3 - Good Practices for Computerised Systems in Regulated “GxP” Environments](#)
- Ref. [4] [Evolution of the Cloud: A Risk-Based Perspective on Leveraging PaaS within a Regulated Life Sciences Company, ISPE, July 2016](#)
- Ref. [5] [ISO/IEC 17789:2014 - Information technology - Cloud computing - Reference architecture](#)
- Ref. [6] [ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements](#)
- Ref. [7] [ISO 9001:2015 Quality management systems — Requirements](#)
- Ref. [8] [ISPE, GAMP 5 - A Risk-Based Approach to Compliant GxP computerized systems, 2008](#)
- Ref. [9] [ISPE, GAMP Good Practice Guide: IT Infrastructure Control and Compliance \(Second Edition\), 2017](#)
- Ref. [10] [ISPE, GAMP Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems \(Second Edition\), 2012](#)
- Ref. [11] [ISPE, GAMP Good Practice Guide: Global Information Systems Control and Compliance \(Second Edition\), 2017](#)
- Ref. [12] [ISPE, GAMP Guide: Records & Data Integrity, 2017](#)
- Ref. [13] [Cloud Standards Customer Council: Practical Guide to Cloud Service Agreements, April 2015](#)
- Ref. [14] [Cloud Standards Customer Council: Impact of Cloud Computing on Healthcare, February 2107](#)
- Ref. [15] [Cloud Standards Customer Council: Practical Guide to Platform-as-a-Service, September 2015](#)
- Ref. [16] [AAMI TIR45:2012, Guidance on the use of Agile practices in the development of medical device software, 2012](#)

### 6.2 Regulations and regulatory guidance

- Ref. [17] [U.S. FDA, Code of Federal Regulations, Title 21 Part 11, Electronic Records; Electronic Signatures](#)
- Ref. [18] [U.S. FDA Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application, August 2003](#)
- Ref. [19] [EudraLex The Rules Governing Medicinal Products in the European Union - Volume 4 - Good Manufacturing Practice - Medicinal Products for Human and Veterinary Use- Annex 11: Computerised Systems](#)
- Ref. [20] [U.S. FDA Data Integrity and Compliance with CGMP - Guidance for Industry \(Draft Guidance\), April 2016](#)
- Ref. [21] [FDA, Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11-- Questions and Answers \(Draft Guidance\), June 2017.](#)

## 6.3 Microsoft resources and reference material

### 6.3.1 Compliance and quality

- Ref. [22] [Standard Response to Request for Information - Microsoft Azure Security, Privacy, and Compliance, Version 4, March 2017](#)
- Ref. [23] [Azure CSA Cloud Controls Matrix](#)
- Ref. [24] [Microsoft Cloud Security for Enterprise Architects](#)
- Ref. [25] [A Practical Guide to Designing Secure Health Solutions Using Microsoft Azure](#)
- Ref. [26] [Microsoft EU-U.S. Privacy Shield](#)
- Ref. [27] [EU General Data Protection Regulation \(GDPR\)](#)
- Ref. [28] [Microsoft Supplier Data Protection Requirements](#)
- Ref. [29] [Training and Certification for Azure](#)
- Ref. [30] [Microsoft Azure Security Incident Management](#)
- Ref. [31] [Shared Responsibilities for Cloud Computing](#)
- Ref. [32] [Microsoft Corporation- Microsoft Azure \(Azure & Azure Government\) Service Organization Controls \(SOC\) 2 Report, October 1, 2016 - June 30, 2017](#)
- Ref. [33] [Azure - Cloud Security Diagnostic Tool 2016](#)
- Ref. [34] [Overview of Microsoft Azure Compliance](#)

### 6.3.2 Technical

- Ref. [35] [Availability Checklist](#)
- Ref. [36] [DevOps Checklist](#)
- Ref. [37] [Resiliency Checklist](#)
- Ref. [38] [Scalability Checklist](#)
- Ref. [39] [Azure Resource Manager Overview](#)
- Ref. [40] [Best practices for creating Azure Resource Manager templates](#)
- Ref. [41] [Azure Automation](#)
- Ref. [42] [Microsoft Security Development Lifecycle](#)
- Ref. [43] [Microsoft SDL Tools](#)
- Ref. [44] [Microsoft Information Security Management System](#)
- Ref. [45] [Microsoft Compliance Framework for Online Services](#)
- Ref. [46] [Protecting Data in Microsoft Azure](#)
- Ref. [47] [Securing the Microsoft Cloud](#)
- Ref. [48] [Security management in Azure](#)
- Ref. [49] [Securing PaaS deployments](#)
- Ref. [50] [Disaster recovery for Azure applications](#)
- Ref. [51] [Designing resilient applications for Azure](#)
- Ref. [52] [Failure mode analysis](#)
- Ref. [53] [Azure Active Directory report retention policies](#)
- Ref. [54] [Understanding Azure: A GUIDE FOR DEVELOPERS](#)
- Ref. [55] [Data in a PaaS World a Guide for New Applications](#)
- Ref. [56] [Azure Active Directory report retention policies](#)
- Ref. [57] [Overview of the features in Azure Backup](#)

- Ref. [58] [Microsoft Visual Studio – What is Infrastructure as Code](#)
- Ref. [59] [Microsoft Enterprise Cloud Red Teaming](#)
- Ref. [60] [Automated Analysis and Debugging of Network Connectivity Policies](#)
- Ref. [61] [Azure subscription and service limits, quotas, and constraints](#)
- Ref. [62] <https://docs.microsoft.com/en-us/rest/api/>
- Ref. [63] <https://github.com/Azure/azure-rest-api-specs>
- Ref. [64] [Test Drive Azure REST APIs](#)
- Ref. [65] [Pillars of software quality](#)
- Ref. [66] [Design principles for Azure applications](#)

#### 6.4 Other references

- Ref. [67] [Strategies for Life Sciences Companies Using Microsoft Azure with GxP Systems](#)

## 7 Appendices

Appendix A: Glossary

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

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

Appendix D: EudraLex Volume 4 Annex 11 Computerised Systems

### Appendix A. Glossary, Abbreviations and Acronyms

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



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

The following table includes the recommended SLA/quality agreement content, per the *GAMP Guidance: IT Infrastructure Control and Compliance (Second Edition)* (Ref. [9]), as well as a description of how the recommended content is addressed via the contractual agreements Microsoft has with its customers. The following summaries are included for your convenience. Customers should refer to the actual text in the most current version of the Microsoft agreements for the exact legal commitments.

| Requirement   | Coverage   |
|---|--|
| Contacts on either side                                       | <p>For each Azure subscription, customers must assign a subscription owner who is considered the customer's primary contact. Contact information for subscription owners is maintained directly within the Azure Management Portal.</p> <p>Depending on the engagement scenario, additional customer contacts may be specified in the Enrollment Agreement or Supplemental Contact Information Form.</p> <p>Microsoft Account Managers typically act as the primary point of contact between Microsoft and its customers.</p> <p>The Microsoft Online Services Terms (OST) also contains a section on "How to Contact Microsoft," which provides instructions for contacting Microsoft should the customer wish to file a complaint.</p> |
| Duration of validity and circumstances triggering reviews     | <p>Product SLAs are valid for the duration of the customer's subscription.</p> <p>The Enterprise and Enrollment Agreements include the effective date and term duration.</p> <p>As stated in the SOC 2 audit report (see Trust Criteria A1.1), Microsoft Azure management performs monthly reviews to evaluate compliance with customer SLA requirements.</p>  |
| Prerequisites and customer deliverables or involvement        | <p>Because of the generic nature of the Azure service offering, there are no specific prerequisites, customer deliverables, or involvement required in the delivery of the services to the customer.</p>   |
| Scope and nature of the required services                     | <p>A detailed description of the Azure service offering is available in Microsoft Azure Services section of the Product Terms. The Product Terms is located at <a href="http://go.microsoft.com/?linkid=9839207">http://go.microsoft.com/?linkid=9839207</a></p>   |
| Metrics in the form of KPIs                                   | <p>Individual product SLAs contain service performance metrics in the form of monthly uptime percentages. Microsoft monitors SLA performance and notifies customers if there is a lapse.</p>   |
| Records demonstrating fulfillment of specified service levels | <p>Microsoft maintains several logs and records related to security and data protection commitments:</p> <ul style="list-style-type: none"> <li>• Microsoft logs, or enables customer to log, access and use of information systems containing customer data, registering the</li> </ul>   |

| Requirement   | Coverage   |
|---|--|
|   | <p>access ID, time, authorization granted or denied, and relevant activity.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Microsoft maintains a record of security privileges of individuals having access to customer data.</li> <li>• Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain customer data.</li> <li>• 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.</li> <li>• 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.</li> </ul> <p>Logs for primary operations related to a customer’s Azure subscription resources are available through the Operation Logs feature in the Azure Management Portal.</p> <p>See the OST for more details, including which Azure Services are in scope.</p> <p>As described in Section 2.5.4, a records management procedure exists that defines records retention for support metrics and trending, which are periodically reviewed as part of the internal Microsoft auditing process as well by external third-party auditors during the SOC audit and ISO certification processes.</p> |
| Pricing arrangements, including penalties in case of shortcomings | Pricing arrangements for enterprise customers are stipulated in the Enterprise Agreement. The individual product SLAs define the service credits that customers will receive should the services fail to meet the stated uptime performance metrics.   |
| Reports, scope, frequency, distribution                           | <p>Microsoft publishes information concerning the current health and status of Azure services on the <a href="#">Azure status</a> page.</p> <p>Microsoft also publishes a history of Azure status reports on the <a href="#">Azure Status History</a> site. These status reports provide summaries of any incidents which have occurred, including root cause analysis and remediation actions which have been taken.</p>  |
| Audit provisions, including preparedness to facilitate            | Microsoft will conduct audits of the security of the computers, computing environment, and physical datacenters, as follows:   |

| Requirement  | Coverage   |
|--|--|
| <p>inspections from regulatory authorities or other regulators</p>   | <ul style="list-style-type: none"> <li>• Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.</li> <li>• Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.</li> <li>• Each audit will be performed by qualified, independent, third-party security auditors at Microsoft’s selection and expense.</li> </ul> <p>Each audit will result in the generation of an audit report that will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft audit report to the satisfaction of the auditor.</p> <p>Microsoft provides customers access to each Microsoft audit report so that customers can verify Microsoft compliance with the security obligations under the Data Processing Terms.</p> <p>Each Online Service follows a written data security policy (Information Security Policy) that complies with the following control standards and frameworks:</p> <ul style="list-style-type: none"> <li>• ISO 27001</li> <li>• Code of Practice ISO 27002</li> <li>• Code of Practice ISO 27018</li> <li>• SOC 1 Type II</li> <li>• SOC 2 Type II</li> </ul> <p>Subject to non-disclosure obligations, Microsoft will make the Information Security Policy available to customers.</p> <p>See the OST for more details, including which Azure Services are in scope.</p> <p>Customers may contact their Microsoft Account Managers for support requests should additional information be requested by a regulatory authority.</p> |
| <p>Defined parameters for roles and responsibilities (for example, maintenance of quality system requirements and controls) as per quality agreements requirements for EU GMP Annex 11 [1]</p> | <p>Microsoft responsibilities, controls, and practices concerning the following quality related activities are defined within the OST:</p> <ul style="list-style-type: none"> <li>• Organization of information security</li> <li>• Asset management</li> <li>• Human resources security</li> <li>• Physical and environmental security</li> <li>• Communications and operations management</li> <li>• Access control</li> <li>• Information security incident management</li> </ul>   |

| Requirement  | Coverage   |
|--|--|
|  | <ul style="list-style-type: none"><li data-bbox="646 289 1089 321">• Business continuity management</li></ul> <p data-bbox="597 363 1360 464">Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to customer data.</p> <p data-bbox="597 506 1390 569">See the OST for more details, including which Azure Services are in scope.</p>   |
| Processes to be supported and managed between the two parties, and the service levels including escalation, (for example, parameters for backup frequency, retention periods, and retrieval times) | <p data-bbox="597 615 1398 783">The OST includes a description of the Microsoft Data Recovery Procedures and Data Retention policy which states that Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of a customer's subscription so that the customer may extract the data.</p> <p data-bbox="597 825 1419 961">The customer's selected support plan specified as part of the Enterprise Agreement will indicate the range of support coverage, incident response time commitments, and the type of escalation and account management services to be provided.</p> |



# Microsoft Azure GxP Guidelines

## Appendix C

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

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

Microsoft responsibilities are mapped to Trust Criteria and Cloud Controls Matrix (CCM) Criteria evaluated as part of the most recent SOC2 report for Microsoft Azure (Ref. [32]). The Trust and CCM Criteria pertain to trust service principles and criteria that are met by control activities provided by Microsoft Azure and Microsoft datacenters.

| U.S. FDA 21 CFR Part 11  | Customer / Microsoft responsibilities  |
|--|--|
| <b>Subpart B — Electronic Records</b>  |  |
| <b>Sec. 11.10 Controls for closed systems.</b>   |  |
| <p><b>11.10</b><br/> <i>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</i></p> |  |
| <p><b>11.10 (a)</b><br/> <i>Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</i></p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Perform and document the validation activities to demonstrate that any GxP system managing electronic records is fit for its intended use and conforms to the specified requirements.</li> <li>- Establish appropriate system performance monitoring to ensure consistent availability and performance of GxP system(s).</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Procedures and controls are in place to ensure the Azure platform is developed and tested in accordance with industry best practices and standards (for example, ISO 9001 and ISO/IEC 27001) to ensure quality, security, as well as consistent and reliable performance. <b>(Refer to SOC 2 Report Controls: CC4.1, CCC-01, STA-03, CC7.1 to CC7.4).</b></li> <li>- Controls have been implemented to ensure the integrity of virtual machine images and provide alerts to customers of potential changes and events that may affect security or availability of the services in a timely manner <b>(Refer to SOC 2 Report Controls: IVS-02).</b></li> </ul> |

| U.S. FDA 21 CFR Part 11   | Customer / Microsoft responsibilities  |
|---|--|
| <p><b>11.10 (b)</b><br/> <i>The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.</i></p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Follow <a href="#">Azure Network Best Security Practices</a> to secure and protect data transferred from the GxP system(s) hosted in Azure.</li> <li>- Verify electronic records copied from the GxP system(s) are accurate and complete, ensuring that data integrity is maintained.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Controls are implemented to ensure system output is complete, accurate, distributed, and retained to meet the processing integrity commitments and system requirements. <b>(Refer to SOC 2 Report Controls: PI1.5).</b></li> <li>- SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity <b>(Refer to SOC 2 Report Controls: A1.1).</b></li> </ul>  |
| <p><b>11.10 (c)</b><br/> <i>Protection of records to enable their accurate and ready retrieval throughout the records retention period.</i></p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Follow <a href="#">Azure Data Security and Encryption Best Practices</a> to secure and protect data stored within the GxP system(s) hosted in Azure.</li> <li>- Implement appropriate security controls governing access to Azure services and GxP system(s) including permissions to regulated data.</li> <li>- Ensure backup processes are tested so that data integrity is maintained.</li> <li>- Define record retention policies for regulated data.</li> <li>- Ensure disaster recovery and business continuity processes are in place and tested.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Security controls to protect Azure cloud services and infrastructure are in place <b>(Refer to SOC 2 Report Controls: TVM-02).</b></li> <li>- Controls are implemented to ensure data is stored and maintained completely, accurately, and in a timely manner for its specified lifespan. <b>(Refer to SOC 2 Report Controls: PI1.4).</b></li> <li>- SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity <b>(Refer to SOC 2 Report Controls: A1.1).</b></li> <li>- Controls are in place to oversee the service of data backup or mirroring <b>(Refer to SOC 2 Report Controls: CC5.5, CC5.7, A1.2, A1.3, PI1.1).</b></li> </ul> |

| U.S. FDA 21 CFR Part 11   | Customer / Microsoft responsibilities   |
|---|---|
| <p><b>11.10 (d)</b><br/> <i>Limiting system access to authorized individuals.</i></p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Establish appropriate logical security processes governing the administration of system users/administrators to ensure segregation of duties and assignment of permissions according to the principle of least privilege.</li> <li>- Verify control mechanisms for limiting access are properly configured.</li> <li>- Implement periodic review of assigned access rights.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Physical and logical security policies are in place to limit access to authorized individuals based on the individual's job duties. <b>(Refer to SOC 2 Report Controls: CC5.1-CC5.8, CC6.2, DCS-02, IAM-01 to IAM-13, IVS-08, STA-01).</b></li> </ul>   |
| <p><b>11.10 (e)</b><br/> <i>Use of secure, computer-generated time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.</i></p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Verify that any GxP system generates secure audit trails as required by predicate rules for regulated electronic records.</li> <li>- Implement appropriate security controls to restrict access to regulated audit trail data, for example, that audit trail functionality cannot be disabled.</li> <li>- Ensure that data backup processes are in place and have been tested for applicable audit trail data.</li> <li>- Establish record retention policies that include relevant audit trail data.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Azure has established an Audit Log Management policy. Access to the log is restricted to authorized individuals <b>(Refer to SOC 2 Report Controls: IVS-01).</b></li> <li>- Security controls to protect cloud services and infrastructure are implemented <b>(Refer to SOC 2 Report Controls: TVM-02).</b></li> <li>- Controls are in place to oversee service of data backup or mirroring <b>(Refer to SOC 2 Report Controls: CC5.5, CC5.7, A1.2, A1.3, PI1.1, PI1.4).</b></li> </ul> |
| <p><b>11.10 (f)</b><br/> <i>Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.</i></p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- 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).</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul>   |

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



| U.S. FDA 21 CFR Part 11   | Customer / Microsoft responsibilities  |
|---|--|
| <p><b>11.10 (k)</b><br/> <i>Use of appropriate controls over systems documentation including:</i></p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Documents under the scope of these requirements are procedures, requirements, specifications, validation documents, and so on.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Documents under the scope of these requirements are system descriptions, procedures, and technical specifications.</li> </ul>   |
| <p><b>11.10 (k)(1)</b><br/> <i>Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</i></p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Implement procedural controls to manage the distribution, access, and use of system documentation for GxP systems hosted within Azure.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Procedural controls are in place to appropriately manage the distribution, access, and use of system documentation produced for Azure operations and maintenance. <b>(Refer to SOC 2 Report Controls: CC2.1).</b></li> </ul>  |
| <p><b>11.10 (k)(2)</b><br/> <i>Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</i></p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- 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.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Documentation and change management controls (that is, procedures) are in place <b>(Refer to SOC 2 Report Controls: CC7.1-CC7.4).</b></li> </ul>   |
| <p><b>Sec. 11.30 Controls for Open Systems</b></p>  |  |
| <p><b>11.30</b><br/> <i>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.</i></p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Configure encryption and access controls to ensure that the integrity of data is maintained.</li> <li>- Ensure that every GxP system hosted within Azure is assessed to determine if it is considered open or closed based on this definition.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- A series of procedural and technical controls are in place to ensure the protection and confidentiality of customer data <b>(Refer to SOC 2 Report Controls: C1.1-C1.8).</b></li> <li>- Internal communication where customer data is transmitted / involved is secured using SSL or equivalent mechanisms and travels within secured tunnel <b>(Refer to SOC 2 Report Controls: CC5.6, CC5.7, C1.2, EKM-03, IVS-10-IVS-12, IPY-04).</b></li> </ul> |
| <p><b>Sec. 11.50 Signature manifestations</b></p>   |  |

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

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

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



# Microsoft Azure GxP Guidelines

## Appendix C

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

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

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

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

| EU Volume 4 Annex 11  | Customer / Microsoft responsibilities  |
|---|--|
| <b>General</b>  |  |
| <b>1. Risk Management</b>   |  |
| <p>Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Document the assessment of risks related to patient safety, data integrity, and product quality as part of the validation activities around the GxP system(s) hosted within Azure.</li> <li>- Define and implement the necessary controls to mitigate risks and ensure data integrity.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Risk management is incorporated into processes around the development and maintenance of the Microsoft Azure platform (Refer to SOC 2 Report Controls: CC1.2, CC3.1, CC3.2, BCR-06, BCR-09, DSI-02, CCC-05, GRM-02, GRM-04, GRM-08, GRM-10, GRM-11, HRS-02, IAM-05, IAM-07, IVS-04, STA-01, STA-05, STA-06, TVM-02).</li> </ul> |
| <b>2. Personnel</b>   |  |

| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities   |
|--|---|
| <p>There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.</p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Identify key stakeholders for all GxP systems hosted in Azure.</li> <li>- Implement appropriate user, developer, and/or administrator training processes.</li> <li>- Ensure personnel have adequate experience/qualification/training to perform their job duties.</li> <li>- Ensure personnel training and qualifications are documented (that is, training records, CV).</li> <li>- Establish appropriate logical security processes that govern the administration of system users/administrators to ensure segregation of duties and assignment of permissions according to the principle of least privilege.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Training procedures have been established to evaluate the competency of personnel and engaged third parties (contractors) based on their job function. <b>(Refer to SOC 2 Report Controls: CC1.3, CC2.1, CC2.2, CC2.3, CC2.4, BCR-10, HRS-09).</b></li> <li>- Physical and logical security policies are in place to limit access to authorized individuals based on the individual's job duties. <b>(Refer to SOC 2 Report Controls: CC5.1-CC5.8, CC6.2, DCS-02, IAM-01 to IAM-13, IVS-08, STA-01).</b></li> </ul> |
| <p><b>3. Suppliers and Service Providers</b></p>   |   |
| <p>3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that formal agreements are implemented with suppliers that clearly define the roles and responsibilities of each party.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- 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. <b>Refer to SOC 2 Report Controls: STA-06 – STA-09).</b></li> <li>- Formal agreements are implemented between Microsoft and its customers that include statements of responsibilities as described with in the Online Service Terms (OST) (see details in Section 3.1.5).</li> </ul>   |

| EU Volume 4 Annex 11  | Customer / Microsoft responsibilities   |
|---|---|
| <p>3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that the supplier assessment process is documented and provides rationale to support the method implemented to qualify a selected supplier.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Risks related to external parties are assessed and addressed (<b>Refer to SOC 2 Report Controls: STA-05, STA-06</b>).</li> </ul>   |
| <p>3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.</p>                     | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Define regulated user requirements.</li> <li>- Review product documentation published on <a href="#">Microsoft Azure Documentation</a> site and within the <a href="#">Service Trust Platform (STP)</a> to ensure regulated user requirements are fulfilled.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Microsoft continuously publishes and updates content on the <a href="#">Microsoft Azure Documentation</a> site and within the <a href="#">Service Trust Platform (STP)</a> to ensure it accurately reflects the current product portfolio and capabilities.</li> <li>- 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 <a href="#">Azure training website</a>.</li> </ul> |
| <p>3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.</p>        | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Review the most recent Microsoft Azure ISO and SOC audit reports produced by independent third-party organizations and document the results of the assessment as necessary based on internal processes.</li> <li>- Ensure that supplier/vendor assessment information is available to inspectors when requested.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) (<b>Refer to SOC 2 Report Controls: AAC-01 – AAC-03</b>)</li> </ul>   |
| <p><b>Project Phase</b></p>   |   |
| <p><b>4. Validation</b></p>   |   |



| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities  |
|--|--|
| <p>4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Implement a formal computer system validation policy or procedure that conforms to the specified requirements.</li> <li>- Perform and document the qualification/validation of GxP system(s) hosted within Microsoft Azure based on a risk assessment.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Procedures and controls are in place to ensure the Azure platform is developed and tested in accordance with industry best practices and standards (for example, ISO 9001 and ISO/IEC 27001) to ensure quality and security as well as consistent and reliable performance. <b>(Refer to SOC 2 Report Controls: CC4.1, CCC-01, STA-03, CC7.1 to CC7.4).</b></li> <li>- Risk management is incorporated into processes around the development and maintenance of the Microsoft Azure platform <b>(Refer to SOC 2 Report Controls: CC1.2, CC3.1, CC3.2, BCR-06, BCR-09, DSI-02, CCC-05, GRM-02, GRM-04, GRM-08, GRM-10, GRM-11, HRS-02, IAM-05, IAM-07, IVS-04, STA-01, STA-05, STA-06, TVM-02).</b></li> </ul> |
| <p>4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.</p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Implement formal change control and deviation management processes in conjunction with validation of GxP applications.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- A formal change management process is defined governing how changes are made to the Azure platform (including products, services, and supporting hardware) <b>(Refer to SOC 2 Report Controls: AIS-01, CCC-01, STA-03, CC7.1-CC7.4).</b></li> </ul>   |

| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities   |
|--|---|
| <p>4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.</p> <p>For critical systems, an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Implement formal change control and deviation management processes in conjunction with validation of GxP applications.</li> <li>- Ensure controls are established to maintain current copies of any system documentation required to manage applicable GxP computerized systems</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Microsoft Azure maintains an inventory of key information assets. Procedures are established to review the inventory on a quarterly basis. <b>(Refer to SOC 2 Report Controls: DSI-02).</b></li> <li>- Controls are in place to ensure the Azure platform (including products, services, and supporting hardware) is maintained in a state of control and compliance <b>(Refer to SOC 2 Report Controls: AIS-01, CCC-01, STA-03, CC7.1-CC7.4).</b></li> <li>- A detailed system description of Azure services is contained with the SOC and ISO/IEC 27001 audit reports, which is available to customers via the Service Trust Platform (STP).</li> </ul> |
| <p>4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.</p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Implement formal change control and deviation management processes in conjunction with validation of GxP applications.</li> <li>- Ensure controls are established to maintain current copies of any system documentation required to manage applicable GxP computerized systems.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Microsoft Azure 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) <b>(Refer to SOC 2 Report Controls: CC7.1).</b></li> <li>- Formal risk assessments are performed on a regular basis <b>(Refer to SOC 2 Report Controls: GRM-10).</b></li> </ul>   |

| EU Volume 4 Annex 11  | Customer / Microsoft responsibilities  |
|---|--|
| <p>4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.</p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Review the most recent Microsoft Azure ISO and SOC audit reports produced by independent third-party organizations and document the results of the assessment as necessary based on internal processes.</li> <li>- Ensure that supplier/vendor assessment information is available to inspectors when requested.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Microsoft Azure regularly undergoes independent audits performed by qualified third-party accredited assessors for ISO (27001, 27018 &amp; 9001), SOC (1, 2, 3), HITRUST, FedRAMP and PCI (Refer to Section 2.4)</li> <li>- Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) <b>(Refer to SOC 2 Report Controls: AAC-01 – AAC-03)</b>.</li> </ul> |
| <p>4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.</p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Establish controls to ensure the assessment of quality and performance metrics throughout the GxP computerized system’s lifecycle.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Microsoft Azure development teams follow defined processes for verifying newly developed products and features, as well as for product changes and enhancements <b>(Refer to SOC 2 Report Controls: CCC-03)</b>.</li> <li>- Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) <b>(Refer to SOC 2 Report Controls: AAC-01 – AAC-03)</b></li> </ul>  |
| <p>4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure the implementation and use of a formal computer system validation policy or procedure that meets these requirements.</li> <li>- Document the qualification and validation testing activities in accordance with established processes.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Microsoft Azure development teams follow defined processes for verifying newly developed products and features, as well as for product changes and enhancements <b>(Refer to SOC 2 Report Controls: CCC-03)</b></li> <li>- Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) <b>(Refer to SOC 2 Report Controls: AAC-01 – AAC-03)</b></li> </ul>  |

| EU Volume 4 Annex 11  | Customer / Microsoft responsibilities  |
|---|--|
| <p>4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.</p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Establish data migration plan and testing strategy to ensure data integrity is maintained during the migration process.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul>  |
| <p><b>Operational Phase</b></p>   |  |
| <p><b>5. Data</b></p>   |  |
| <p>Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.</p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that encryption and access controls are in place so that the integrity of data is maintained.</li> <li>- Ensure that appropriate logical security policies are established and training has been documented.</li> <li>- Implement appropriate user access management practices to ensure that users are assigned permissions based on their job functions.</li> <li>- Implement periodic review of assigned access rights.</li> <li>- Verify GxP system only permits authorized actions to be taken with respect to regulated content.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Encryption and access controls have been implemented to ensure that the integrity of data is maintained (<b>Refer to SOC 2 Report Controls: CC5.6, CC5.7, C1.2, EKM-03, IVS-10-IVS-12, IPY-04</b>).</li> </ul> |
| <p><b>6. Accuracy Checks</b></p>  |  |
| <p>For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Establish procedural controls to enforce review of manually entered data or implement automated accuracy check mechanisms as part of the GxP system design / configuration.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul>  |
| <p><b>7. Data Storage</b></p>   |  |

| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities   |
|--|---|
| <p>7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Follow <a href="#">Azure Data Security and Encryption Best Practices</a> to secure and protect data stored within the GxP system(s) hosted in Azure.</li> <li>- Implement appropriate security controls governing access to Azure services and GxP system(s) including permissions to regulated data.</li> <li>- Ensure backup processes and systems are tested so that data integrity is maintained.</li> <li>- Define record retention policies for regulated data.</li> <li>- Ensure disaster recovery and business continuity processes are in place and tested.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Security controls to protect Azure cloud services and infrastructure are in place (<b>Refer to SOC 2 Report Controls: TVM-02</b>).</li> <li>- Controls are implemented to ensure data is stored and maintained completely, accurately, and in a timely manner for its specified life span. (<b>Refer to SOC 2 Report Controls: PI1.4</b>).</li> <li>- SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (<b>Refer to SOC 2 Report Controls: A1.1</b>).</li> <li>- Controls are in place to oversee the service of data backup or mirroring (<b>Refer to SOC 2 Report Controls: CC5.5, CC5.7, A1.2, A1.3, PI1.1</b>).</li> </ul> |
| <p>7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.</p>                           | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that backup infrastructure and policies are in place and have been tested for applications/systems/data maintained within the Azure environment.</li> <li>- Ensure appropriate governance of system administration activities around the management of Microsoft Azure services.</li> <li>- Ensure that encryption and access controls are in place to ensure that the integrity of data is maintained.</li> <li>- Verify that any GxP system hosted within the Azure environment conforms to the specified regulatory requirement.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (<b>Refer to SOC 2 Report Controls: A1.1</b>).</li> <li>- Physical and logical security policies are in place and followed (<b>Refer to SOC 2 Report Controls: CC5.1-CC5.8, CC6.2, DCS-02</b>).</li> <li>- 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 (<b>Refer to SOC 2 Report Controls: C1.1-C1-8</b>).</li> </ul>  |

| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities   |
|--|---|
| <b>8. Printouts</b>  |   |
| <p>8.1 It should be possible to obtain clear printed copies of electronically stored data.</p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure through verification that the transfer of data from applications/systems installed within the Microsoft Azure environment (which may store data) does not affect data integrity.</li> <li>- Verify that any GxP system hosted within the Azure environment conforms to the specified regulatory requirement.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul> |
| <p>8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.</p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Verify that any GxP system hosted within the Azure environment conforms to the specified regulatory requirement.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul>  |
| <b>9. Audit Trails</b>   |   |
| <p>Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Perform a risk assessment to determine where audit trails need to be implemented and verified within the GxP system(s).</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul>   |
| <b>10. Change and Configuration Management</b>   |   |

| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities   |
|--|---|
| <p>Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.</p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that appropriate logical security policies are established and training has been documented.</li> <li>- Ensure that appropriate security controls are defined to govern application/system/Azure access along with permissions related to data.</li> <li>- Ensure appropriate system administration practices are followed for applications/systems installed within the Azure environment.</li> <li>- Ensure appropriate governance of system administration activities around the management of Microsoft Azure services.</li> <li>- Ensure that backup infrastructure and policies are in place and have been tested for GxP system(s) hosted the Azure environment.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- A formal change management process is in place (<b>Refer to SOC 2 Report Controls: CC7.1-CC7.4, CCC-05</b>).</li> <li>- Azure notifies customers of potential changes and events that may affect security or availability of the services (<b>Refer to SOC 2 Report Controls: STA-05, CC2.6</b>).</li> </ul> |
| <p><b>11. Periodic evaluation</b></p>  |   |
| <p>Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that procedural controls are in place to periodically review the state of applications deployed within Azure.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Controls are in place to periodically review the state of components deployed within Azure to ensure their configuration is aligned with the baseline configuration (<b>Refer to SOC 2 Report Controls: CC4.1, CC7.2, STA-04</b>).</li> </ul>  |
| <p><b>12. Security</b></p>   |   |

| EU Volume 4 Annex 11  | Customer / Microsoft responsibilities   |
|---|---|
| <p>12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.</p> <p>12.2 The extent of security controls depends on the criticality of the computerised system.</p> <p>12.3 Creation, change, and cancellation of access authorisations should be recorded.</p> <p>12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that appropriate security controls are defined to govern application/system/Azure access along with permissions related to data.</li> <li>- Ensure that appropriate logical security policies are established and training has been documented.</li> <li>- Ensure appropriate system administration practices are followed for applications/systems installed within the Azure environment.</li> <li>- Ensure that audit trails have been properly defined and verified.</li> <li>- Ensure procedure controls are in place to help meet this requirement.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Security policies are in place (<b>Refer to SOC 2 Report Controls: CC1.1, CC1.2, CC1.4, CC2.1-CC2.4, AIS-04</b>).</li> <li>- SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (<b>Refer to SOC 2 Report Controls: A1.1</b>).</li> <li>- Physical and logical security policies are in place and followed (<b>Refer to SOC 2 Report Controls: CC5.1-CC5.8, CC6.2, DCS-02</b>).</li> </ul> |
| <p><b>13. Incident Management</b></p>   |   |
| <p>All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.</p>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure procedure controls are in place to manage system incidents and perform root cause analysis to identify corrective and preventive actions.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure procedure controls are in place to manage system incidents and perform root cause analysis to identify corrective and preventive actions (<b>Refer to SOC 2 Report Controls: CC2.5, CC6.2, BCR-10, SEF-01- SEF-05</b>).</li> </ul>  |
| <p><b>14. Electronic Signature</b></p>  |   |
| <p>Electronic records may be signed electronically. Electronic signatures are expected to:</p> <ol style="list-style-type: none"> <li>a. have the same impact as hand-written signatures within the boundaries of the company,</li> <li>b. be permanently linked to their respective record,</li> <li>c. include the time and date that they were applied.</li> </ol>   | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements.</li> <li>- Ensure procedure controls are in place to govern the use and assignment of electronic signatures.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul>  |
| <p><b>15. Batch Release</b></p>   |   |



| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities   |
|--|---|
| <p>When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.</p>  | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Verify that any GxP system that supports electronic signatures conforms to the specified regulatory requirements.</li> <li>- Ensure procedure controls are in place to govern the use and assignment of electronic signatures.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Not applicable – this requirement applies exclusively to the regulated use of the GxP application.</li> </ul>  |
| <p><b>16. Business Continuity</b></p>  |   |
| <p>For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that mechanisms for disaster recovery and business continuity are in place and tested.</li> <li>- Ensure that backup infrastructure and policies are in place and have been tested.</li> <li>- Implement and test data repatriation plan(s).</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Ensure that mechanisms for disaster recovery and business continuity are in place and tested, should any issue arise with Microsoft Azure services (<b>Refer to SOC 2 Report Controls: CC3.2, CC6.1, A1.1, A1.3, BRC-01- BCR-10</b>).</li> <li>- Ensure that backup infrastructure and policies are in place and have been tested (<b>Refer to SOC 2 Report Controls: CC5.5, CC5.7, A1.2, A1.3, PI1.1, PI1.4</b>).</li> <li>- Implement and test data repatriation plan(s) (<b>Refer to SOC 2 Report Controls: IVS-10, IPY-01</b>).</li> <li>- SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (<b>Refer to SOC 2 Report Controls: A1.1</b>).</li> </ul> |
| <p><b>17. Archiving</b></p>  |   |

| EU Volume 4 Annex 11   | Customer / Microsoft responsibilities   |
|--|---|
| <p>Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.</p> | <p><b>Customer responsibilities</b></p> <ul style="list-style-type: none"> <li>- Follow <a href="#">Azure Data Security and Encryption Best Practices</a> to secure and protect data stored within the GxP system(s) hosted in Azure.</li> <li>- Implement appropriate security controls that govern access to Azure services and GxP system(s) including permissions to regulated data.</li> <li>- Ensure backup processes and systems are tested so that data integrity is maintained.</li> <li>- Define record retention policies for regulated data.</li> <li>- Ensure disaster recovery and business continuity processes are in place and tested.</li> </ul> <p><b>Microsoft responsibilities</b></p> <ul style="list-style-type: none"> <li>- Security controls to protect Azure cloud services and infrastructure are in place (<b>Refer to SOC 2 Report Controls: TVM-02</b>).</li> <li>- Controls are implemented to ensure data is stored and maintained completely, accurately, and in a timely manner for its specified life span. (<b>Refer to SOC 2 Report Controls: PI1.4</b>).</li> <li>- SLA terms for data/service availability and maintenance are defined and monitored to ensure conformity (<b>Refer to SOC 2 Report Controls: A1.1</b>).</li> <li>- Controls are in place to oversee the service of data backup or mirroring (<b>Refer to SOC 2 Report Controls: CC5.5, CC5.7, A1.2, A1.3, PI1.1</b>).</li> </ul> |