Microsoft Azure

Microsoft Azure Compliance Offerings

Microsoft

Abstract

This document provides an overview of Microsoft Azure compliance offerings intended to help customers meet their own compliance obligations across regulated industries and markets worldwide. Azure maintains the largest compliance portfolio in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services in assessment scope). Azure compliance offerings are grouped into four segments: globally applicable, US government, industry specific, and region/country specific. Each offering description provides an up to-date-scope statement and links to useful downloadable resources.

November 2020

https://aka.ms/AzureCompliance

Acknowledgments

Author: Colin Yuen and Stevan Vidich

Reviewers: Derek Harris, Garima Jain, Shont Miller

(c) 2020 Microsoft Corporation. All rights reserved. This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

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.

Contents

Overview

Azure is a multi-tenant hyperscale cloud platform that is available or announced to customers in 60+regions worldwide. Most Azure services enable customers to specify the Region where their Customer Data will be located. Microsoft may replicate Customer Data to other Regions within the same Geo for data resiliency but Microsoft will not replicate Customer Data outside the chosen Geo (e.g., United States). Microsoft makes 5 distinct Azure cloud environments available to customers:

- **Azure** public cloud service is available globally
- **Azure in China** is available through a unique partnership between Microsoft and 21Vianet, one of the country's largest Internet providers
- **Azure Germany** provides services under a data trustee model, which ensures that Customer Data remains in Germany under the control of T-Systems International GmbH, a subsidiary of Deutsche Telecom, acting as the German data trustee
- **Azure Government** is available from 4 regions in the United States to US government agencies and their partners
- **Azure Government for DoD** is available from 2 regions in the United States to the US Department of Defense

To help customers meet their own compliance obligations across regulated industries and markets worldwide, Azure maintains the largest compliance portfolio in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services in assessment scope). To find out which Azure services are available in which regions, customers should explore the Azure global infrastructure product availability dashboard.

Azure compliance offerings are grouped into four segments: **globally applicable, US government, industry specific, and region/country specific**. Compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft. Each offering description in this document provides an up to date scope statement indicating which Azure customer-facing services are in scope for the assessment, as well as links to downloadable resources to assist customers with their own compliance obligations. For select third-party assessments, **Appendices A and B list services in audit scope for Azure and Azure Government**, respectively.

More detailed information about Azure compliance offerings is available from the Trust Center. Moreover, all downloadable documentation is available to Azure customers under a non-disclosure agreement from the Service Trust Portal in sections labeled:

- Audit Reports, which is further divided into FedRAMP, GRC Assessment, ISO, PCI DSS, and SOC reports sections;
- Data Protection Resources, which is further divided into Compliance Guides, FAQ and White Papers, and Pen Test and Security Assessments sections.

Customers are wholly responsible for ensuring their own compliance with all applicable laws and regulations. Information provided in this document does not constitute legal advice, and customers should consult their legal advisors for any questions regarding regulatory compliance.

Globally Applicable

Compliance offerings covered in this section have global applicability across regulated industries and markets. They can often be relied upon by customers when addressing specific industry and regional compliance obligations. For example, ISO 27001 certification provides a baseline set of requirements for many other international standards and regulations.

1 CIS Benchmark

The Center for Internet Security (CIS) has published the CIS Microsoft Azure Foundations Benchmark intended for customers who plan to develop, deploy, assess, or secure solutions that incorporate Azure. The document provides prescriptive guidance for establishing a secure baseline configuration for Azure. The benchmark was created using a consensus review process based on input from subject matter experts with diverse backgrounds spanning consulting, software development, audit and compliance, security research, operations, government, and legal. The resulting best practices guidance can be leveraged by customers to assess and improve the security posture of their applications deployed in Azure.

Each of the guidance recommendations in the CIS Azure Benchmark references one or more CIS Controls that were developed as a set of actions to help organizations improve their cyber defense capabilities. CIS Controls map to many established standards and regulatory frameworks, including the NIST Cybersecurity Framework (CSF), NIST SP 800-53, ISO 27000 series of standards, PCI DSS, HIPAA, NERC CIP, and others.

Applicability	Services in scope
All Azure environments	See the CIS Benchmark for Azure services assessed.

2 CSA STAR Self-Assessment

The Cloud Security Alliance (CSA) is a nonprofit organization led by a broad coalition of industry practitioners, corporations, and other important stakeholders. It is dedicated to defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when transitioning their IT operations to the cloud. In 2013, the CSA and the British Standards Institution launched the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry in which cloud service providers (CSPs) can publish their CSA-related assessments based on the following components:

- Cloud Controls Matrix (CCM): a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a CSP.
- Consensus Assessments Initiative Questionnaire (CAIQ): a set of nearly 300 questions based on the CCM that a customer or cloud auditor may want to ask of CSPs to assess their compliance with CSA best practices.

STAR provides three levels of assurance. CSA STAR Self-Assessment is the introductory offering at Level 1, which is free and open to all CSPs. Going further up the assurance stack, Level 2 of the STAR program involves third-party assessment-based certifications, and Level 3 involves certifications based on continuous monitoring.

As part of the STAR Self-Assessment, CSPs can submit two different types of documents to indicate their compliance with CSA best practices: a completed CAIQ, or a report documenting compliance with CCM. For the CSA STAR Self-Assessment, Microsoft Azure publishes both CAIQ and CCM-based reports.

Applicability	Services in scope
Azure Azure Germany Azure Government	See respective ISO 27001 scope statements.

3 CSA STAR Certification

Microsoft Azure has obtained the Cloud Security Alliance (CSA) STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture. The CSA STAR Certification is based on achieving ISO 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM). It demonstrates that a cloud service provider conforms to the applicable requirements of ISO 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

During the assessment, an accredited CSA certification auditor assigns a Maturity Capability score to each of the 16 CCM control areas. The average score is then used to assign the overall level of maturity and the corresponding Bronze, Silver, or Gold award. Azure was awarded the CSA STAR Certification at the Gold level. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune**, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services have also obtained STAR Certification.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See ISO 27001 scope statement.
Azure Government	See Appendix B.

4 CSA STAR Attestation

The CSA STAR Attestation involves a rigorous independent audit of a cloud provider's security posture based on a SOC 2 Type 2 audit in combination with Cloud Controls Matrix (CCM) criteria. The independent auditor that evaluates a cloud provider's offerings for STAR Attestation must be a certified public accountant (CPA) and is required to have the CSA Certificate in Cloud Security Knowledge (CCSK).

A SOC 2 Type 2 audit is based on the American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria, including security, availability, confidentiality, privacy, and processing integrity, and the criteria in the CCM. STAR Attestation provides an auditor's findings on the design suitability and operating effectiveness of Azure SOC 2 controls. The objective is to meet both the AICPA criteria mentioned above and requirements set forth in the CCM.

Based on this audit, Microsoft Azure has been awarded the CSA STAR Attestation.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See SOC 2 Type 2 scope statement.
Azure Government	See Appendix B.

5 ISO 20000-1:2011

ISO 20000-1:2011 is an international standard for IT service management that defines requirements for the development, implementation, monitoring, maintenance, and improvement of an IT service management system. Additional standards were published subsequently, including ISO 20000-2:2012 that provides guidance on the application of service management systems, as well as ISO 20000-9:2015 that provides guidance on the application of ISO 20000-1 to cloud services. Moreover, ISO 27013:2015 guidance on the integrated implementation of ISO 27001 and ISO 20000-1 was released for organizations who are planning to implement ISO 20000-1 when ISO 27001 is already implemented or who are planning to implement these two standards together. The ISO 20000-1 certificate demonstrates that a cloud service provider has implemented the right IT service management procedures to deliver efficient and reliable IT services that are subject to regular monitoring, review, and improvement. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune**, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the ISO 20000-1 certificate.

Applicability	Services in scope
Azure	See Appendix A.
Azure in China	See Trust Center for more information.
Azure Germany	See ISO 27001 scope statement.
Azure Government	See Appendix B.

6 ISO 22301:2012

ISO 22301:2012 is the premium international standard for business continuity management that provides for a formal certification. Azure has established a Business Continuity Management System (BCMS) in accordance with the ISO 22301:2012 standard and has received the corresponding certificate. ISO 22301:2012 specifies the requirements for a BCMS to help organizations protect against, prepare for, and recover from disruptive incidents. It is a comprehensive standard that organizations can use to demonstrate the highest level of commitment to business continuity and disaster preparedness. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune**, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the ISO 22301:2012 certificate.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See ISO 27001 scope statement.
Azure Government	See Appendix B.

7 ISO 27001:2013

Azure maintains its ISO 27001 certification and makes the corresponding audit report and certificate available to customers from the Service Trust Portal. ISO 27000 family of standards provide a framework for policies and procedures that include all legal, physical, and technical controls involved in an organization's information risk management processes. ISO 27001 specifies the requirements for implementing, maintaining, monitoring, and continually improving an information security management standard (ISMS). ISO 27002 provides guidelines and best practices for information security management; however, an organization cannot get certified against ISO 27002 because it is not a management standard. The audit vehicle is ISO 27001, which relies on detailed guidelines in ISO 27002 for control implementation. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune**, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the ISO 27001:2013 certificate.

Applicability	Services in scope
Azure	See Appendix A.
Azure in China	See Trust Center for more information.
Azure Germany	App Service, Batch, Cloud Services, Functions, Service Fabric, Virtual Machines (including SQL VM), Virtual Machines Scale Sets, Application Gateway, Azure DDOS Protection, Azure DNS, ExpressRoute, Load Balancer, Network Watcher, Traffic Manager, Virtual Network, VPN Gateway, Backup, Cool Storage, Premium Storage, Site Recovery, Storage (Blobs (including Azure Data Lake Storage Gen 2), Disks, Files, Queues, Tables), App Service: API Apps, App Service: Mobile Apps, App Service: Web Apps, Media Services, Notification Hubs, Azure Cosmos DB, Azure SQL Database, Redis Cache, Azure Synapse Analytics, Azure Analysis Services, HDInsight, Stream Analytics, Machine Learning Studio, Event Hubs, IoT Hub, Service Bus, Azure Active Directory (Free, Basic, Premium), Key Vault, Multi-Factor Authentication, Azure Monitor, Azure Policy, Azure Resource Manager, Azure Service Health, Microsoft Azure Portal, Scheduler and supporting infrastructure and platform services.
Azure Government	See Appendix B.

8 ISO 27017:2015

The ISO 27017 code of practice is designed for organizations to use as a reference for selecting cloud services information security controls when implementing a cloud computing information security management system based on ISO 27002. It can also be used by cloud service providers as a guidance document for implementing commonly accepted protection controls. This international standard provides additional cloud-specific implementation guidance based on ISO/IEC 27002, and provides additional controls to address cloud-specific information security threats and risks. The Azure ISO 27017 certificate is available for download. ISO 27017 is unique in providing guidance for both cloud service providers and cloud service customers. It also provides cloud service customers with practical information on what they should expect from cloud service providers. Customers can benefit directly from ISO 27017 by ensuring they understand the concept of shared responsibilities in the cloud. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft**

Intune, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the ISO 27017 certificate.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See ISO 27001 scope statement.
Azure Government	See Appendix B.

9 ISO 27018:2014

ISO 27018 is the first international code of practice for cloud privacy that provides guidelines based on ISO 27002 guidelines and best practices for information security management. Based on EU data-protection laws, it gives specific guidance to cloud service providers acting as processors of personally identifiable information (PII) on assessing risks and implementing state-of-the-art controls for protecting PII. ISO 27018 establishes cloud-specific control objectives and guidelines for PII in accordance with the privacy principles in ISO 29100. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune**, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the ISO 27018:2014 certificate. The Azure ISO 27018 certificate and audit report are available for download from the Service Trust Portal.

Applicability	Services in scope
Azure	See Appendix A.
Azure in China	See Trust Center for more information.
Azure Germany	See ISO 27001 scope statement.
Azure Government	See Appendix B.

10 ISO 27701

ISO 27701 is built as an extension of the widely-used ISO/IEC 27001 standard for information security management, making the implementation of PIMS's privacy information management system a helpful compliance extension for the many organizations that rely on ISO/IEC 27001, as well as creating a strong integration point for aligning security and privacy controls. PIMS accomplishes this through a framework for managing personal data that can be used by both data controllers and data processors, a key distinction for GDPR compliance. In addition, any PIMS audit requires the organization to declare applicable laws/regulations in its criteria for the audit meaning that the standard can be mapped to many of the requirements under GDPR, CCPA (California Consumer Privacy Act), or other laws. This universal framework allows organizations to efficiently operationalize compliance with new regulatory requirements. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune**, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the ISO 27701:2019 certificate. The Azure ISO 27701 certificate and audit report are available from the Service Trust Portal.

Applicability	Services in scope
Azure	See Appendix A.

Azure Germany	See ISO 27001 scope statement.
Azure Government	See Appendix B.

11 ISO 9001:2015

ISO 9001 is an international standard that establishes the criteria for a quality management system. It is the only standard in the ISO 9000 family that results in a formal certification. The standard is based on several quality management principles, including clear focus on meeting customer requirements, strong corporate governance and leadership commitment to quality objectives, process-driven approach to meeting objectives, and focus on continuous improvement. ISO 9001 helps organizations improve customer satisfaction by focusing on the consistency and quality of products and services provided to customers. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune**, **Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the ISO 9001:2015 certificate. The Azure ISO 9001 certificate and audit report are available from the Service Trust Portal. Customers can leverage Azure ISO 9001 certification in sector-specific standards for quality management systems, including ISO 13485 for medical devices, ISO 29001 for petrochemical and natural gas industries, ISO 90003 for software engineering, ISO 17852 for government electoral organizations, ISO 16949 for automotive production and service parts organization, Good Clinical, Laboratory, Manufacturing practices (GxP) in life sciences, and more.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See ISO 27001 scope statement.
Azure Government	See Appendix B.

12 SOC 1 Type 2

The American Institute of Certified Public Accountants (AICPA) has established three Service Organization Controls (SOC) reporting options (SOC 1, SOC 2, and SOC 3) to assist CPAs with examining and reporting on a service organization's controls. The SOC 1 Type 2 attestation is based on the AICPA Statement on Standards for Attestation Engagements 18 (SSAE 18) standard (see AT-C Section 105) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). For Azure Germany, the attestation is done in accordance with the IDW PS 951 standard. The SOC 1 attestation has replaced SAS 70, and it is appropriate for reporting on controls at a service organization relevant to user entities internal controls over financial reporting. A Type 2 report includes auditor's opinion on the control effectiveness to achieve the related control objectives during the specified monitoring period. Customers can leverage the Azure SOC 1 Type 2 attestation when pursuing their own financial industry specific compliance requirements such as Sarbanes-Oxley (SOX), Federal Financial Institutions Examination Council (FFIEC), Gramm-Leach-Bliley Act (GLBA), etc. Azure maintains a SOC 1 Type 2 attestation that is based on a rolling 12-month run window (audit period) with new reports issued quarterly. Customers can download the latest attestation report form the Service Trust Portal (see SOC Reports section). Aside from Azure services listed in Appendices A and Azure Government services in Appendix B, the following online services are also included in the SOC 1 attestation report: **Intune, Microsoft Cloud App Security, Microsoft Graph, Microsoft Managed Desktop, Microsoft Stream, Microsoft Threat Experts, Microsoft Threat Protection, Power Apps, Power Automate, Power BI,**

Power Virtual Agents, Microsoft Forms Pro, Microsoft 365 Defender, Microsoft Defender for Endpoint and Microsoft Defender for Identity.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See SOC 2 Type 2 scope statement.
Azure Government	See Appendix B.

13 SOC 2 Type 2

SOC 2 Type 2 is a restricted use report intended to report on controls relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy system attributes. SOC 2 engagements are conducted in accordance with the Trust Services Principles and Criteria, as well as the requirements stated in the AICPA AT Section 101 standard. In addition, Azure SOC 2 Type 2 report addresses the requirements set forth in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM). Azure SOC 1 and SOC 2 attestations are based on rigorous independent third-party audits conducted by a reputable CPA firm. At the conclusion of a SOC 1 or SOC 2 audit, the auditor renders an opinion in a SOC 1 Type 2 or SOC 2 Type 2 report, which describes the cloud service provider's (CSP's) system and assesses the fairness of the CSP's description of its controls. It also evaluates whether the CSP's controls are designed appropriately, were in operation on a specified date, and were operating effectively over a specified time period. Azure SOC 2 Type 2 report is relevant to the Security, Availability, Confidentiality, and Processing Integrity trust principles. Azure maintains a SOC 2 Type 2 attestation that is based on a rolling 12-month run window (audit period) with new reports issued quarterly. Customers can download the latest attestation report form the Service Trust Portal (see SOC Reports section). Aside from Azure services listed in Appendices A and Azure Government services in Appendix B, the following online services are also included in the SOC 2 Type 2 attestation report: **Intune, Microsoft Cloud App Security, Microsoft Graph, Microsoft Managed Desktop, Microsoft Stream, Microsoft Threat Experts, Microsoft Threat Protection, Power Apps, Power Automate, Power BI, Power Virtual Agents, Microsoft Forms Pro, Microsoft 365 Defender, Microsoft Defender for Endpoint and Microsoft Defender for Identity.**

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	App Service (API Apps, Mobile Apps, Web Apps), Azure Functions, Application Gateway, Azure Active Directory (Free and Basic), Azure Analysis Services, Azure Backup, Azure Cache for Redis, Azure Cosmos DB, Azure Data Explorer, Azure DNS, Azure ExpressRoute, Azure Private Link, Azure IoT Hub, Azure Media Services, Azure Monitor, Azure Resource Manager, Azure Service Fabric, Azure Site Recovery, Azure SQL Database, Azure Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium Storage, Azure Stream Analytics, Azure Synapse Analytics, Batch, Cloud Services, Event Hubs, HDInsight, Key Vault, Load Balancer, Machine Learning Studio (Classic), Microsoft Azure Portal, Multi-Factor Authentication, Network Watcher, Notification Hubs, Power BI Embedded, Scheduler, Service Bus, SQL Server on Virtual Machines, Traffic Manager, Virtual Machine Scale Sets, Virtual Machines, Virtual Network, VPN Gateway, Dynamics 365 Customer Engagement, Dynamics 365 Portals, and supporting infrastructure and platform services.

Azure Government	See Appendix B.

14 SOC 3

A SOC 3 report is a short, publicly facing version of the SOC 2 Type 2 attestation report, for users who want assurances about the cloud service provider's controls but do not need a full SOC 2 report. Azure SOC 3 report can be downloaded from the Service Trust Portal. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B, the following online services are also included in the SOC 3 report: **Intune, Microsoft Cloud App Security, Microsoft Graph, Microsoft Managed Desktop, Microsoft Stream, Microsoft Threat Experts, Microsoft Threat Protection, Power Apps, Power Automate, Power BI, Power Virtual Agents, Nomination Portal, Microsoft Forms Pro, Microsoft 365 Defender, Microsoft Defender for Endpoint and Microsoft Defender for Identity.**

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See SOC 2 Type 2 scope statement.
Azure Government	See Appendix B.

15 WCAG 2.0 (ISO 40500:2012)

The Web Content Accessibility Guidelines 2.0 (WCAG 2.0) provide a framework for developing web content that improves accessibility for people with disabilities, as well as users of devices with limited graphical abilities. WCAG 2.0 was published in 2008 by the World Wide Web Consortium (W3C). In 2012, WCAG 2.0 was also published by the International Organization for Standardization (ISO) as ISO/IEC 40500:2012.

WCAG 2.0 is organized around four principles, which in turn have 12 guidelines. Each guideline has testable success criteria, which are scored at three conformance levels: A, AA, and AAA. Microsoft publishes WCAG 2.0 AA reports that reflect the complete product or service. We generally do not create a report for individual features or components. In some cases, we may release a new component for an existing product, or a new version of an existing component, which users may choose to install separately, and we may publish a WCAG 2.0 AA report for that component.

Applicability	WCAG 2.0 AA reports
Azure Azure Government	See list of WCAG 2.0 AA reports for Microsoft products.

US Government

The following compliance offerings are focused primarily on addressing the needs of US Government. Azure, Azure Government, and Azure Government for DoD have the same comprehensive security controls in place, as well as the same Microsoft commitment on the safeguarding of Customer Data. Azure Government provides additional controls regarding US Government specific background screening requirements, including maintaining US persons for Azure Government operations. Azure Government for DoD is reserved for exclusive use by the Department of Defense.

16 CJIS

The Criminal Justice Information Services (CJIS) Division of the US Federal Bureau of Investigation (FBI) gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI)—for example, fingerprint records and criminal histories. Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage, or processing of CJI complies with the CJIS Security Policy, which establishes minimum security requirements and controls to safeguard CJI. All private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. It also commits the contractor to maintaining a security program consistent with federal and state laws, regulations, and standards, and limits the use of CJI to the purposes for which a government agency provided it.

Microsoft will sign the CJIS Security Addendum in states with CJIS Information Agreements. These agreements tell state law enforcement authorities responsible for compliance with CJIS Security Policy how Microsoft's cloud security controls help protect the full lifecycle of data and ensure appropriate background screening of operations personnel with potential access to CJI. Microsoft continues to work with state governments to enter into CJIS Information Agreements. Microsoft has agreements signed with 34 states, including Alabama, Alaska, Arizona, Arkansas, California, Colorado, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nevada, New Jersey, New York, North Carolina, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, and Washington.

Customers subject to CJIS requirements should review the CJIS Implementation Guidelines for Azure Government. Also available is the Microsoft Cloud – CJIS Cloud Computing Requirements Mapping, which details CJIS specific requirements and Microsoft cloud provider's responses.

Applicability	Services in scope
Azure Government	See Azure Government services in FedRAMP High audit scope.

17 CNSSI 1253

The Committee on National Security Systems (CNSS) Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems" provides all federal government departments, agencies, bureaus, and offices with a guidance for security categorization of National Security Systems (NSS) that collect, generate, process, store, display, transmit, or receive National Security Information. The CNSSI 1253 builds on the NIST SP 800-53, which provides the control baseline for Azure Government FedRAMP High authorization. There are some key differences between the CNSSI 1253 and NIST publications, including the approach adopted by the CNSSI 1253 to define explicitly the associations of Confidentiality, Integrity, and Availability to security controls, as well as to refine the use of security control overlays for the national security community.

NSS are categorized using separate Low, Medium, and High categorization for each of the security objectives, Confidentiality, Integrity, and Availability, resulting in categorizations such as "Moderate-Moderate-Low", "Moderate-Moderate-High", etc., CNSSI 1253 then provides the appropriate security baselines for each of the possible system categorizations using controls from NIST SP 800-53. To assist customers who require support for the CNSSI 1253 High-High-High baseline, Azure Government has

been validated by an independent third-party assessment organization (3PAO). The resulting Security Assessment Plan documents the testing conducted to validate Azure Government against a selection of CNSSI 1253 security controls for systems requiring High Confidentiality, High Integrity, and High Availability.

Azure Government currently possesses a FedRAMP High Provisional Authorization to Operate issued by the Joint Authorization Board (JAB), as well as the Department of Defense Provisional Authorization at the Security Requirements Guide (SRG) Impact Level 5. Leveraging these authorizations, the 3PAO performed an analysis on the security controls that have already been tested to determine which additional CNSSI 1253 security controls needed to be assessed to ensure compliance with a High-High-High baseline. The results of this testing are provided in the accompanying Security Assessment Report (SAR).

The SAR from the Azure Government assessment testing provides a complete assessment of the applicable security controls as stipulated in the SAP. Evidence and interviews were conducted to validate the successful implementation of the various security controls. The attestation of compliance with the CNSSI 1253 High-High-High baseline can be downloaded from the Service Trust Portal GRC Assessment Reports section.

Applicability	Services in scope
Azure Government	See Azure Services in FedRAMP and DoD SRG Audit Scope

18 DFARS

Defense contractors whose information systems process, store, or transmit covered defense information (CDI) must comply with the Department of Defense (DoD) Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, which specifies requirements for the protection of controlled unclassified information (CUI) in accordance with NIST SP 800-171, cyber incident reporting obligations, and other considerations for cloud service providers. All DoD contractors are required to comply with DFARS requirements for adequate security "as soon as practical, but not later than 31 December 2017.

Azure Government has attained a FedRAMP High Provisional Authorization to Operate (P-ATO) as well as a DoD DISA SRG Level 4 Provisional Authorization (PA) whereas Azure Government for DoD has attained a DoD DISA SRG Level 5 PA. These authorizations allow DoD mission partners to host CDI within the Azure Government and Azure Government for DoD clouds. Microsoft provides a contract amendment to help defense contractors meet the requirements in the DFARS Clause 252.204-7012 that apply to cloud service providers. When defense contractors are required to include the DFARS Clause 252.204-7012 flow-downs in subcontracts, Microsoft can accept the flow-down terms applicable to cloud service providers for Azure Government and Azure Government for DoD.

An accredited third-party assessment organization (3PAO) has attested that Azure Government meets the applicable requirements of DFARS Clause 252.204-7012. The attestation of compliance with DFARS can be downloaded from the Service Trust Portal GRC Assessment Reports section. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune** online service also meet the applicable requirements of DFARS Clause 252.204-7012.

Applicability	Services in scope
Azure Government	See Azure Services in FedRAMP and DoD SRG Audit Scope
Azure Government for DoD	See Azure Services in FedRAMP and DoD SRG Audit Scope

19 DoD DISA SRG Level 2

The Defense Information Systems Agency (DISA) is an agency of the US Department of Defense (DoD) that is responsible for developing and maintaining the DoD Cloud Computing Security Requirements Guide (SRG). The SRG defines the baseline security requirements used by DoD to assess the security posture of a cloud service provider (CSP), supporting the decision to grant a DoD Provisional Authorization (PA) that allows a CSP to host DoD missions. It incorporates, supersedes, and rescinds the previously published DoD Cloud Security Model (CSM).

Azure maintains a DoD PA at SRG Impact Level 2, which covers non-controlled unclassified information including all data cleared for public release, for the in-scope services.

Applicability	Services in scope
Azure	See Appendix A.
Azure Government	See Appendix B.

20 DoD DISA SRG Level 4

Azure Government maintains a DoD Provisional Authorization (PA) at SRG Impact Level 4, which accommodates Controlled Unclassified Information (CUI) and other mission critical data, for the in-scope services. CUI contains many categories which require protection from unauthorized disclosure. Designating information as CUI or mission critical data to be protected at Impact Level 4 is the responsibility of the owning organization. Aside from Azure services listed in Appendix B, **Microsoft Intune** and **Power BI** online services have also received PA at SRG Impact Level 4.

Applicability	Services in scope
Azure Government	See Appendix B.

21 DoD DISA SRG Level 5

Azure Government for DoD maintains a DoD Provisional Authorization (PA) at SRG Impact Level 5, which accommodates Controlled Unclassified Information (CUI) that may require a higher level of protection than that afforded by Impact Level 4, for the in-scope services. Moreover, Impact Level 5 supports unclassified National Security Systems. Aside from Azure services listed in Appendix B, Microsoft **Power BI** online service has also received PA at SRG Impact Level 5.

Applicability	Services in scope
Azure Government for DoD	See Appendix B.

22 DoE 10 CFR Part 810

The US Department of Energy (DoE) export control regulation 10 CFR Part 810 implements section 57b.(2) of the Atomic Energy Act of 1954 (AEA), as amended by section 302 of the Nuclear Nonproliferation Act of 1978 (NNPA). It is administered by the National Nuclear Security Administration

(NNSA). The revised Part 810 (final rule) became effective on 25 March 2015, and, among other things, it controls the export of unclassified nuclear technology and assistance. It enables peaceful nuclear trade by helping to assure that nuclear technologies exported from the United States will not be used for non-peaceful purposes. § 810.7 (b) states that specific DoE authorization is required for providing or transferring sensitive nuclear technology to any foreign entity.

Azure Government can accommodate customers subject to DoE 10 CFR Part 810 export control requirements because it is designed to meet specific controls that restrict access to information and systems to US persons among Azure operations personnel. Customers deploying data to Azure Government are responsible for their own security classification process. For data subject to DoE export controls, the classification system is augmented by the Unclassified Controlled Nuclear Information (UCNI) controls established by section 148 of the AEA.

The Nuclear Regulatory Commission (NRC) regulates the export and import of nuclear facilities and related equipment and materials under 10 CFR Part 110. The NRC does not regulate nuclear technology and assistance related to these items which are under the DoE jurisdiction. Consequently, NRC 10 CFR Part 110 regulations would not be applicable to Azure.

Applicability	Services in scope
Azure Government	See Azure Services in FedRAMP and DoD SRG Audit Scope

23 EAR

The US Department of Commerce is responsible for enforcing the Export Administration Regulations (EAR) through the Bureau of Industry and Security (BIS). According to BIS definitions, Export is the transfer of protected technology or information to a foreign destination or release of protected technology or information to a foreign person in the United States (aka Deemed Export). Items subject to EAR can be found on the Commerce Control List (CCL), and each item has a unique Export Control Classification Number (ECCN) assigned. Items not listed on the CCL are designated as EAR99.

The EAR is applicable to dual-use items that have both commercial and military applications, as well as to items with purely commercial application. The BIS has provided guidance holding that cloud service providers (CSP) are not exporters of customers' data due to the customers' use of cloud services. Moreover, in the final rule published on 3 June 2016, BIS clarified that EAR licensing requirements would not apply if the transmission and storage of unclassified technical data and software were encrypted end-to-end using FIPS 140-2 validated cryptographic modules and not intentionally stored in a military-embargoed country (i.e., Country Group D:5 as described in Supplement No. 1 to Part 740 of the EAR) or in the Russian Federation.

Both Azure and Azure Government can help customers subject to the EAR meet their compliance requirements. Except for the Hong Kong region, Azure and Azure Government datacenters are not located in proscribed countries or in the Russian Federation. Azure and Azure Government rely on FIPS 140-2 validated cryptographic modules in the underlying operating system, and provide customers with a wide range of options for encrypting data in transit and at rest, including encryption key management using Azure Key Vault, which can store encryption keys in FIPS 140-2 validated Hardware Security Modules (HSM) under customer control (Customer Managed Keys, CMK). Keys generated inside the Azure Key Vault HSMs are not exportable – there can be no clear version of the key outside the HSMs.

This binding is enforced by the underlying HSM. Moreover, Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents do not see or extract customer keys.

Customers are responsible for choosing Azure or Azure Government regions for deploying their applications and data. Moreover, customers are responsible for designing their applications to leverage end-to-end data encryption that meets EAR requirements. Microsoft does not inspect or approve customer applications deployed in Azure or Azure Government.

Azure Government provides an additional layer of protection to customers through contractual commitments regarding storage of Customer Data in the United States and limiting potential access to systems processing Customer Data to screened US persons. For additional information regarding the EAR, customers should review "Microsoft Azure Export Controls Whitepaper" available from the Service Trust Portal (see FAQ and White Papers section).

Applicability	Services in scope
Azure	See Azure services in FedRAMP High audit scope.
Azure Government	See Azure Government services in FedRAMP High audit scope.

24 FedRAMP High (NIST SP 800-53)

The US Federal Risk and Authorization Management Program (FedRAMP) was established in December 2011 to provide a standardized approach for assessing, monitoring, and authorizing cloud service providers (CSPs). CSPs desiring to sell services to a federal agency requiring FedRAMP can take three paths to demonstrate FedRAMP compliance: 1) earn a Provisional Authorization to Operate (P-ATO) from the Joint Authorization Board (JAB); 2) receive an Authorization to Operate (ATO) from a federal agency; or 3) work independently to develop a CSP Supplied Package that meets program requirements. Each of these paths requires a stringent technical review by the FedRAMP Program Management Office (PMO) and an assessment by an independent third-party assessment organization (3PAO) that is accredited by the program.

FedRAMP is based on the National Institute of Standards and Technology (NIST) SP 800-53 Rev 4 standard, augmented by FedRAMP controls and enhancements. FedRAMP authorizations are granted at three impact levels based on the NIST FIPS 199 guidelines—Low, Moderate, and High. These levels rank the impact that the loss of confidentiality, integrity, or availability could have on an organization—Low (limited effect), Moderate (serious adverse effect), and High (severe or catastrophic effect). The number of controls in the corresponding baseline increases as the impact level increases, e.g., FedRAMP Moderate baseline has 325 controls whereas FedRAMP High baseline has 421 controls.

The FedRAMP High authorization represents the highest bar for FedRAMP compliance. The FedRAMP Joint Authorization Board (JAB) is the primary governance and decision-making body for FedRAMP. Representatives from the Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA) serve on the board. The board grants a P-ATO to cloud service providers that have demonstrated FedRAMP compliance. It's important to note that FedRAMP is not a point-in-time certification but an assessment and authorization program that also comes with provisions for continuous monitoring mandated by the DHS.

Azure and Azure Government maintain FedRAMP High P-ATOs issued by the JAB in addition to more than 90 Moderate and High ATOs issued by individual federal agencies for the in-scope services. Aside from Azure services listed in the Azure Services in FedRAMP and DoD SRG Audit Scope, **Microsoft Cloud App Security, Microsoft Intune, Microsoft Flow, Microsoft PowerApps, Microsoft Graph (Azure Government only), Microsoft Stream,** and **Power BI** online services are also included in the P-ATO packages. Customers can leverage the FedRAMP High Blueprint for assistance with implementing FedRAMP-compliant workloads in Azure.

Applicability	Services in scope
Azure	See Appendix A.
Azure Government	See Appendix B.

25 FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government standard that defines minimum security requirements for cryptographic modules in products and systems. Validation against the FIPS 140-2 standard is required for all US federal government agencies that use cryptography-based security systems to protect sensitive but unclassified information stored digitally. NIST publishes a list of vendors and their cryptographic modules validated for FIPS 140-2. Microsoft certifies the cryptographic modules used in Microsoft products with each new release of the Windows operating system, and Azure relies on FIPS 140-2 validated modules in the underlying operating system. Moreover, Azure customers can store their own cryptographic keys and other secrets in FIPS 140-2 validated hardware security modules (HSM).

Applicability	Validated cryptographic modules
Azure Azure Government Azure Government for DoD	See Microsoft current and in-process validations.

26 IRS 1075

Internal Revenue Service Publication 1075 (IRS 1075) provides safeguards for protecting Federal Tax Information (FTI) at all points where it is received, processed, stored, and maintained. It applies to federal, state, and local agencies with whom IRS shares FTI, and it defines a broad set of management, operations, and technology specific security controls that must be in place to protect FTI. The core control scope is based on NIST SP 800-53 R4 that Azure Government covers as part of the existing FedRAMP High authorization. Additional requirements cover protection of FTI in a cloud computing environment (aka Exhibit 16), and place much emphasis on FIPS 140-2 validated data encryption in transit and at rest.

Microsoft can provide customers with contractual commitment to demonstrate that Azure Government has appropriate security controls and capabilities in place necessary for customers to meet the substantive IRS 1075 requirements. Customers can download the Azure IRS 1075 Safeguard Security Report from the Service Trust Portal GRC Assessment Reports section to understand how Azure Government implements the applicable IRS controls. Moreover, Microsoft provides another document, Azure Government Compliance Considerations, directly to the IRS to outline how an agency can use

Azure Government services in a way that complies with IRS 1075 requirements. Government customers under NDA can request this document.

Applicability	Services in scope
Azure Government	See Azure Government services in FedRAMP High audit scope.

27 ITAR

The US Department of State has export control authority over defense articles, services, and related technologies under the International Traffic in Arms Regulations (ITAR) managed by the Directorate of Defense Trade Controls (DDTC). Items under ITAR protection are documented on the United States Munitions List (USML). Customers who are manufacturers, exporters, and brokers of defense articles, services, and related technologies as defined on the USML must be registered with DDTC, must understand and abide by ITAR, and must self-certify that they operate in accordance with ITAR.

DDTC revised the ITAR rules effective 25 March 2020 to align them more closely with the EAR. These ITAR revisions introduced an end-to-end data encryption carve-out that incorporated many of the same terms that the Commerce Department adopted in 2016 for the EAR. Specifically, the revised ITAR rules state that activities that do not constitute exports, re-exports, re-transfers, or temporary imports include (among other activities) the sending, taking, or storing of technical data that is 1) unclassified, 2) secured using end-to-end encryption, 3) secured using FIPS 140-2 compliant cryptographic modules as prescribed in the regulations, 4) not intentionally sent to a person in or stored in a country proscribed in § 126.1 or the Russian Federation, and 5) not sent from a country proscribed in § 126.1 or the Russian Federation. Moreover, DDTC clarified that data in-transit via the Internet is not deemed to be stored. End-to-end encryption implies the data is kept encrypted at all times between the originator and intended recipient, and the means of decryption are not provided to any third party.

There is no ITAR compliance certification; however, both Azure and Azure Government can help customers subject to ITAR meet their compliance obligations. Except for the Hong Kong region, Azure and Azure Government datacenters are not located in proscribed countries or in the Russian Federation. Azure and Azure Government rely on FIPS 140-2 validated cryptographic modules in the underlying operating system, and provide customers with a wide range of options for encrypting data in transit and at rest, including encryption key management using Azure Key Vault, which can store encryption keys in FIPS 140-2 validated Hardware Security Modules (HSM) under customer control (Customer Managed Keys, CMK). Keys generated inside the Azure Key Vault HSMs are not exportable – there can be no clear version of the key outside the HSMs. This binding is enforced by the underlying HSM. Moreover, Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents do not see or extract customer keys.

Customers are responsible for choosing Azure or Azure Government regions for deploying their applications and data. Moreover, customers are responsible for designing their applications to leverage end-to-end data encryption that meets ITAR requirements. Microsoft does not inspect or approve customer applications deployed in Azure or Azure Government.

Azure Government provides an additional layer of protection to customers through contractual commitments regarding storage of Customer Data in the United States and limiting potential access to systems processing Customer Data to screened US persons. For additional information regarding ITAR,

customers should review "Microsoft Azure Export Controls Whitepaper" available from the Service Trust Portal (see FAQ and White Papers section).

Applicability	Services in scope
Azure	See Azure services in FedRAMP High audit scope.
Azure Government	See Azure Government services in FedRAMP High audit scope.

28 NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) was published in February 2014 as guidance for critical infrastructure organizations to better understand, manage, and reduce their cybersecurity risks. The CSF was developed in response to the Presidential Executive Order on Improving Critical Infrastructure Security, which was issued in February 2013. NIST provided a draft 1.1 update to the CSF in January 2017, incorporating feedback received since the original CSF release. An Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure signed in May 2017 requires US government agencies to use the NIST CSF or any successor document when conducting risk assessments for agency systems. Each agency head is required to produce a risk management report documenting cybersecurity risk mitigation and describing the agency's action plan to implement the CSF.

Microsoft has developed a Customer Responsibility Matrix (CRM) for NIST CSF that lists all control requirements that require customer implementation, shared responsibility controls, and control implementation details for controls owned by Microsoft. For questions about the NIST CSF template or access to the CRM, customers should visit https://servicetrust.microsoft.com/ViewPage/BlueprintLegacy. Moreover, an accredited third-party assessment organization (3PAO) has attested that Microsoft Azure system conforms to the NIST CSF risk management practices, as defined in the *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, dated February 12, 2014. The Azure NIST CSF control mapping demonstrates alignment of the Azure FedRAMP authorized services against the CSF Core. In the course of this assessment, Microsoft also leveraged the NIST CSF Draft Version 1.1, which includes guidance for a new Supply Chain Risk Management category and three additional subcategories. Customers can download the 3PAO attestation letter from the Service Trust Portal (see GRC Assessment Reports section). Also available for download from the Service Trust Portal (see GRC Assessment Reports section) are several NIST CSF specific guides, including the NIST CSF Risk Assessment Checklist, NIST CSF Enablement Detect Function, NIST CSF Enablement Protect Function, and NIST CSF Enablement Identity Function.

Applicability	Services in scope
Azure	See Azure Services in FedRAMP and DoD SRG Audit Scope
Azure Government	See Azure Services in FedRAMP and DoD SRG Audit Scope

29 NIST SP 800-171

The NIST SP 800-171 provides guidelines for the protection of controlled unclassified information (CUI) in nonfederal information systems and organizations. Mapping tables in Appendix D (D1 through D14) provide control mapping between CUI security requirements and relevant security controls in NIST SP 800-53, indicating that NIST SP 800-171 represents a subset of the NIST SP 800-53 controls for which Azure has already been assessed and authorized under the FedRAMP program. Consequently, customers can be assured that FedRAMP High baseline addresses fully and exceeds the requirements of

NIST SP 800-171. All Azure Government services that have received FedRAMP authorizations conform to the NIST SP 800-171 requirements and can accommodate customers looking to deploy CUI workloads.

An accredited third-party assessment organization (3PAO) has attested that Azure Government meets the criteria in the NIST SP 800-171 if the system processes CUI. Customers can download the 3PAO attestation letter from the Service Trust Portal (see GRC Assessment Reports section).

Moreover, the Azure Security and Compliance Blueprint for NIST SP 800-171 is available to help customers deploy a secure and compliant Data analytics, Data warehouse, IaaS web application, and PaaS web application environment that implements a subset of NIST SP 800-171 controls. The NIST SP 800-171 Blueprint consists of four reference architectures with supporting deployment guidance, security control mapping, threat model, and customer responsibility matrix. More information is available from the NIST SP 800-171 Blueprint landing page on Service Trust Portal.

Applicability	Services in scope
Azure	See Azure Services in FedRAMP and DoD SRG Audit Scope
Azure Government	See Azure Services in FedRAMP and DoD SRG Audit Scope

30 Section 508 VPATs

Section 508 is an amendment to the Rehabilitation Act of 1973, a US federal law. Section 508 requires US federal government agencies to give employees and members of the public with disabilities access to electronic information and technology that is comparable to access available to others. Agencies must also consider accessibility when purchasing or using information technology.

A Voluntary Product Accessibility Template (VPAT) is a standardized form developed by the Information Technology Industry Council to document whether a product meets key Section 508 requirements. Federal procurement officers and other buyers can use completed templates to help evaluate products they are considering. Microsoft offers detailed VPATs for many Azure services, describing the accessibility features of those services.

Applicability	VPATs
Azure Azure Government Azure Government for DoD	See Section 508 VPATs for Microsoft products.

Industry Specific

The following compliance offerings are intended to address the needs of customers subject to various industry regulations such as those in financial services, healthcare and life sciences, media and entertainment, education, etc. Azure is not subject directly to oversight by these regulators; however, Azure can help customers meet their own compliance requirements by furnishing a variety of documents ranging from formal independent third-party assessments to guidance documentation and contractual commitments produced by Microsoft.

31 23 NYCRR 500

The State of New York recently adopted a rule that imposes a new set of cybersecurity requirements (23 NYCRR 500) on financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (DFS). This regulation is designed to protect customer data and the information technology systems of regulated institutions. It requires each financial institution to assess its specific risk profile and design a program that addresses the risks. Microsoft has prepared a document ("Microsoft Cloud – NYDFS") to explain how Azure can help financial institutions comply with 23 NYCRR 500 requirements. Customers can download this document from the Service Trust Portal (see Compliance Guides section).

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

32 AFM and DNB (Netherlands)

The primary financial services regulators in the Netherlands are the Dutch Authority for the Financial Markets (Autoriteit Financiële Markten, AFM) and the Dutch Central Bank (De Nederlandsche Bank, DNB). They are responsible for the supervision of banks, pension funds, insurers, payment service providers, investment firms, and other financial institutions. There are several requirements and guidelines that financial institutions in the Netherlands should be aware of when moving to the cloud, including:

- Financial Supervision Act (Wet op het financieel toezicht, FSA), issued by the Dutch legislature in February 2018.
- Decree on Prudential Rules Pursuant to the FSA (Besluit prudentiële regels Wft, "Bpr"), issued by the Dutch government executive branch in January 2018.
- Circulaire Cloud Computing, issued by the DNB in January 2012.
- Commission Delegated Regulation EU 2017/565 of 25 April 2016 supplementing Directive 2014/65 of the European Parliament and of the Council (MODR)
- And others.

DNB's point of view is that cloud computing involving third-party services qualifies as a form of outsourcing. For example, the Circulaire states that DNB expects to be informed of prospective outsourcing arrangements before a supervised Dutch institution engages in cloud computing. Supervised institutions must ensure that operational processes and risks are under control.

To assist financial institutions in the Netherlands with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in the Netherlands" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

33 AMF and ACPR (France)

The French Financial Authority (*Autorité des Marchés Financiers*, AMF) and the French Prudential Authority (*Autorité de Contrôle Prudentiel et de Résolution,* ACPR) are the primary regulators in France responsible for the supervision of financial markets, investment firms, banks, and insurance companies among other financial industry participants. There are several requirements and guidelines that financial institutions in France should be aware of when moving to the cloud, including:

- The AMF General Regulation.
- The Monetary Financial Code.
- ACPR Guidelines on the risks associated with cloud computing.
- Order dated 3-Nov-2014 relating to the internal control of banking sector, payment services, and investment services subject to the ACPR supervision.
- *Commission Nationale de l'Informatique et des Libertés'* (CNIL) recommendations for companies planning to use cloud computing services.
- And others.

The AMF and/or ACPR need to be notified regarding outsourcing arrangements in certain cases involving material outsourcing and particularly if the outsourcing involves "critical or important provision of services or operational tasks and functions". There are also mandatory terms that must be included in contracts with cloud service providers per the Order dated 3-Nov-2014 and the AMF General Regulation.

To assist financial institutions in France with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud Checklist France" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

34 APRA (Australia)

The Australian Prudential Regulation Authority (APRA) oversees banks, credit unions, insurance companies, and other financial services institutions (FSIs) in Australia. Recognizing the momentum towards cloud computing, APRA has called on regulated entities to implement a thoughtful cloud adoption strategy with effective governance, thorough risk assessment, and regular assurance processes. APRA's information paper, "Outsourcing involving shared computing services (including

cloud)", outlines important guidance for regulated entities in their assessment of cloud providers and cloud services.

Customers should review the Microsoft Response to the APRA Information Paper on Cloud, which follows the structure and topics of the APRA's information paper on outsourcing. The paper provides a detailed response to each issue raised by APRA to demonstrate how FSIs can move data and workloads to Azure and comply with the APRA guidance. Moreover, for the next level of detail, the "Microsoft Cloud – Checklist for Financial Institutions in Australia" can be downloaded from the Service Trust Portal (see Compliance Guides section). The checklist covers regulatory issues that need to be addressed under regulations such as APRA CPS 231, APRA PPG 231, and others. More information is available from the Australian FSI Trusted Cloud webpage.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

35 CDSA

The Content Delivery & Security Association (CDSA) Content Protection & Security (CPS) Standard provides guidance and requirements for securing media assets within a Content Security Management System (CSMS). The standard specifies a set of controls designed to ensure the integrity of intellectual property and the confidentiality and security of media assets at every stage of the digital media supply chain.

The CPS certification audit is administered directly by the CDSA and consists of over 300 distinct controls that help secure and manage physical datacenters, harden services, and protect storage facilities. All controls are optimized to handle sensitive and valuable media assets. Once a system is validated by the CDSA assessor, the CDSA issues a certificate of compliance. To maintain compliance, the certified entity must submit the results of annual audits to the CDSA. Customers can download the Azure Media Services Certificate of Compliance as well as the Azure CDSA CPS Audit Report from the Service Trust Portal (see GRC Assessment Reports section). Also available for download from the Service Trust Portal (see Compliance Guides section) is the CDSA CPS Implementation Guide, which describes how Azure Media Services can help customers create CDSA CPS compliant solutions securely, as well as how customers can create, protect, and operate digital media services on Azure.

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

36 CFTC 1.31 (US)

The United States Commodity Futures Trading Commission (CFTC) Rule 1.31 defines recordkeeping obligations using requirements that are similar to those of SEC 17a-4, in addition to specifying that electronic records must be kept for the full 5-yr maintenance period and be readily accessible during that entire period. To address the transition to electronic regulatory records, the CFTC amended and modernized its recordkeeping regulation to adopt principles-based standards that are less prescriptive. The amendments adopted in 2017 provide greater flexibility in how the records need to be maintained and make the regulation more technology neutral.

Azure Immutable Blob Storage can help customers address their records retention requirements. Microsoft retained an independent third-party assessment firm that specializes in records management and information governance to evaluate Azure Immutable Blob Storage compliance with CFTC Rule 1.31(c)-(d) requirements. The resulting report "Cohasset Assessment – Microsoft Azure WORM Storage" can be downloaded from the Service Trust Portal GRC Assessment Reports section. It is the assessor's opinion that Azure Immutable Blob Storage with Policy Lock option when utilized to retain time-based Blobs in a non-erasable and non-rewritable format, meets the relevant storage requirements of CFTC Rule 1.31(c)-(d).

Applicability	Services in scope
Azure	Storage (Blobs) including all tiers (hot, cool, archive).

37 DPP (UK)

The Digital Production Partnership (DPP) partnered with the North American Broadcasters Association (NABA) to develop the NABA DPP Broadcasters Cyber Security Requirements, which are endorsed by chief information security officers from the UK broadcasters as being the minimum set of requirements for cyber security. The DPP worked with broadcasters and supplier security experts to create a self-assessment format designed to enable suppliers to demonstrate commitment to achieving security best practices. This work has led to the establishment of a formal Committed to Security Program that DPP launched in October 2017 with two different logos: Broadcast Checklist and Production Checklist.

Microsoft Azure has been awarded the DPP Committed to Security Mark (Broadcast Checklist) as mentioned on the DPP web site. Moreover, customers can download the Azure NABA DPP Broadcaster Cyber Security Requirements Checklist from the Service Trust Portal (see Compliance Guides section).

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

38 European Banking Authority (EBA)

The European Banking Authority (EBA) is an independent EU authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector. In December 2017, the EBA issued a Final Report on Recommendations on Outsourcing to Cloud Services Providers which outlines, for the first time, a comprehensive approach for addressing outsourcing of cloud computing at an EU-wide level. The EBA recommendations took effect in July 2018, and they build on the general outsourcing guidelines published in 2006 by the Committee of European Banking Supervisors (CEBS).

To assist financial institutions in the EU with cloud adoption, Microsoft published a guidance document addressing key points in EBA's cloud computing recommendations. This document is titled "Microsoft Cloud – European Banking Authority Guidance", and it can be downloaded from the Service Trust Portal (see Compliance Guides section). The purpose of the document is to explain how Microsoft meets the requirements applicable to it as a Cloud Service Provider and to help customers meet their obligations under the EBA framework. Specifically, the document covers:

- Flexibility and adaptation to emerging technologies

- Audit rights for customers and regulators
- Notification to regulators regarding outsourcing activities
- Data residency
- Notification regarding subcontractors
- Business continuity provisions and exit strategies
- Security of data and systems

Microsoft welcomes the Recommendations on Outsourcing to Cloud Service Providers as they provide clarity on cloud usage permissibility, apply a principles-based approach towards measuring risk from a technology-neutral perspective, and strive towards greater harmonization within Europe and beyond.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

39 FACT (UK)

Copyrighted content comes in many forms—pictures, videos, music, contracts, scripts, workflows, art, architecture, and more—and represents the core assets of many businesses. To underscore Microsoft's commitment to protect customers when they entrust such assets to the public cloud, Microsoft Azure has been certified by the Federation Against Copyright Theft (FACT) in the United Kingdom. FACT certification is based on ISO 27001, focusing on physical and digital security, staff screening and training, and access control. The FACT content protection and security program draws on expertise across law enforcement, technology partners, and industry associations to fight copyright infringement and content theft, such as peer-to-peer sharing, illegal disc duplication, and signal theft. Customers can download the Azure FACT certificate.

Applicability	Services in scope
Azure	Automation, Azure Active Directory (Free and Basic), Batch, Cloud Services, Content Delivery Network, Event Hubs, ExpressRoute, Import/Export, Key Vault, Load Balancer, Media Services, Microsoft Azure Portal, Redis Cache, Scheduler, SQL Database, Storage (Blobs, Disks, Files, Queues, Tables) including Premium Storage, Traffic Manager, Virtual Machines, Virtual Network, and supporting infrastructure and platform services.

40 FCA and PRA (UK)

The Prudential Regulation Authority (PRA) is responsible for the prudential supervision of banks, insurance companies, building societies, credit unions, and certain large investment firms. The Financial Conduct Authority (FCA) has responsibility for business supervision of all financial services firms, including those supervised by the PRA, which are therefore dual regulated. The FCA is also responsible for supervision of outsourcing arrangements established by firms not supervised by the PRA.

In July 2016, the FCA published the "FG 16/5 – Guidance for firms outsourcing to the cloud and other third-party IT services" intended to help firms authorized under the Financial Services and Markets Act (FSMA) oversee all aspects of their outsourcing arrangements. To help firms that are authorized and regulated by the FCA and the PRA comply with their regulatory obligations, Microsoft published a document detailing how Azure helps customers meet the standards set out in the FCA Guidance. The

document is titled "Microsoft Cloud – Microsoft Approach to Enabling Compliance with FCA Finalized Guidance", and it can be downloaded from the Service Trust Portal (see Compliance Guides section). The sections in the document track the "Area of interest" titles found in the FCA Guidance for ease of reference and navigation.

Aside from the FCA FG 16/5 Guidance, there are additional requirements and guidelines that financial institutions in the United Kingdom should be aware of when moving to the cloud, including the Financial Services and Markets Act 2000, the Senior Management Arrangements, Systems, and Controls Sourcebook (SYSC) in the FCA Handbook, the European Banking Authority (EBA) Final Report on Recommendations on Outsourcing to Cloud Service Providers EBA/REC/2017/03, and others. To assist UK financial services firms regulated by the FCA and PRA with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in the UK" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains a Compliance Checklist as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

41 FERPA (US)

The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of students' education records, including personally identifiable and directory information. FERPA was enacted to ensure that parents and students age 18 and older can access those records, request changes to them, and control the disclosure of information, except in specific and limited cases where FERPA allows for disclosure without consent. The law applies to schools, school districts, and any other institution that receives funding from the US Department of Education—that is, virtually all public K–12 schools and school districts, as well as most post-secondary institutions, both public and private.

FERPA does not require or recognize audits or other certifications, so any academic institution that is subject to FERPA must assess for itself whether and how its use of a cloud service affects its ability to comply with FERPA requirements. In its Online Services Terms, Microsoft agrees to be designated as a "school official" with "legitimate educational interests" in Customer Data as defined under FERPA. Customer Data would include any student records provided through a school's use of Azure. When handling student education records, Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) just as school officials do. Customers subject to FERPA can download the Azure FERPA Compliance Framework Mapping from the Service Trust Portal (see Compliance Guides section) for assistance with satisfying FERPA compliance requirements.

COPPA and CIPA are additional laws intended to protect the privacy of children; however, they are not directly applicable to Azure. The Children's Online Privacy Protection Act (COPPA) is a US federal law enacted to protect the privacy of children under 13. It is managed by the Federal Trade Commission (FTC). COPPA applies to websites and online services directed to children and stipulates that these sites and services must require parental consent for the collection and use of any personal information belonging to children. The Children's Internet Protection Act (CIPA) was enacted to address concerns about children's access to harmful content over the Internet. The Federal Communications

Commission (FCC) issued rules implementing CIPA and defined requirements for schools and libraries subject to CIPA. Customers enquiring about COPPA and CIPA in the context of Azure adoption should review the section titled Educational Institutions in the Online Services Terms where we explain that customers are responsible for obtaining any parental consent for any end user's use of Microsoft online services.

Applicability	Services in scope
Azure Azure Government	See respective ISO 27001 scope statements.

42 FFIEC (US)

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body comprised of five banking regulators that is responsible for the federal examination of financial institutions in the United States. The FFIEC Examiner Education Office publishes IT Examination Handbooks intended for field examiners from the FFIEC member agencies. The FFIEC Audit IT Examination Handbook contains guidance on third-party reviews of technology service providers that enables financial institutions to review sufficiently detailed independent audit reports of technology service providers (TSPs) as part of their overall responsibility to manage their relationships with TSPs. Specifically, AICPA's SOC 1, SOC 2, and SOC 3 attestation reports are mentioned in the Audit Handbook as examples of independent audit reports pertinent to TSPs. However, FFIEC also mentions that financial institutions should not rely solely on the information contained in these reports and should instead use additional verification and monitoring procedures discussed in more detail in the FFIEC Outsourcing Technology Services IT Examination Handbook.

Azure provides financial institutions with SOC 1 Type 2, SOC 2 Type 2, and SOC 3 attestation reports produced by an independent CPA firm to help customers meet their own FFIEC compliance obligations. For example, the SOC 1 Type 2 attestation is based on the AICPA SSAE 18 standard (see AT-C Section 105) that replaced SAS 70, and it is appropriate for reporting on controls at a service organization relevant to user entities internal controls over financial reporting. This is the formal audit that financial institutions can leverage for third-party reviews of technology service providers when pursuing their own FFIEC specific compliance obligations for assets deployed to Azure. It includes auditor's opinion on control effectiveness to achieve the related control objectives during the specified monitoring period.

Moreover, Azure has developed an Excel-based Cloud Security Diagnostic Tool that customers can download from the Service Trust Portal (see Compliance Guides section). This tool is meant to expedite a risk assessment that a financial institution may want to conduct relative to Azure services. The tool is based on a spreadsheet featuring 19 tabs (each for a separate information security domain) that track requirements set forth by relevant standards and financial services regulations, including FFIEC IT Examination Handbooks. The tool is prepopulated with explanations how Azure complies with requirements applicable to cloud service providers and can assist customers in meeting their own FFIEC compliance requirements. Also available for download in the Compliance Guides section of the Service Trust Portal is the Azure FFIEC Cloud Security Diagnostic workbook companion that offers guidance on the use of Azure cloud services and considerations for customer compliance with FFIEC requirements.

Finally, the Azure Security and Compliance FFIEC Financial Services Blueprint is available to help customers deploy a secure and compliant Data analytics, Data warehouse, IaaS web application, and

PaaS web application environment suitable for the collection, storage, and retrieval of financial data regulated by the FFIEC. The FFIEC Blueprint consists of four reference architectures with supporting deployment guidance, security control mapping, threat model, and customer responsibility matrix. More information is available from the FFIEC Blueprint landing page on Service Trust Portal.

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

43 FINMA (Switzerland)

The Swiss Financial Market Supervisory Authority (FINMA) is Switzerland's independent financial markets regulator with prudential supervision over banks, insurance companies, exchanges, securities dealers, and other financial industry participants. FINMA Circular 2018/3 Outsourcing – Banks and Insurers defines the risk-based supervisory requirements applicable to outsourcing solutions at banks, securities dealers, and insurance companies. Moreover, when moving to the cloud, Swiss financial institutions should be aware of additional requirements and guidelines, including the Swiss Bank Act, Swiss Bank Ordinance, Swiss Insurance Supervision Act, and others.

To assist financial institutions in Switzerland with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in Switzerland" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

44 FINRA 4511 (US)

The Financial Industry Regulatory Authority (FINRA) Rule 4511 relies on SEC 17a-4 for the format in which books and records must be preserved. For example, FINRA states explicitly that "all books and records to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA (Securities Exchange Act) Rule 17a-4". Additionally, FINRA Rule 4511 requires firms to preserve for a period of at least 6 years those FINRA books and records for which there is no specified retention period under the FINRA rules or applicable SEA rules. Effectively, if the books and records pertain to an account, the retention period is mandated to be 6 years following account closure; otherwise, the retention period is for 6 years after such books and records are created.

Azure Immutable Blob Storage can help customers address their records retention requirements. Microsoft retained an independent third-party assessment firm that specializes in records management and information governance to evaluate Azure Immutable Blob Storage compliance with FINRA Rule 4511(c) requirements. The resulting report "Cohasset Assessment – Microsoft Azure WORM Storage"

can be downloaded from the Service Trust Portal GRC Assessment Reports section. It is the assessor's opinion that Azure Immutable Blob Storage with Policy Lock option when utilized to retain time-based Blobs in a non-erasable and non-rewritable format, meets the relevant storage requirements of FINRA Rule 4511(c).

Applicability	Services in scope
Azure	Storage (Blobs) including all tiers (hot, cool, archive).

45 FISC (Japan)

Supporting members, including major financial institutions, insurance and credit companies, securities firms, computer manufacturers, and telecommunications enterprises.

In collaboration with its member institutions, the Bank of Japan, and the Financial Services Agency, the FISC created guidelines for the security of banking information systems. These guidelines include basic auditing standards for computer system controls, contingency planning in the event of a disaster, and development of security policies and standards encompassed in more than 300 controls.

Although the application of these guidelines in a cloud computing environment is not required by regulation, most financial institutions in Japan that implement cloud services have built information systems that satisfy these security standards. Microsoft engaged outside assessors to validate that Microsoft Azure meet the requirements of the FISC Security Guidelines on Computer Systems for Financial Institutions 9th Edition Revised. Financial institutions can rely on this evaluation of compliance for the in-scope infrastructure and platform services of these services. Aside from Azure services listed in table below **Microsoft Cloud App Security** online service is also included in the Scope.

Applicability	Services in scope
Azure	App Service (Mobile Apps and Web Apps), Azure Active Directory (Free and Basic), Azure Advanced Threat Protection, Azure Information Protection (including Azure Rights Management), Batch, BizTalk Services, Cloud Services, ExpressRoute, HDInsight, Media Service, Multi-Factor Authentication, Notification Hubs, Scheduler, Service Bus, SQL Database, Storage (Blobs, Disks, Files, Queues, Tables), Traffic Manager, Virtual Machines, Virtual Network, and supporting infrastructure and platform services.

46 FSA (Denmark)

The Danish Financial Supervisory Authority (FSA, in Danish: Finanstilsynet) is a government agency residing under the Ministry of Industry, Business and Financial Affairs but with a separate board of directors. The principal role of the FSA is to prepare regulatory guidelines for financial institutions in Denmark, cooperate with other authorities and regulators on a regional and international level, and monitor financial institutions' regulatory compliance.

There are several requirements and guidelines that financial institutions in Denmark should be aware of when moving to the cloud, including:

- Danish Act on Financial Institutions (in Danish: Bekendtgørelse af lov om Finansiel Virksomhed), Ministry of Industry, Business and Financial Affairs, released in September 2017.
- Executive Order on Outsourcing of Significant Areas of Activity (In Danish: Bekendtgørelse om outsourcing af væsentlige aktivitetsområder), Ministry of Industry, Business and Financial Affairs, released in January 2010 and amended in December 2017).
- Guideline for Executive Order on Outsourcing of Significant Areas of Activity" (in Danish: Vejledning til bekendtgørelse om outsourcing af væsentlige aktivitetsområder), Ministry of Industry, Business and Financial Affairs, released in May 2010.
- Guidance on Use of Cloud Services as Part of IT-Outsourcing (in Danish: Anvendelse af cloud-tjenester som led I IT-outsourcing), FSA.

To assist financial institutions in Denmark with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in Denmark" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

47 GLBA (US)

The Gramm-Leach-Bliley Act (GLBA) is a US public law that reformed the financial services industry and addressed concerns about consumer privacy protection. It required the Federal Trade Commission (FTC) and other financial services regulators to implement regulation addressing GLBA privacy provisions such as the Financial Privacy Rule and Safeguards Rule. GLBA requirements to safeguard sensitive consumer data apply to financial institutions that offer financial products and services to consumers (e.g., loans, investment advice, etc.). Azure can help customers comply with the security requirements of the GLBA by providing technical and organizational safeguards to help customers maintain security and prevent unauthorized usage.

Azure has developed an Excel-based Cloud Security Diagnostic Tool that customers can download from the Service Trust Portal (see Compliance Guides section). This tool is meant to expedite a risk assessment that a financial institution may want to conduct relative to Azure services. The tool is based on a spreadsheet featuring 19 tabs (each for a separate information security domain) that track requirements set forth by relevant standards and financial services regulations, including GLBA (see Column R in the spreadsheet). The tool is prepopulated with explanations how Azure complies with requirements applicable to cloud service providers and can assist customers in meeting their own compliance requirements, including the security requirements of GLBA.

Applicability	Services in scope

Azure	See ISO 27001 scope statement.

48 GxP (FDA 21 CFR Part 11)

Azure can help customers meet their requirements under Good Clinical, Laboratory, and Manufacturing Practices (GxP), as well as regulations enforced by the US Food and Drug Administration (FDA) under 21 CFR Part 11. There is no GxP or 21 CFR Part 11 certification for cloud service providers; however, Azure has undergone independent third-party audits for quality management and information security, including ISO 9001 and ISO 27001 among many others. Customers deploying applications to Azure should determine the GxP requirements that apply to the computerized system based on its intended use and follow internal procedures governing qualification and/or validation processes to demonstrate that the GxP requirements are met.

Customers should review a white paper "Strategies for Life Sciences Companies using Microsoft Azure with GxP Systems" produced by Accenture to learn how to analyze controls required to leverage Azure, define how Azure can meet those controls, and define the levels of ownership from Life Sciences companies when validating and maintaining GxP systems hosted on Azure. Among other things, the white paper shows how certain FDA regulations (21 CFR Part 820 and 21 CFR Part 11) apply to Azure.

Moreover, Microsoft retained Montrium, an independent organization specializing in quality assurance and regulatory GxP compliance for the life sciences industry, to conduct the Azure GxP qualification review. The resulting qualification guideline is intended for any regulated customer within the life sciences industry, aiming to use the Azure platform to host GxP regulated computerized systems. The guideline identifies the responsibility shared by Microsoft and its customers for meeting the regulatory requirements of FDA 21 CFR Part 11 for electronic records and signatures and EudraLex Volume 4 – Annex 11 for computerized systems. It describes recommended activities and controls that can be established by customers in order to qualify and maintain control over the GxP computerized systems installed on the Azure platform. The qualification approach outlined within this guideline is based on industry best practices with an emphasis on the concepts presented and described within ISPE's GAMP series of Good Practice Guides and PIC/S PI 011-3 Good Practices for Computerized Systems in Regulated GxP Environments.

Applicability	Services in scope
Azure	See Appendix A.
Azure Government	See Appendix B.

49 HDS (France)

Microsoft Azure has been granted the Health Data Hosting (Hébergeurs de Données de Santé, HDS) certification, which is required for all entities hosting personal health data governed by French law. This made Microsoft the first major cloud service provider to meet the strict French standards for storing and processing health data. This certification, required by the revision to the 2018 French Public Health Code, imposes advanced security and privacy requirements on hosting services and cloud providers to ensure that the confidentiality and integrity of sensitive data is adequately protected.

Microsoft Azure compliance with the HDS requirements has been audited and certified by the BSI Group, an independent certifying body accredited by French authorities to conduct HDS audits.

The HDS certification enables healthcare providers in France to use Microsoft cloud services to save costs by improving clinical and operational efficiency, and it opens the door to the development of innovative, cutting-edge healthcare solutions. Providers will be able to develop smart applications or use third-party applications hosted on Azure to implement predictive analytics to personalize healthcare, evaluate and treat patients at a distance (telemedicine), and sharpen therapeutic drug monitoring.

Applicability	Services in scope
Azure	See ISO 27001 scope statement within the France, Amsterdam, and Ireland data centers (Azure Region: Central France, South France, North Europe, and West Europe)

50 HIPAA and the HITECH Act (US)

The Health Insurance Portability and Accountability Act (HIPAA) is a US law that establishes requirements for the use, disclosure, and safeguarding of protected health information (PHI). It applies to covered entities—doctors' offices, hospitals, health insurers, and other healthcare companies—with access to PHI, as well as to business associates, such as cloud service providers, that process PHI on their behalf. The scope of HIPAA was extended with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act that was created to stimulate the adoption of electronic health records and supporting information technology.

HIPAA regulations require that covered entities and their business associates enter into a contract called a Business Associate Agreement (BAA) to ensure the business associates will protect PHI adequately. Azure has enabled the physical, technical, and administrative safeguards required by HIPAA and the HITECH Act inside the in-scope Azure services, and offers a HIPAA BAA as part of the Microsoft Online Services Terms to all customers who are covered entities or business associates under HIPAA for use of such in-scope Azure services. In the BAA, Microsoft makes contractual assurances about data safeguarding, reporting (including breach notifications), data access in accordance with HIPAA and the HITECH Act, and many other important provisions. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune, Microsoft Power BI and Microsoft Healthcare Bot** online services are also included.

Customers subject to HIPAA/HITECH Act compliance obligations should review Microsoft Azure HIPAA/HITECH Act Implementation Guidance, as well as the white paper "Practical guide to designing secure health solutions using Microsoft Azure" to learn about concrete steps needed to maintain compliance on Azure and to better understand what it takes to adopt a cloud platform in a secure manner. Also available to customers is the Azure Security and Compliance HIPAA/HITRUST Blueprint, which offers a turnkey deployment of an Azure PaaS solution to demonstrate how to securely ingest, store, analyze, and interact with health data while addressing industry compliance requirements.

Applicability	Services in scope
Azure	See Appendix A.
Azure Government	See Appendix B.

51 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 below it. An organization with the highest level, CFS-certified, meets all the CSF certification requirements. Microsoft Azure is one of the first hyperscale cloud service providers to receive a formal certification for the HITRUST CSF (available for download from the Service Trust Portal GRC Assessments Reports section). Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune, Microsoft Power BI and Microsoft Healthcare Bot** online services are also received HITRUST CSF certification.

Also available to customers is the Azure Security and Compliance HIPAA/HITRUST Blueprint, which offers a turnkey deployment of an Azure PaaS solution to demonstrate how to securely ingest, store, analyze, and interact with health data while addressing industry compliance requirements.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	App Service (API Apps, Mobile Apps, Web Apps), Application Gateway, Automation, Azure Active Directory (Free and Basic), Azure Cosmos DB, Azure DNS, Azure Monitor, Azure Resource Manager, Azure Site Recovery, Backup, Batch, Cloud Services, Event Hubs, ExpressRoute, Functions, HDInsight, IoT Hub, Key Vault, Load Balancer, Machine Learning Studio (formerly Machine Learning), Media Services, Microsoft Azure Portal, Multi-Factor Authentication, Network Watcher, Notification Hubs, Power BI Embedded, Redis Cache, Scheduler, Service Bus, Service Fabric, Azure Synapse Analytics, SQL Database, Storage (Blobs, Disks incl. Managed Disks, Files, Queues, Tables) including Cool and Premium Storage, Stream Analytics, Traffic Manager, Virtual Machine Scale Sets, Virtual Machines, Virtual Network, VPN Gateway, and supporting infrastructure and platform services.
Azure Government	See Appendix B.

52 K-ISMS

Based on a rigorous evaluation by the Korea Internet & Security Agency (KISA), Microsoft Azure achieved the Korea Information Security Management System (K-ISMS) certification to host data. The certification covers Azure services that encompass compute, storage, networking, databases, and security, and the datacenter infrastructure of the Microsoft Korea Central and Korea South regions. The specifications for K-ISMS certification are based on ISO/IEC 27001, ISO/IEC 27018, and other international standards that govern the hosting of data.

Achieving this certification means Azure customers in Korea can more easily demonstrate adherence to local legal requirements to protect key digital information assets and meet KISA compliance standards more easily. In addition, Korean organizations that have a legislated mandate to obtain their own K-ISMS certification—certain internet and information network service providers, large hospitals and schools, and so on—can more efficiently meet their own KISMS compliance requirements by building on the Azure certification.

The Azure K-ISMS certification can be reviewed for details. The audit covered the measures Microsoft takes to secure data and protect its confidentiality including the:

- Certification of Microsoft business cloud services (with annual audits for compliance) to ISO/IEC 27001:2013 Information Security Management Standards.
- High level of privacy protection based on Microsoft compliance with the ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud.
- Layered approach in how Microsoft datacenters are designed, built, and operated to strictly control physical access to the areas where customer data is stored.

Aside from Azure services listed in Appendices A, **Microsoft Intune, Microsoft Power BI and Microsoft Healthcare Bot** online services are also included in the Azure K-ISMS certification.

Applicability	Services in scope
Azure	See Appendix A.

53 KNF (Poland)

The Polish Financial Supervision Authority (*Komisja Nadzoru Finansowego,* KNF) is the financial regulatory authority in Poland, responsible for supervising the financial markets, including the oversight over banking, capital markets, insurance, pension schemes, and other market sectors. There are several requirements and guidelines that financial institutions in Poland should be aware of when moving to the cloud, including:

- The Banking Act of 1997
- 2017 KNF Announcement regarding the use of data processing services in cloud computing environments
- 2013 Recommendation D on the management of information technology at banks
- 2014 guidelines on the management of information technology and ICT environment security at insurance companies, investment firms, and general pension companies
- And others.

The Banking Act does not regulate cloud services directly but instead sets out legal requirements for the outsourcing of banking operations. Cloud services could be subject to the Banking Act provisions if the outsourced services are of key significance for the bank, or if outsourcing involves giving the service provider access to sensitive data subject to banking secrecy.

To assist financial institutions in Poland with cloud adoption, Microsoft published a guidance document titled “Microsoft Cloud Checklist Poland” that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

54 MARS-E (US)

In 2012, the Center for Medicare and Medicaid Services (CMS) published the Minimum Acceptable Risk Standards for Exchanges (MARS-E) in accordance with CMS information security and privacy programs. The suite of documents, including guidance, requirements, and templates, was designed to address mandates of the Patient Protection and Affordable Care Act (ACA) and regulations of the Department of Health and Human Services that apply to the ACA. The National Institute of Standards and Technology (NIST) Special Publication 800-53 serves as the parent framework that establishes the security and compliance requirements for all systems, interfaces, and connections between ACA-mandated health exchanges and marketplaces.

Following the updated NIST SP 800-53 R4, CMS revised the MARS-E framework to align with the updated controls and parameters in NIST SP 800-53 R4, publishing MARS-E 2.0 in 2015. These updates address the confidentiality, integrity, and availability in health exchanges of protected data, which includes personally identifiable information, protected health information, and federal tax information. The MARS-E 2.0 framework aims to secure this protected data and applies to all ACA administering entities, including exchanges or marketplaces—federal, state, state Medicaid, or Children's Health Insurance Program (CHIP) agencies—and supporting contractors.

There is no formal certification process for MARS-E. However, Microsoft maintains a FedRAMP High authorization for Azure and for Azure Government issued by the FedRAMP Joint Authorization Board (JAB). Although FedRAMP does not specifically focus on MARS-E, the MARS-E control requirements and objectives are very closely aligned with FedRAMP and serve to protect the confidentiality, integrity, and availability of data on Azure.

Applicability	Services in scope
Azure	See Azure Services in FedRAMP and DoD SRG Audit Scope
Azure Government	See Azure Services in FedRAMP and DoD SRG Audit Scope

55 MAS and ABS (Singapore)

In July 2016, the Monetary Authority of Singapore (MAS) issued an updated version of the MAS Guidelines on Outsourcing, setting out MAS expectations for outsourcing by financial institutions in Singapore. The MAS Guidelines on Outsourcing emphasize that financial institutions can use cloud services, including public cloud, and that they stand to benefit from doing so. The MAS Guidelines on

Outsourcing apply to all regulated financial institutions in Singapore, including banks, insurance companies, and trust companies.

Shortly after the release of the MAS Guidelines on Outsourcing, the Association of Banks in Singapore (ABS) introduced the ABS Cloud Implementation Guide, a non-binding practical guide designed to assist banks in Singapore as they implement cloud services. The ABS Cloud Implementation Guide applies only to banks and not to other categories of financial institutions.

In response to the release of the MAS Guidelines on Outsourcing and the ABS Cloud Implementation Guide, Microsoft produced a document to:

- Help financial institutions understand the key issues raised by the MAS Guidelines and the ABS Guide as they apply to cloud services
- Set out Microsoft's interpretations of and responses to each of the key issues
- Provide financial institutions with information about how Microsoft helps facilitate compliance with the new guidelines

The document is titled "Microsoft Cloud – Singapore MAS and ABS requirements implementation guide," and it can be downloaded from the Service Trust Portal (see Compliance Guides section).

Moreover, to assist financial institutions in Singapore with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in Singapore" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains a Compliance Checklist as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

56 MPAA (US)

The Motion Picture Association of America (MPAA) provides best-practices guidance and control frameworks to help major studio partners and vendors design infrastructure and solutions to ensure the security of digital film assets. The MPAA also performs content security assessments on behalf of its member companies. In February 2016, Microsoft Azure became the first hyperscale, multitenant cloud service provider to successfully complete a formal assessment by independent MPAA auditors and comply with all three of the MPAA content security best practices frameworks: Common, Application, and Cloud Security Guidelines.

The MPAA assessment covers 48 security topics in the Common Guidelines and an additional six in the Application and Cloud Security Guidelines. These topics are built on industry-accepted security standards such as ISO 27001 and NIST SP 800-53, and are aligned to industry best practices, such as the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

The formal assessment of Azure compliance means that companies who do business with major studios can use Azure to help reduce the IT costs that are normally associated with the secure creation, management, storage, and distribution of content while complying with MPAA requirements. Azure services in scope for the MPAA assessment provide a content workflow engine in the cloud that

customers can use to build secure and scalable production processes while protecting media assets downstream.

Customers can download Azure responses to the Common Guidelines and the Application and Cloud Security Guidelines from the Service Trust Portal (see Compliance Guides section).

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

57 NBB and FSMA (Belgium)

The primary financial services regulators in Belgium are the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA). The NBB is responsible for prudential supervision of credit institutions, insurers, stockbroking firms, settlement and clearing institutions, and other financial institutions. Moreover, NBB has been designated the national authority in charge of macroprudential policy contributing to the stability of the financial system. The FSMA is responsible for the supervision of financial markets and financial information disseminated by companies, compliance with conduct of business rules, financial services providers and intermediaries, supplementary pensions, etc.

There are several requirements and guidelines that financial institutions in Belgium should be aware of when moving to the cloud, including:

- Circular NBB PPB 2004/5 on sound management practices in outsourcing by credit institutions and investment firms and the broadly equivalent provisions of the Circular FSMA dated 5 June 2007 on the organizational requirements for firms providing investment services.
- Circular NBB_2009_17 on financial services via the Internet: Prudential requirements.
- Circular NBB_2015_32 on additional prudential expectations regarding operational business continuity and security of systemically important financial institutions.

To assist financial institutions in Belgium with cloud adoption, Microsoft published a guidance document titled “Microsoft Cloud – Checklist for Financial Institutions in Belgium” that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

58 NEN 7510:2011 (Netherlands)

Many healthcare organizations in the Netherlands have to perform periodic audits and demonstrate compliance with the NEN 7510 standard. When using Azure, some of the NEN 7510 controls for

deployed applications are managed by Microsoft. Even though Microsoft is not subject to compliance with NEN 7510, Dutch healthcare organizations are seeking ways to demonstrate compliance with NEN 7510 when using Azure. They need to determine if the Azure services they are using meet the requirements of NEN 7510.

Microsoft retained an independent, third-party auditing firm to analyze the extent to which current Azure certifications and attestations (such as ISO 27001 and SOC 2 Type 2) cover the part of NEN 7510 that Microsoft is responsible for. The resulting NEN 7510 Coverage Report provides a mapping of these existing certifications and attestations to the controls listed in the NEN 7510 standard. Customers in the Dutch healthcare industry can use the report as a tool to help adopt Azure in a NEN 7510 compliant way. The report clearly demonstrates which NEN 7510 controls are covered by Microsoft and which controls remain to be covered by the customers. The "Microsoft Cloud – Azure and Office 365 NEN 7510-2011 Standard Coverage" report can be downloaded from the Service Trust Portal GRC Assessment Reports section. Also available for download is the "Microsoft Cloud – Azure and Office 365 NEN 7510-2011 Standard Coverage User Guide" (see the Service Trust Portal Compliance Guides section).

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

59 NERC

The North American Electric Reliability Corporation (NERC) is a nonprofit regulatory authority whose mission is to ensure the reliability of the North American bulk power system. NERC is subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. In 2006, FERC granted the Electric Reliability Organization (ERO) designation to NERC in accordance with the Energy Policy Act of 2005 (U.S. Public Law 109-58). NERC develops and enforces reliability standards known as NERC Critical Infrastructure Protection (CIP) standards.

All bulk power system owners, operators, and users must comply with NERC CIP standards. These entities are required to register with NERC. Cloud Service Providers and third-party vendors are not subject to NERC CIP standards; however, the CIP standards include goals that should be considered when Registered Entities use vendors in the operation of the Bulk Electric System (BES). Microsoft customers operating Bulk Electric Systems are wholly responsible for ensuring their own compliance with NERC CIP standards. Neither Azure nor Azure Government constitutes a BES or BES Cyber Asset.

As stated by NERC in the current set of CIP standards and NERC's Glossary of Terms, BES Cyber Assets perform real-time functions of monitoring or controlling the BES, and would affect the reliable operation of the BES within 15 minutes of being impaired. To properly accommodate BES Cyber Assets and Protected Cyber Assets in cloud computing, existing definitions in NERC CIP standards would need to be revised. However, there are many workloads that deal with CIP sensitive data and do not fall under the 15-minute rule, including the broad category of BES Cyber System Information (BCSI).

Both Azure and Azure Government are suitable for Registered Entities deploying certain workloads subject to NERC CIP standards, including BCSI workloads. Microsoft makes the following documents available to Registered Entities interested in deploying data and workloads subject to NERC CIP compliance obligations in Azure or Azure Government:

- **NERC CIP Standards and Cloud Computing** is a white paper that discusses compliance considerations for NERC CIP requirements based on established third-party audits that are applicable to cloud service providers such as FedRAMP. It covers background screening for cloud operations personnel and answers common question about logical isolation and multi-tenancy that are of interest to Registered Entities. It also addresses security considerations for on-premises vs. cloud deployment.
- **Cloud Implementation Guide for NERC Audits** is a guidance document that provides control mapping between the current set of NERC CIP standards requirements and NIST SP 800-53 Rev 4 control set that forms the basis for FedRAMP. It is designed as a technical how-to guidance to help Registered Entities address NERC CIP compliance requirements for assets deployed in the cloud. The document contains pre-filled Reliability Standard Audit Worksheets (RSAWs) narratives that help explain how Azure controls address NERC CIP requirements, as well as guidance for Registered Entities on how to use Azure services to implement controls that they own.

The NERC ERO Enterprise released a Compliance Monitoring and Enforcement Program (CMEP) practice guide to provide guidance to ERO Enterprise CMEP staff when assessing a Registered Entity's process to authorize access to designated BCSI storage locations and any access controls the Registered Entity implemented. Moreover, NERC reviewed Azure control implementation details and FedRAMP audit evidence related to NERC CIP-004-6 and CIP-011-2 standards that are applicable to BCSI. Based on the ERO issued practice guide and reviewed FedRAMP controls to ensure Registered Entities encrypt their data, no additional guidance or clarification is needed for Registered Entities to deploy BCSI and associated workloads in the cloud; however, Registered Entities are ultimately responsible for compliance with NERC CIP standards according to their own facts and circumstances. Registered Entities should review the Cloud Implementation Guide for NERC Audits for help with documenting their processes and evidence used to authorize electronic access to BCSI storage locations, including encryption key management used for BCSI encryption in Azure and Azure Government.

Applicability	Services in scope
Azure	See Azure Services in FedRAMP and DoD SRG Audit Scope
Azure Government	See Azure Services in FedRAMP and DoD SRG Audit Scope

60 OSFI (Canada)

The Office of the Superintendent of Financial Institutions (OSFI) is an independent agency of the Government of Canada responsible for the prudential regulation and supervision of federally regulated financial institutions. OSFI published the OSFI B-10 Guidelines on the Outsourcing of Business Activities, Functions, and Processes to set out expectations for federally regulated entities that outsource their business activities to a service provider. A memorandum published subsequently by OSFI reminded federally regulated financial institutions that B-10 Guidelines remain current and continue to apply to technology-based outsourcing services.

The financial institution's use of cloud services must also comply with the Personal Information Protection and Electronic Documents Act (PIPEDA), and in some instances one or more of the provincial data privacy laws.

To assist financial institutions in Canada with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in Canada" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

61 PCI DSS Level 1

The Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data. Compliance with PCI DSS is required for any organization that stores, processes, or transmits payment and cardholder data. Microsoft Azure maintains a PCI DSS validation using an approved Qualified Security Assessor (QSA) and is certified as compliant under PCI DSS version 3.2.1 at Service Provider Level 1. The Attestation of Compliance (AOC) produced by the QSA is available to customers for download. Customers who want to develop a cardholder environment or card processing service can leverage the Azure validation, thereby reducing the associated effort and costs of getting their own PCI DSS validation. Aside from Azure services listed in Appendices A and Azure Government services in Appendix B **Microsoft Intune, Microsoft Power BI, Microsoft Healthcare Bot and Microsoft Defender Advanced Threat Protection** online services are also included in the PCI DSS version 3.2.1 Attestation of Compliance.

It is, however, important to understand that Azure PCI DSS compliance status does not automatically translate to PCI DSS validation for the services that customers build or host on the Azure platform. Customers are responsible for ensuring that they achieve compliance with PCI DSS requirements. The Azure PCI DSS Responsibility Matrix specifies areas of responsibility for each PCI DSS requirement, and whether it is assigned to Azure or the customer, or if the responsibility is shared. Moreover, customers should review the Azure Security and Compliance PCI DSS Blueprint, which provides guidance for the deployment of a PCI DSS-compliant Platform as a Service (PaaS) environment suitable for handling sensitive payment card data.

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	App Service (API Apps, Mobile Apps, Web Apps), Application Gateway, Azure Active Directory (Free and Basic), Azure Cosmos DB, Azure Resource Manager, Azure Site Recovery, Batch, Backup, Cloud Services, Event Hubs, ExpressRoute, HDInsight, IoT Hub, Key Vault, Load Balancer, Machine Learning Studio, Media Services, Microsoft Azure Portal, Multi-Factor Authentication, Notification Hubs, Power BI Embedded, Redis Cache, Scheduler, Service Bus, Service Fabric, Azure Synapse Analytics, SQL Database, Storage (Blobs, Disks, Files, Queues,

	Tables), Stream Analytics, Traffic Manager, Virtual Machine Scale Sets, Virtual Machines, Virtual Network, VPN Gateway, and supporting infrastructure and platform services.
Azure Government	See Appendix B.

62 RBI and IRDAI (India)

The Reserve Bank of India (RBI), Insurance Regulatory and Development Authority of India (IRDAI), Ministry of Electronics and Information Technology (MEITY), Ministry of Finance, Securities and Exchange Board of India (SEBI), and National Critical Information Infrastructure Protection Centre (NCIIP) are some of the key financial industry regulators in India overseeing banks, insurance organizations, and market infrastructure institutions. The financial services regulatory landscape in India is broad, and it includes:

- Guidelines on Managing Risk and Code of Conduct in Outsourcing of Financial Services by Banks, published by the RBI in November 2006
- Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, published by the RBI in April 2011
- Outsourcing of Activities by Indian Insurers Regulation, published by the IRDAI in 2017
- And others as documented in the "Microsoft Cloud – Checklist for Financial Institutions in India" available to customers from the Service Trust Portal.

Moreover, the financial institution's use of cloud services must also comply with privacy rules, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Financial institutions must report outsourcing arrangements where the scale and nature of the activities outsourced by the financial institution are significant or require extensive data sharing with service providers. Insurance organizations are required to report outsourcing of certain support functions of core activities within 45 days of entering into an outsourcing agreement.

To assist financial institutions in India with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in India" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape;
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Applicability	Services in scope
Azure	See SOC 2 Type 2 scope statement.

63 SEC Regulation SCI

In November 2014, the SEC adopted Regulation Systems Compliance and Integrity (and Form SCI for reporting SCI events) to bolster the technology infrastructure in the US securities markets. The regulation is designed to reduce the frequency of system outages, improve resiliency when such incidents do occur, and increase SEC oversight of securities market technology and enforcement of its regulations.

The SCI rules apply to SCI entities, which include such self-regulatory organizations (SROs) as stock and options exchanges, registered clearing agencies, and alternative trading systems (ATSs). The rules primarily regulate the systems that directly support key securities market functions: trading, clearance and settlement, order routing, market data, market regulation, and market surveillance.

The US Securities and Exchange Commission (SEC) adopted Regulation SCI to strengthen the technology infrastructure of the financial organizations that operate and support the US securities markets. Under SEC oversight, its requirements are designed to ensure that these systems have high availability, strong resiliency, and low latency (high volume of messages with little delay).

To help guide US financial services customers who must comply with this regulation, Microsoft has published the Microsoft Azure SEC Regulation Systems Compliance and Integrity Cloud Implementation Guide. The guidance within this document:

- Provides an overview of overall Azure capabilities that support strong resiliency, high availability, and low latency.
- Makes clear which control areas and regulatory aspects Azure addresses. This point-by-point mapping of Azure features and services to SCI requirements measures Azure compliance against the regulatory framework. It also helps customers understand where they can shift security responsibilities to Azure that they had fully owned when they operated on premises. These capabilities are backed by the promises Microsoft makes in Azure SLAs.
- Specifies each Regulation SCI requirement that is the customer's responsibility to address, and offers Azure documentation and services to help them address these responsibilities.

This document provides a thorough checklist of critical Regulation SCI focus areas. This will help financial organizations understand how they can adopt Azure to help assure their regulators, customers, and leadership that they can comply with the applicable regulatory requirements.

Applicability	Services in scope
Azure	Storage (Blobs) including all tiers (hot, cool, archive).

64 SEC 17a-4 (US)

The SEC Rule 17a-4 was established by the United States Securities and Exchange Commission (SEC) to regulate records retention requirements for securities broker-dealers. The SEC has documented recordkeeping requirements, including retention periods, in 17 CFR 240.17a-3 and 240.17a-4. The SEC subsequently amended 17 CFR 240.17a-4 paragraph (f) and issued two interpretative releases pertaining to paragraph (f) to expressly allow books and records to be retained on electronic storage media, subject to meeting certain conditions. The SEC Rule 17a-4(f) clarified that electronic storage combined with proper software to prevent alteration or erasure of records is acceptable. Retention periods vary

from 3 to 6 years based on record types, with immediate accessibility mandated for the first 2 years. Moreover, one of the interpretative releases requires the storage system to be capable of retaining records beyond the SEC-established retention period to comply with subpoenas, legal hold, or other similar requirements.

Records retention requirements established by the SEC Rule 17a-4(f) are relied upon by other regulators such as the Financial Industry Regulatory Authority (FINRA) and Commodity Futures Trading Commission (CFTC) as described elsewhere in this document. Azure Immutable Blob Storage can help customers address their records retention requirements. Microsoft retained an independent third-party assessment firm that specializes in records management and information governance to evaluate Azure Immutable Blob Storage compliance with SEC 17a-4(f) requirements. The resulting report "Cohasset Assessment – Microsoft Azure WORM Storage" can be downloaded from the Service Trust Portal GRC Assessment Reports section. It is the assessor's opinion that Azure Immutable Blob Storage with Policy Lock option when utilized to retain time-based Blobs in a non-erasable and non-rewritable format, meets the relevant storage requirements of SEC Rule 17a-4(f).

Applicability	Services in scope
Azure	Storage (Blobs) including all tiers (hot, cool, archive).

65 Shared Assessments

The Shared Assessment Program (formerly known as BITS Shared Assessments) is used by many commercial, retail, and investment banks around the world as a proxy for managing their third-party vendor risk assessment process. Microsoft Azure aligns to the Program's Standard Information Gathering (SIG) questionnaire and the Agreed Upon Procedures (AUP) by way of Azure's self-assessment to the Cloud Security Alliance (CSA) STAR program. Azure maintains STAR registry submissions based on both the Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ). The CCM maps to the Shared Assessments SIG v6.0 and AUP v5.0. Azure also maintains formal CSA STAR Certification and CSA STAR Attestation as documented in the STAR registry. Customers can download the "Azure Standard Response to Request for Information – Security, Privacy, and Compliance" from the Service Trust Portal (see FAQ and White Papers section).

Applicability	Services in scope
Azure Azure Government	See respective ISO 27001 scope statements.

66 SOX (US)

The Sarbanes-Oxley Act of 2002 (SOX) is a US federal law administered by the Securities and Exchange Commission (SEC). There is no SOX certification or validation for cloud service providers; however, Azure can help customers meet their obligations under SOX, which is heavily influenced by customer's internal processes especially when it comes to controls for financial reporting. Customers enquiring about Azure SOX compliance should review the Azure SOC 1 Type 2 attestation that is based on the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) standard (see AT-C Section 105) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). This attestation has replaced SAS 70, and it is appropriate for reporting on controls at a service organization relevant to user entities internal controls over financial

reporting. Customers can download this attestation report from the Service Trust Portal. Moreover, Azure has produced customer guidance for SOX that is available for download from the Service Trust Portal (see Compliance Guides section). It covers case studies and lessons learned from migrating internal Microsoft SOX relevant applications to Azure.

Applicability	Services in scope
Azure Azure Government	See respective SOC 2 Type 2 scope statements.

67 TISAX (Germany)

The protection of business processes and information is a core management task in any industry. In the automotive industry, connected and autonomous vehicles, cloud-based services, and digital communication between OEM and supplier have increased the pressure for information security, data protection, and trustworthy solutions. The Trusted Information Security Assessment Exchange (TISAX) developed by the German Association of the Automotive Industry supplies that level of trusted security standards for the industry.

Applicability	Services in scope
Azure	See respective ISO 27001 scope statements.

Region / Country Specific

The following compliance offerings are specific to various regional and country laws and regulations. Some of these offerings are based on independent third-party certifications and attestations, whereas others provide contract amendments and guidance documentation to help customers meet their own compliance obligations.

68 Argentina PDPA

In accordance with the Argentine National Constitution, the Argentina Personal Data Protection Act 25,326 aims to protect personal information recorded in data files, registers, banks, and elsewhere to help protect the privacy of individuals, and also provide a right of access to the information that may be recorded about them. In a data transfer agreement available to customers, Microsoft contractually commits that Azure in-scope services have implemented the applicable technical and organizational security measures stated in Regulation 11/2006 of the Argentine Data Protection Authority. Moreover, Microsoft makes additional important commitments regarding notifications, auditing of our facilities, and use of subcontractors.

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

69 Australia IRAP

The risk management framework used by the Australian Cyber Security Center (ACSC) Information Security Manual (ISM) draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Within this risk management framework, the identification of risks and selection of security controls can be undertaken using a variety of risk management standards, such as International Organization for Standardization (ISO) 31000:2018, Risk management – Guidelines. Broadly, the risk management framework used by the ISM has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system.

The Information Security Registered Assessor Program (IRAP) provides a comprehensive process for the independent assessment of a system's security against the ISM controls and is the mechanism for cloud services to assess security controls within their platforms. An IRAP assessment has been completed for the Azure in-scope services for the processing of government data up to and including at the PROTECTED level in Microsoft Australian-based public cloud. Additional compensating controls are to be implemented on a risk-managed basis by individual agencies prior to agency authorisation and subsequent use of these cloud services. The ACSC encourages adoption of a risk-managed approach with respect to the controls listed in the Australian Government Information Security Manual (ISM) and Protective Security Policy Framework (PSPF).

Through the previous Australian Government certification process, Azure was IRAP assessed and certified by the ACSC at both the Unclassified Dissemination Limiting Markings (DLM) and PROTECTED levels. This resulted in Azure being included on the Certified Cloud Services List (CCSL) which was used to identify cloud services that had successfully completed an IRAP assessment and awarded certification by

the ACSC. Azure remains on the CCSL for services that have been previously assessed by the ACSC. Microsoft will continue to have services IRAP assessed, and agencies will conduct the approval process. Agencies can engage the ACSC through their normal channels for assistance in that approval process. To assist customers with their authorisation decision, Microsoft makes our IRAP assessment report and supporting documents available to customers and partners on an Australia-specific page of the Microsoft Service Trust Portal.

Also available to customers is the Australia PROTECTED Blueprint Guidance that consists of reference architecture for IaaS and PaaS applications, threat model, and control implementation guidance. For more information, see the AU-PROTECTED Blueprint landing page on Service Trust Portal. This Blueprint enables customers to deploy Azure solutions that are suitable for processing, storage, and transmission of sensitive and official information that is classified up to and including PROTECTED. Additional documents and configuration guidance for operating at PROTECTED are available from the Azure Australia Microsoft Docs page.

Applicability	Services in scope
Azure	See Appendix A.

70 Canadian Privacy Laws

Canadian privacy laws—such as the Privacy Act, Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta Personal Information Protection Act (PIPA), and British Columbia Freedom of Information and Protection of Privacy Act (BC FIPPA)—aim to protect the privacy of individuals and give them the right to access information gathered about them. The laws require organizations to take reasonable steps to safeguard information in their custody or control and cover personal information that is held and processed by governments and private organizations in data files, registers, and elsewhere.

To assist Canadian customers with cloud adoption, Microsoft published a guidance document titled "Microsoft Cloud – Checklist for Financial Institutions in Canada" that can be downloaded from the Service Trust Portal (see Compliance Guides section). This document contains:

- Overview of the regulatory landscape, including privacy regulations
- Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Azure cloud services against those issues; and
- Pointers to additional information.

Compliance Checklist can be used as a tool to measure compliance against a regulatory framework and to help customers conduct their own risk assessment.

Ultimately, the responsibility and ownership of personal data lies with our business customers, per the Online Services Terms. However, Microsoft contractually commits that Azure in-scope services have implemented security safeguards to help them protect the privacy of individuals, based on established industry standards such as ISO 27001 and SOC 2 Type 2. We have assessed our practices in risk, security, and incident management; access control; data integrity protection; and other areas relative to the recommendations from the Office of the Privacy Commissioner of Canada and have determined that the in-scope services are capable of meeting those recommendations.

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

71 China GB 18030:2005

GB 18030 is the Chinese ideographic character set and encoding standard mandated by the Chinese government. Microsoft Azure operated by 21Vianet is certified as compliant with the mandatory part of this standard by the China Electronics Standardization Institute (CESI).

Applicability	Services in scope
Azure in China	See Trust Center for more information.

72 China DJCP (MLPS) Level 3

Microsoft Azure operated by 21Vianet was evaluated by an assessment organization authorized by the Ministry of Public Security (MPS) in accordance with GB/T 22239*2019 Information Security Technology—Baseline for classified protection of cybersecurity* and *GB/T 28448-2019 Information Security Technology—Evaluation requirement for classified protection of cybersecurity.* The evaluation organization confirmed Microsoft Azure operated by 21Vianet compliant with DJCP 2.0 requirements and rate as Level 3 in terms of classified protection of cybersecurity.

Applicability	Services in scope
Azure in China	See Trust Center for more information.

73 China TCS

Trusted Cloud Service Evaluation is a band of cloud service evaluation under China Academy of Information and Communications Technology (CAICT). It is a serial of quality evaluation system organized by the Trusted Cloud Service Workgroup of Open Source Cloud Alliance for Industry (OSCA) under the guide of Ministry of Industry and Information Technology of China (MIIT). Trusted Cloud Service Evaluation is also the authoritative evaluation system for cloud computing services in China. The evaluation aims to cultivate the Chinese public cloud service market, enhance users' confidence on cloud services, and protect certified cloud service providers. Microsoft Azure operated by 21Vianet has passed the evaluation and obtained Trusted Cloud Service Evaluation of Virtual Machine, Cloud Storage, Cloud Database, Load Balancing, Cloud Engine and Cloud Backup.

Applicability	Services in scope
Azure in China	See Trust Center for more information.

74 EU EN 301 549

Accessibility requirements suitable for public procurement of ICT products and services in Europe (EN 301 549) is a set of standards for information and communications technologies (ICT) products and services, including websites, software, and digital devices. EN 301 549 was published in 2014 by the European Telecommunications Standards Institute (ETSI) in response to a request from the European Commission and is intended for use in procurement by government and public-sector organizations.

Applicability	EN 301 549 reports
Azure Azure Government	See list of EN 301 459 reports for Microsoft products.

75 EU ENISA IAF

The European Network and Information Security Agency (ENISA) Information Assurance Framework (IAF) is a set of assurance criteria that organizations can review with cloud service providers to ensure they have sufficient protections in place around Customer Data. The IAF is intended to assess the risk of cloud adoption and reduce the assurance burden on cloud service providers.

Microsoft Azure aligns to the IAF by way of Azure's self-assessment to the Cloud Security Alliance (CSA) STAR program. Azure maintains STAR registry submissions based on both the Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ). The CCM maps to the IAF. Azure also maintains formal CSA STAR Certification and CSA STAR Attestation as documented in the STAR registry. Customers can download the "Azure Standard Response to Request for Information – Security, Privacy, and Compliance" from the Service Trust Portal (see FAQ and White Papers section).

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

76 EU Model Clauses

European Union (EU) data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA), which includes all EU countries and Iceland, Liechtenstein, and Norway. Microsoft offers customers the EU Standard Contractual Clauses (EU Model Clauses) that provide specific guarantees around transfers of personal data for in-scope services. Microsoft provided its Standard Contractual Clauses to the EU's Article 29 Working Party for review and approval. The Article 29 Working Party includes representatives from the European Data Protection Supervisor, the European Commission, and each of the 28 EU Data Protection Authorities (DPAs). The group determined that implementation of the provisions in Microsoft agreements was in line with their stringent requirements.

The EU Model Clauses ensure that any personal data leaving the EU will be transferred in accordance with EU data protection law and meet the requirements of the EU Data Protection Directive 95/46/EC. Microsoft makes the EU Model Clauses available to customers as described in the Online Services Terms.

Applicability	Services in scope
Azure	See Microsoft Azure Core Services in Appendix A of the Online Services Terms.

77 EU-US Privacy Shield

Microsoft and its controlled U.S. subsidiaries (Microsoft) comply with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Microsoft has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. Microsoft's participation in the Privacy Shield applies to all personal data that is subject to the Microsoft

Privacy Statement and is received from the European Union, European Economic Area, and Switzerland. Microsoft will comply with the Privacy Shield Principles with respect to such personal data. More information is available from the EU-US Privacy Shield page.

Applicability	EU-U.S. Privacy Shield compliance
Microsoft	Microsoft and its controlled US subsidiaries.

78 GDPR

The General Data Protection Regulation (GDPR) is a European privacy law that became effective in May 2018. It imposes new rules on organizations that offer goods and services to people in the European Union (EU) or that collect and analyze data belonging to EU individuals. The GDPR requires that data controllers (such as organizations using Azure) only use data processors (such as Microsoft) that provide sufficient guarantees to meet key requirements of the GDPR. Microsoft provides customers with a contractual commitment regarding the GDPR in the Online Services Terms (OST), which can be found in Attachment 4 to the OST, at the end of the document.

Microsoft provides tools and documentation to support customer's GDPR accountability including support for Data Subject Requests, Data Protection Impact Assessments, and Data Breach Notification, as described in Getting Started: Support for GDPR Accountability. Additional Azure online documentation and white papers are available to help customers meet their own GDPR compliance obligations, including specific documentation for Data Subject Requests, Data Protection Impact Assessments, and Data Breach Notification. Azure Security and Compliance GDPR Blueprint can assist customers in building and deploying cloud applications that meet GDPR requirements, including guidance and common reference architecture designed to simplify Azure adoption in support of GDPR compliance initiatives. Finally, customers can have transparent access to Azure controls in support of GDPR obligations via the Service Trust Portal Compliance Manager.

Applicability	Services in scope
Azure	All generally available Azure services as stated in the Scope statement of the Data Protection Terms in the Online Services Terms. Preview services are excluded.

79 Germany C5

The Cloud Computing Compliance Controls Catalogue (C5) outlines minimum security requirements that cloud service providers should meet for cloud services offered to customers. C5 was developed by the Federal Office for Information Security (BSI) as an auditing standard. It is intended for cloud service providers, their auditors, and customers of the cloud service providers. The catalog consists of 114 requirements across 17 domains, and it is based on established standards, including ISO 27001, Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01, AICPA Trust Services Principles and Criteria 2014, and others. However, C5 adds additional transparency controls to provide information on data location, provision of services, place of jurisdiction, existing certifications, and information disclosure obligations towards government agencies.

According to Section 3.3.3 "Use of evidence from other audits" (see Page 22 in the C5 Catalogue), a SOC 2 audit can be leveraged as attestation vehicle for C5 requirements. Microsoft Azure maintains a SOC 2 Type 2 attestation report that customers can download from the Service Trust Portal. This document details an audit assessment performed by a third-party independent auditor on controls relevant to security, availability, processing integrity, and confidentiality trust principles (SOC 2), Cloud Controls Matrix (CCM) criteria, and Cloud Computing Compliance Controls Catalogue (C5).

Applicability	Services in scope
Azure	See Appendix A.
Azure Germany	See Appendix A.
Azure Government	See Appendix B.

80 Germany IT-Grundschutz Workbook

The Federal Office for Information Security (BSI) provides the IT-Grundschutz methodology, consisting of an ISO 27001 compatible Information Security Management System (BSI Standards 100-1, 100-2), a dedicated risk analysis method (BSI Standard 100-3), and the IT-Grundschutz Catalogues, a standard set of threats and safeguards for typical business environments. The Azure Germany IT-Grundschutz workbook was developed by HiSolutions AG, an independent consulting and auditing firm in Germany. The workbook is based on the most recent version of the IT-Grundschutz Catalogues v.15 (2015), which includes modules covering internet and cloud usage, such as M 1.17 Cloud Usage. The purpose of the workbook is to help Azure Germany customers implement the IT-Grundschutz methodology within the scope of their existing or planned ISO 27001 certification based on IT-Grundschutz.

Applicability	Services in scope
Azure Germany	See ISO 27001 scope statement.

81 India MeitY

In November 2017, Microsoft became one of the first global Cloud Service Providers (CSPs) to achieve full accreditation by the Ministry of Electronics and Information Technology (MeitY) for the Government of India. MeitY provides accreditation (referred to by MeitY as empanelment) of CSPs, which enables public sector organizations to select empaneled cloud services though the government Cloud Services Directory.

MeitY accreditation was the result of a systematic audit process conducted by the Standardization Testing and Quality Certification (STQC) Directorate, a government organization that provides quality assurance services. The evaluation framework is based on the Meghraj Cloud initiative, established by the Government of India, which governs the implementation of public sector IT services. MeitY's accreditation enables government agencies and departments in India to choose Microsoft Azure to advance their digital transformation and optimize IT operations. More details can be found on the MeitY site.

Applicability	Services in scope
Azure	IaaS, PaaS, Disaster Recovery as a Service (DRaaS), Dev/Test environment as a Service, Virtual Desktop as a Service, Managed Services: Backup Services, Managed Services: Disaster Recovery & Business Continuity Services, and

	supporting infrastructure services at Microsoft Chennai, Pune, and Mumbai datacenters.

82 Japan CS Mark Gold

The Cloud Security Mark (CS Mark) is the first security standard for cloud service providers (CSPs) in Japan. It is based on ISO 27017, the international code of practice for cloud services information security controls. The CS Mark is accredited by the Japan Information Security Audit Association (JASA), a nonprofit organization established by the Ministry of the Interior and the Ministry of Economy, Trade, and Industry to strengthen information security in Japan.

JASA developed the Authorized Information Security Audit System (AISAS), which specifies the audit of approximately 1,500 controls that needs to be performed by an independent auditor authorized by JASA. Microsoft Azure completed a rigorous audit by a JASA-certified auditor and received CS Mark Gold accreditation for in-scope services. Customers can download the accreditation (in Japanese) from JASA web site.

Applicability	Services in scope
Azure	See Appendix A.

83 Japan My Number Act

The My Number Act (Japanese and English) was enacted in 2013, and took effect in January 2016. It assigns a unique number—My Number that is also called the Social Benefits and Tax Number—to every resident of Japan, whether Japanese or foreign. The Personal Information Protection Commission has issued guidelines and Q&A (in Japanese) to ensure that companies properly handle and adequately protect My Number data as required by law.

While the responsibility and ownership of personal data is with our customers, per the Online Services Terms, Microsoft contractually commits that Azure in-scope cloud services have implemented technical and organizational security safeguards to help our customers protect individuals' privacy. These safeguards are based on established industry standards, such as ISO 27001 and SOC 2 Type 2.

Furthermore, Microsoft does not have standing access to My Number data stored in these in-scope cloud services, so companies do not need to supervise handling of data by Microsoft (as outlined in Q3-12). Nonetheless, companies are required to take appropriate safety measures to protect My Number data stored in the cloud (Q3-13).

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

84 Netherlands BIR 2012

Organizations operating in the Netherlands government sector have to perform periodic audits to demonstrate compliance with the Baseline Informatiebeveiliging Rijksdienst standard (BIR 2012). The BIR 2012 provides a standard framework based on ISO 27001. When using Azure, some of the BIR 2012 controls for deployed applications are managed by Microsoft in line with the shared responsibility model in cloud computing. Even though Microsoft is not subject to compliance with BIR 2012, Dutch public

sector organizations are seeking ways to demonstrate compliance with BIR 2012 when using Azure. They need to determine if the Azure services they are using meet the requirements of BIR 2012.

Microsoft retained an independent, third-party auditing firm to analyze the extent to which current Azure certifications and attestations (such as ISO 27001 and SOC 2 Type 2) cover the part of BIR 2012 that Microsoft is responsible for. The resulting BIR 2012 Coverage Report provides a mapping of these existing certifications and attestations to the controls listed in the BIR 2012 standard. Customers can use the report as a tool to help adopt Azure in a BIR 2012 compliant way. The report clearly demonstrates which BIR 2012 controls are covered by Microsoft and which controls remain to be covered by the customers. The "Microsoft Cloud – Azure and Office 365 BIR 2012 Baseline Coverage" report can be downloaded from the Service Trust Portal GRC Assessment Reports section. Also available for download from the Service Trust Portal Compliance Guides section is the "Microsoft Cloud – Azure and Office 365 BIR 2012 Baseline Coverage User Guide" (in Dutch).

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

85 New Zealand Government CC Framework

To assist New Zealand government agencies in conducting consistent and robust due diligence on potential cloud solutions, the Government CIO has published a document titled "Cloud Computing: Information Security and Privacy Considerations" (Cloud Computing ISPC). This document contains more than 100 questions focused on data sovereignty, privacy, security, governance, confidentiality, data integrity, availability, and incident response and management.

To help agencies undertake their analysis and evaluation of Microsoft enterprise cloud services, Microsoft New Zealand has produced a series of documents showing how its enterprise cloud services address the questions set out in the Cloud Computing ISPC by linking them to the standards against which Microsoft cloud services are certified. These certifications are central to how Microsoft assures both public and private sector customers that its cloud services are designed, built, and operated to effectively mitigate privacy and security risks and address data sovereignty concerns. The Azure response to Cloud Computing IPSC is available to customers for download.

Applicability	Services in scope
Azure	App Service (Mobile Apps and Web Apps), Azure Active Directory (Free and Basic), Azure Rights Management, Batch, BizTalk Services, Cloud Services, ExpressRoute, HDInsight, Media Services, Microsoft Azure Portal, Multi-Factor Authentication, Notification Hubs, Scheduler, Service Bus, Service Fabric, SQL Database, Storage (Blobs, Disks, Files, Queues, Tables), Traffic Manager, Virtual Machines, Virtual Network, and supporting infrastructure and platform services.

86 Singapore MTCS Level 3

The Multi-Tier Cloud Security (MTCS) Standard for Singapore was prepared under the direction of the Information Technology Standards Committee (ITSC) of the Infocomm Media Development Authority of

Singapore (IMDA). The ITSC promotes national programs to standardize IT and communications and facilitates Singapore's participation in international standardization activities.

The MTCS builds upon recognized international standards such as ISO 27001. It includes a total of 535 controls and it addresses different levels of security, covering basic security in Level 1, more stringent governance and tenancy controls in Level 2, and reliability and resiliency for high-impact information systems in Level 3.

After a rigorous assessment conducted by the MTCS Certification Body, Microsoft Azure was granted certification at Level 3. A Level 3 certification means that in-scope Azure services can host high-impact data for regulated organizations with the strictest security requirements. It's required for certain cloud solution implementations by the Singapore government. Azure MTCS certificate and MTCS cloud service provider self-disclosure can be downloaded from the IMDA web site for certified cloud services. Aside from Azure services listed in Appendices A, **Virtual Agents**, **Microsoft Graph**, **Microsoft Power BI**, **Microsoft Cloud App Security**, **Power Automate**, **Microsoft Intune**, **Microsoft PowerApps**, **Microsoft Stream** and **Microsoft Service Map** online services are also included in the Azure MTCS certificate.

Applicability	Services in scope
Azure	See Appendix A.

87 Singapore OSPAR

The OSPAR framework was established by the Association of Banks in Singapore (ABS), which formulated IT security guidelines for outsourced service providers (OSPs) that seek to provide services to Singapore's financial institutions. The ABS Guidelines are intended to assist financial institutions in understanding approaches to due diligence, vendor management, and key technical and organizational controls that should be implemented in cloud outsourcing arrangements, particularly for material workloads. The OSPAR attestation requires a rigorous audit of security capabilities through an independent third party.

Microsoft Azure has achieved the OSPAR attestation in the Asia Pacific (Singapore) Region. You can download the detail OSPAR assessment report in Service Trust Portal. Aside from Azure services listed in Appendix A, the following online services are also included in OSPAR attestation report: **Intune, Microsoft Graph, Microsoft Stream, Power Apps, Power Automate, Power BI and Power Virtual Agents**.

Applicability	Services in scope
Azure	See Appendix A.

88 Spain DPA

The Spanish Data Protection Agency (Agencia Española de Protección de Datos – AEPD) has examined Microsoft Online Services Terms with specific focus on international data transfers and protection of personal data belonging to Spanish citizens. Following the assessment, the agency issued a resolution stating that Azure provides adequate protection for personal data to comply with Spanish Data Protection Law (Ley Orgánica de Protección de Datos – LOPD). The resolution covers the export of data

to Microsoft Corporation in the United States and, through the EU Model Clauses provisions, the possibility of onward transfer to subcontractors in other countries where Microsoft operates. The resolution affirms Microsoft's commitment to helping Azure customers meet their LOPD compliance requirements.

Moreover, Microsoft has retained an independent third-party auditing firm in Spain to assess Azure compliance with LOPD. The resulting certificate and audit report (in Spanish) can be downloaded from the Service Trust Portal GRC Assessment Reports section.

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

89 Spain ENS High

In 2007, the Spanish government enacted Law 11/2007, which established a legal framework to give citizens electronic access to public services. This law is the basis for the National Security Framework (Esquema Nacional de Seguridad – ENS), which is governed by Royal Decree (RD) 3/2010. The goal of the framework is to build trust in the provision of electronic services. The framework applies to all public organizations and government agencies in Spain that purchase cloud services, as well as to providers of information and communications technologies.

The framework establishes core policies and mandatory requirements that both government agencies and their service providers must meet. It defines a set of security controls, many of which align directly with ISO 27001. The sensitivity of the information—Low, Intermediate, or High—determines the security measures that must be applied to protect it. The framework prescribes an accreditation process that is voluntary for systems handling information of Low sensitivity, but mandatory for systems handling information at an Intermediate or High level of sensitivity. An audit is performed by an accredited independent auditor; the report is then reviewed as part of a certification process before risk-management controls are approved in the final accreditation step.

Microsoft Azure has completed a rigorous assessment by an accredited independent auditor and has obtained an official statement of compliance indicating a Favorable ruling at the ENS High level for the final audit report. Customers can download the Azure ENS Certificate and Audit Assessment Report from the Service Trust Portal GRC Assessment Reports section.

Applicability	Services in scope
Azure	See Appendix A.

90 TruSight

TruSight is a third-party risk-assessment utility created by leading US banks for the collective benefit of financial institutions, their suppliers, partners, and other third parties. TruSight simplifies assessments by executing best-practice, standardized evaluations once and making them available to many—enabling financial institutions to gain greater visibility into potential risks and manage third-party relationships more efficiently and effectively. The foundation of TruSight's methodology is the robust, standardized Best Practices Questionnaire (BPQ) created by TruSight's founding banks and updated in partnership with their customers and industry experts. Its 27 diversified control domains are designed to

meet the industry's evaluation needs across the categories of information and cyber security, privacy, business resiliency, and other operational risk domains. For Microsoft, TruSight conducted a rigorous and comprehensive onsite assessment of Microsoft Azure validate the design and implementation of controls according to BPQ requirements. The comprehensive validation procedures included structured inquiries, policy and procedure inspections, reviews with supporting evidence, and onsite dynamic control observations.

Applicability	Services in scope
Azure	See SOC 1,2,3 Scope in Appendix A

91 UK Cyber Essentials Plus

Cyber Essentials is a UK government-backed scheme designed to help organizations assess and mitigate risks from common cyber security threats to their IT systems. It is required for all UK government suppliers handling personal data. The scheme assurance framework has defined two different levels of certification:

- Cyber Essentials is the first level and includes a self-assessment for organizations to check the most important IT security controls of their IT infrastructure. The responses are independently reviewed by an external certifying body.
- Cyber Essentials Plus offers the same controls coverage as Cyber Essentials and also includes additional assurance by carrying out systems tests of implemented controls through an authorized third-party certifying body.

Microsoft Azure has attained the Cyber Essentials Plus badge and meets the requirements outlined in the Cyber Essentials Scheme Assurance Framework. Azure production systems are frequently tested and audited to provide evidence of a world-leading compliance portfolio. The Azure Cyber Essentials Plus certification is available to customers for download. Customers can also download the Azure Cyber Essentials Plus compliance report from the Service Trust Portal GRC Assessment Reports section.

Applicability	Services in scope
Azure	Administration of the Azure production environment.

92 UK G-Cloud

Government Cloud (G-Cloud) is a UK government initiative to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements with cloud services suppliers (such as Microsoft), and a listing of their services in an online store—the Digital Marketplace. This approach enables public-sector organizations to compare and procure cloud services without having to do their own full review process. Inclusion in the Digital Marketplace requires a self-attestation of compliance, followed by a verification performed by the Government Digital Service (GDS) branch at its discretion.

The G-Cloud appointment process requires cloud service providers to self-certify and supply evidence in support of the UK National Cyber Security Centre (NCSC) 14 Cloud Security Principles. Every year, Microsoft Azure prepares documentation and submits evidence to attest that its in-scope cloud services comply with the principles, giving potential G-Cloud customers an overview of its risk environment. A

GDS accreditor then performs several random checks on the Microsoft assertion statement, samples the evidence, and makes a determination of compliance.

The appointment of Microsoft Azure to the Digital Marketplace means that UK government agencies and partners can use in-scope services to store and process UK OFFICIAL government data, which comprises the vast majority of government data. The following documents are available to customers for download from the Service Trust Portal GRC Assessment Reports section:

- Azure UK G-Cloud Risk Environment
- Azure UK G-Cloud Residual Risk Statement
- Azure UK G-Cloud Security Assessment

Customers should also review a white paper that describes how Azure addresses the UK government 14 cloud security principles. Moreover, the Azure Security and Compliance Blueprint provides guidance and automation scripts to deliver an Azure based architecture appropriate for handling many workloads classified as OFFICIAL. A set of Azure Resource Manager templates can be used to deploy an environment that aligns to the NCSC 14 Cloud Security Principles and the Center for Internet Security (CIS) Critical Security Controls. More information is available from the UK OFFICIAL Blueprint landing page on Service Trust Portal.

Applicability	Services in scope
Azure	See ISO 27001 scope statement.

93 UK PASF

Microsoft Azure can support UK law enforcement IT customers who require Police Assured Secure Facilities (PASF) audit assurance. The Home Office's National Policing Information Risk Management Team (NPIRMT) has completed a comprehensive review of Azure UK datacenter physical infrastructure security and concluded that there were no compliance issues or necessary remedial actions identified as a result of this assessment. Risks identified during PASF audits are managed according to the National Policing Accreditation Policy as stated in the National Policing Information Risk Management Policy. The NPIRMT PASF assessment is available from the Home Office to policing customers when conducting their own risk assessment related to the use of cloud services.

Applicability	Services in scope
Azure	Azure UK datacenter physical infrastructure.

Appendix A: Azure Services in Audit Scope[1]

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
API Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
App Service: API Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
App Service: Mobile Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
App Service: Web Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Change Analysis	✓		✓	✓	✓	✓	✓	✓	✓												
Application Gateway	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Insights	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Automation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Active Directory (Free and Basic)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Active Directory (Premium P1 + P2)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Active Directory B2C	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Active Directory Domain Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Advanced Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓		✓
Azure Advisor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Analysis Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure API for FHIR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓		✓
Azure App Configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓		✓		
Azure Archive Storage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				✓
Azure Bastion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓		✓		✓		✓		✓
Azure Blueprints	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓			✓		✓		✓

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
Azure Bot Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Cache for Redis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Confidential Computing		✓								✓							✓				
Azure Cognitive Search	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Container Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓
Azure Cosmos DB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure Data Box	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓			✓		✓		✓
Azure Data Box Edge and Gateway	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓					✓		✓
Azure Data Explorer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓		✓
Azure Data Lake Storage Gen1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓		✓
Azure Database for MariaDB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Database for MySQL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Database for PostgreSQL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Database Migration Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Databricks[2 3]					✓		✓			✓		✓	✓								
Azure Data Share	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				✓
Azure DDoS Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Dedicated HSM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓		✓		✓
Azure Defender for IoT		✓								✓							✓				
Azure DevOps (formerly VSTS)[3]		✓			✓		✓			✓	✓	✓				✓	✓				
Azure DevTest Labs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
Azure DNS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure ExpressRoute	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure File Sync	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓				✓
Azure Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Firewall Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				✓
Azure for Education	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓		✓				
Azure Front Door	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Functions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure HPC Cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓		✓		✓
Azure Import/Export	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure Information Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Internet Analyzer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				
Azure IoT Central	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓
Azure IoT Hub	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Kubernetes Service (AKS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure Lab Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure Lighthouse	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓		✓		✓		✓
Azure Machine Learning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Managed Applications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓		✓		✓		✓
Azure Maps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓		✓		✓
Azure Media Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
Azure Migrate	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Monitor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure NetApp Files [3]		✓	✓		✓	✓	✓		✓			✓					✓				
Azure Open Datasets	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓		✓		✓
Azure Peering Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				
Azure Performance Diagnostic	✓		✓	✓	✓	✓	✓	✓	✓												
Azure Policy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Azure Private Link	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓		✓		✓		✓
Azure Public IP		✓								✓							✓				
Azure Red Hat OpenShift	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓				✓		✓		✓
Azure Resource Graph	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓		✓		✓		✓
Azure Resource Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Security Center	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure Security for IoT	✓		✓	✓	✓	✓	✓	✓	✓												
Azure Sentinel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓		✓		✓		✓
Azure Service Fabric	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure Service Health	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓					✓		✓
Azure Service Manager (RDFE)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure SignalR Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓		✓		✓
Azure Signup Portal		✓								✓							✓				
Azure Site Recovery	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
Azure Spring Cloud Service		✓								✓							✓				
Azure Sphere	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓		✓		
Azure SQL Database	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Synapse Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Azure Ultra Disk		✓								✓							✓				
Azure Virtual WAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓
Azure VMWare Solution	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				
Azure Web Application Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓		✓				✓
Azure Spatial Anchors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓			✓				
Backup	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Batch	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cloud Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cloud Shell	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Anomaly Detector		✓								✓							✓				✓
Cognitive Services: Computer Vision	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Content Moderator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Custom Vision	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓		✓
Cognitive Services: Face	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Form Recognizer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓					✓				✓
Cognitive Services: Language Understanding	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Personalizer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				✓

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
Cognitive Services: QnA Maker	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Speech Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Text Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Translator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Cognitive Services: Video Indexer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Container Instances	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓		✓
Container Registry	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Content Delivery Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Customer Lockbox for Microsoft Azure	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓				
Data Catalog	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Data Factory	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓		✓
Data Lake Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Event Grid	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Event Hubs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HDInsight	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key Vault	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Load Balancer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Log Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Logic Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Lustre as a Service	✓		✓	✓	✓	✓	✓	✓	✓												
Machine Learning Studio (Classic)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
Microsoft Azure Portal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft Genomics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓		✓		✓
Microsoft Healthcare Bot		✓								✓							✓				
Multi-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network Watcher	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Notification Hubs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Power BI Embedded	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Scheduler	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Service Bus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SQL Server on Virtual Machines		✓								✓							✓				
Storage: Archive	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
Storage: Blobs (incl. Azure Data Lake Storage Gen 2)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Disks (incl. Managed Disks)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Files	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Queues	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Tables	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
StorSimple	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stream Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Time Series Insights	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓		✓		✓
Traffic Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Machine Scale Sets	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Virtual Machines (incl. Reserved Instances)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Azure Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701:2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	K-ISMS	PCI DSS	Australia IRAP	Germany C5	Japan CS Mark Gold	Singapore MTCS Level 3	Spain ENS High	Singapore OSPAR
Virtual Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Network Address Translation (NAT)	✓		✓	✓	✓	✓	✓	✓	✓												
Virtual WAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓		✓		✓
VPN Gateway	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows Virtual Desktop	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓			✓				✓		
Windows 10 IoT Core Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓		✓		✓		✓

[1] For the Azure FedRAMP High, DoD SRG, and NIST CSF Scope please refer to the following site.

[2] Azure Databricks SOC attestation includes SOC 2 Type 2 report only.

[3] Service has only achieved the certificates listed in the table above, any other inherited scope references are not applicable.

Appendix B: Azure Government Services in Audit Scope[1]

Azure Government Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701: 2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	PCI DSS	Germany C5
API Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
App Service: API Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
App Service: Mobile Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
App Service: Web Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Gateway	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Insights	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Active Directory (Free and Basic)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Active Directory (Premium P1 + P2)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Active Directory Domain Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Advanced Threat Protection	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	
Azure Advisor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Analysis Services	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure App Configuration		✓								✓					✓
Azure Archive Storage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓
Azure Bastion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Blueprints	✓		✓		✓	✓	✓	✓	✓						
Azure Bot Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Cache for Redis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Cognitive Search	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Azure Government Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701: 2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	PCI DSS	Germany C5
Azure Container Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Cosmos DB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Data Box	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Data Box Edge and Gateway	✓		✓	✓	✓	✓	✓	✓	✓						
Azure Data Explorer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Data Lake Storage Gen1	✓		✓	✓	✓	✓	✓	✓	✓					✓	
Azure Database for MariaDB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Database for MySQL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Database for PostgreSQL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure DDoS Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Dedicated HSM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Defender for IoT		✓								✓					✓
Azure DevTest Labs	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure DNS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure ExpressRoute	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure File Sync	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
Azure Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
Azure Front Door	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Functions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure HPC Cache		✓								✓					✓
AI Builder		✓								✓			✓		✓

Azure Government Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701: 2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	PCI DSS	Germany C5
Azure Import/Export	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Information Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure IoT Central		✓								✓					✓
Azure IoT Hub	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Kubernetes Service (AKS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Lab Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Lighthouse	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Machine Learning		✓								✓					✓
Azure Managed Applications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Maps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Media Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Migrate	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Azure Monitor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Peering Service		✓								✓					✓
Azure Policy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Azure Private Link	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
Azure Public IP		✓								✓					✓
Azure Resource Graph	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Azure Resource Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Security Center	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Sentinel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓

Azure Government Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701: 2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	PCI DSS	Germany C5
Azure Service Fabric	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Service Health	✓		✓	✓	✓	✓	✓	✓	✓						
Azure Service Manager (RDFE)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure SignalR Service		✓								✓				✓	✓
Azure Site Recovery	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Azure SQL Database	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Stream Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Synapse Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Virtual WAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
Azure Web Application Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Backup	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Batch	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cloud Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cloud Shell	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓
Cognitive Services: Computer Vision	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cognitive Services: Content Moderator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cognitive Services: Face	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cognitive Services: Language Understanding	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cognitive Services: Speech Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cognitive Services: Text Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cognitive Services: Translator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Azure Government Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701: 2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	PCI DSS	Germany C5
Cognitive Services: Personalizer		✓								✓					✓
Cognitive Services: QnA Maker	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Container Instances	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
Container Registry	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Content Delivery Network		✓								✓				✓	✓
Customer Lockbox for Microsoft Azure		✓								✓					✓
Cost Management	✓		✓	✓	✓	✓	✓	✓	✓						
Data Factory	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Data Lake Analytics														✓	
Event Grid	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Event Hubs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HDInsight	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key Vault	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Load Balancer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Log Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Logic Apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Machine Learning Service	✓		✓	✓	✓	✓	✓	✓	✓					✓	
Microsoft Azure Portal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft Defender Advanced Threat Protection	✓		✓	✓	✓	✓	✓	✓	✓					✓	
Multi-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network Watcher	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓

Azure Government Service	CSA STAR Certification	CSA STAR Attestation	ISO 20000-1:2011	ISO 22301:2012	ISO 27001:2013	ISO 27017:2015	ISO 27018:2014	ISO 27701: 2019	ISO 9001:2015	SOC 1, 2, 3	GxP (FDA 21 CFR Part 11)	HIPAA BAA	HITRUST	PCI DSS	Germany C5
Notification Hubs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Power BI Embedded	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Scheduler	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Service Bus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SQL Server on Virtual Machines		✓								✓					✓
Storage: Archive	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Storage: Blobs (incl. Azure Data Lake Storage Gen 2)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Disks (incl. Managed Disks)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Files	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Queues	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage: Tables	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
StorSimple	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Traffic Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Machine Scale Sets	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Machines (incl. Reserved Instances)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Network Address Translation (NAT)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓
Virtual WAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓
VPN Gateway	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

[1] For the Azure FedRAMP High, DoD SRG, CJIS, IRS 1075, NIST CSF, and NIST SP 800-171 Scope please refer to the following site.