Microsoft

Compliance:

Azure conforms to global standards

Trusted Cloud:
Microsoft Azure Security, Privacy, Compliance,
Resiliency, and Protected IP

Author
Debra Shinder

Compliance plays a critical role in providing assurance for customers, and is an important element in the trust relationship. Through rigorous and widely recognized formal standards that are certified by independent third parties, Microsoft helps organizations comply with constantly shifting requirements and regulations governing the security, collection, and use of individuals' data.

Azure offers a broad set of key global and industry-specific standards and supporting materials for key regulations, including ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1, 2, and 3Reports. Azure also meets regional and national standards that include the EU Model Clauses, EU-U.S. Privacy Shield, Singapore MTCS, and the CS Mark in Japan. You'll find a complete list of Azure compliance offerings below.

Rigorous audits (many of which require annual review of Azure facilities and capabilities) are conducted by independent accredited third parties such as BSI and Deloitte, which validate Azure's adherence to these standards.

Through its long-standing relationship with the legal and compliance community, Microsoft has developed a wealth of resources for professionals who need relevant information on the key regulatory and compliance considerations associated with cloud computing. This includes both privacy law requirements that apply across all industries, and sector-specific guidelines and regulations.

While it is up to you to determine whether Azure services comply with the specific laws and regulations that are applicable to your business, we help you make these assessments, by providing the specifics of our compliance programs, including audit reports and compliance packages. Your auditors can compare Azure results with your own legal and regulatory requirements, and you can verify the Azure implementation of controls by requesting detailed audit results and reports, many of which are free to Azure customers and trial customers through the Service Trust Platform.

Learn more: For the most current information about Azure compliance, visit the Microsoft Trust Center compliance offerings and choose Azure from the Product or Service list.

Azure compliance offerings

Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider to help you comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data.

These include compliance offerings that are: globally applicable, US government regulations, other region- or country-specific regulations, and industry-specific requirements. Below is a list of our compliance offerings as of October 2019.

Globally applicable offerings

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.

- **CIS Benchmark.** The Center for Internet Security Microsoft Azure Foundations Benchmark.
- **CSA STAR Attestation.** The Cloud Security Alliance audit of a cloud provider's security posture.
- **CSA STAR Certification.** The Cloud Security Alliance certification that involves an independent third-party assessment of a cloud provider's security posture.
- **CSA STAR Self Assessment.** The Cloud Security Alliance level 1 offering that is free and open to all cloud services providers.
- **ISO/IEC 20000-1:2011.** International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) certification in Information Technology Service Management.
- **ISO 22301.** International Organization for Standardization (ISO) Business Continuity Management Standard.

- **ISO/IEC 27001.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Information Security Management Standards.
- **ISO/IEC 27017.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Code of Practice for Information Security Controls.
- **ISO/IEC 27018.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Code of Practice for Protecting Personal Data in the Cloud.
- **ISO 9001.** International Organization for Standardization Quality Management Systems Standards.
- **SOC 1, 2, and 3.** Service Organization Controls standards for operational security.
- **WCAG 2.0.** Web Content Accessibility Guidelines 2.0.

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.

- **CJIS**. Criminal Justice Information Services Security Policy.
- **DFARS.** Defense Federal Acquisition Regulation Supplement for defense contractors.
- **DoD DISA L2, L4, L5.** US Department of Defense Provisional Authorization.
- **DoE 10 CFR Part 810.** Department of Energy Code of Federal Regulations.
- **EAR.** US Export Administration Regulations.
- **FDA CFR Title 21 Part 11.** Food and Drug Administration Code of Federal Regulations.
- **FedRAMP.** Federal Risk and Authorization Management Program.
- **FERPA.** Family Educational Rights and Privacy Act.
- **FIPS 140-2.** Federal Information Processing Standard.
- **IRS 1075.** US Internal Revenue Service Publication.
- **ITAR.** International Traffic in Arms Regulations.
- **NIST 800-171.** National Institute of Standards and Technology Special Publication on Protecting Unclassified Information in Nonfederal Information Systems and Organizations.
- **NIST Cybersecurity Framework (CSF).** National Institute of Standards and Technology Cybersecurity Framework.

Other region- and country-specific regulations

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

- **Argentina PDPA.** Personal Data Protection Act 25,326.
- **Australia IRAP Unclassified.** Information Security Registered Assessors Program.
- **Australia IRAP PROTECTED.** Information Security Registered Assessors Program highly sensitive data security level.
- **Canada Privacy Laws.** 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).

Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider—the deepest and broadest coverage in the industry.

- **China GB 18030:2005.** Chinese Coded Character Set standard set by the China Electronics Standardization Institute (CESI).
- **China DJCP (MLPS) Level 3.** Information Security Technology—Basic Requirements for Classified Protection of Information System Security (multilevel protection scheme).
- **China TRUCS / CCCPPF.** Trusted Cloud Service Certification.
- **EU EN 301 549.** European Union Accessibility Requirements Suitable for Public Procurement of ICT Products and Services.
- **EU ENISA IAF.** The European Union Agency for Network and Information Security Information Assurance Framework.
- **EU GDPR.** European Union General Data Protection Regulation.
- **EU Model Clauses.** European Union data protection law Standard Contractual Clauses.
- **EU-US Privacy Shield.** Designed by the U.S. Department of Commerce, and the European Commission.
- **Germany C5.** Cloud Computing Compliance Controls Catalog.
- **Germany IT-Grundschutz workbook.** IT-Grundschutz workbook for Internet and cloud usage.
- **India MeitY.** Ministry of Electronics and Information Technology accreditation for public cloud, government virtual private cloud, and government community cloud.
- **Japan CS Mark Gold.** Cloud Security Gold Mark for IaaS and PaaS.
- **Japan My Number Act.** Social Benefits and Tax Number resident identification number system.
- **Netherlands BIR 2012.** Baseline Informatiebeveiliging Rijksdienst standard.
- **New Zealand Gov CC Framework.** New Zealand Government Cloud Computing Security and Privacy Considerations.
- **Singapore MTCS Level 3.** Multi-Tier Cloud Security Standard for Singapore certification for IaaS, PaaS, and SaaS.
- **Spain ENS High.** Spain Esquema Nacional de Seguridad (ENS) High Level Security Measures.
- **Spain DPA.** Spanish Data Protection Agency guidelines.
- **TISAX (Germany).** Trusted Information Security Assessment Exchange.
- **UK Cyber Essentials Plus.** Cyber Essentials PLUS requirements outlined in the Cyber Essentials Scheme Assurance Framework.
- **UK G-Cloud.** United Kingdom Government-Cloud services classification v6.
- **UK PASF.** United Kingdom Police Assured Secure Facility standards.

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, and education. Azure is not subject directly to oversight by these regulators; however, Azure can help customers meet their own compliance requirements.

- **23 NYCRR Part 500.** New York State cybersecurity requirements for licensed financial institutions.
- **AFM and DNB (Netherlands).** Dutch Authority for the Financial Markets (Autoriteit Financiële Markten, AFM) and the Dutch Central Bank (De Nederlandsche Bank, DNB) financial services regulations.
- **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) financial services and insurance industry regulations.

- **APRA (Australia).** The Australian Prudential Regulation Authority (APRA) regulations for banks, credit unions, insurance companies, and other financial services institutions.
- **CDSA.** The Content Delivery & Security Association (CDSA) Content Protection & Security (CPS) Standard.
- **CFTC 1.31.** The United States Commodity Futures Trading Commission (CFTC) Rule 1.31 recordkeeping requirements.
- **DPP (UK).** The Digital Production Partnership (DPP) and North American Broadcasters Association (NABA) broadcasters cybersecurity requirements.
- **EBA (EU).** European Banking Authority.
- **FACT (UK).** Federation Against Copyright Theft.
- **FCA and PRA (UK).** Financial Conduct Authority and Prudential Regulation Authority.
- **FFIEC.** The US Federal Financial Institutions Examination Council.
- **FINMA (Switzerland).** The Swiss Financial Market Supervisory Authority.
- **FINRA 4511.** The Financial Industry Regulatory Authority Rule 4511.
- **FISC (Japan).** The Center for Financial Industry Information Systems.
- **FSA (Denmark).** The Danish Financial Supervisory Authority.
- **GLBA.** The Gramm-Leach-Bliley Act regulating the US financial services industry.
- **GxP.** Good Clinical, Laboratory, and Manufacturing Practices (GxP), and regulations enforced by the US Food and Drug Administration (FDA) under CFR Title 21 Part 11.
- **HDS (France).** Health Data Hosting (Hébergeurs de Données de Santé, HDS) certification.
- **HIPAA/HITECH.** Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health.
- **HITRUST.** Health Information Trust Alliance.
- **KNF (Poland).** The Polish Financial Supervision Authority (Komisja Nadzoru Finansowego).
- **MARS-E.** The Center for Medicare and Medicaid Services Minimum Acceptable Risk Standards for Exchanges.
- **MAS + ABS (Singapore).** Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore.
- **MPAA.** Motion Picture Association of America.
- **NBB and FSMA (Belgium).** National Bank of Belgium (NBB) and the Financial Services and Markets Authority.
- **NEN-7510 (Netherlands).** Dutch Standardisation Institute healthcare standard.
- **NERC.** North American Electric Reliability Corporation.
- **NHS IG Toolkit (UK).** National Health Service Information Governance toolkit.
- **OSFI (Canada).** Office of the Superintendent of Financial Institutions.
- **PCI DSS.** Payment Card Industry Data Security Standards.
- **RBI and IRDAI (India).** The Reserve Bank of India and Insurance Regulatory and Development Authority of India.
- **SEC 17a-4.** United States Securities and Exchange Commission.
- **Shared Assessments.** Shared Assessment Program formerly known as BITS Shared Assessments, used in the banking industry.
- **SOX.** Sarbanes-Oxley Act of 2002, administered by the Securities and Exchange Commission.

- **TISAX (Germany).** Trusted Information Security Assessment Exchange for the automotive industry.

Compliance tools and guidance

Frequent updates to the laws and rules from the many regulatory bodies around the world create a challenge for organizations. Compliance personnel need assistance to help meet evolving requirements. Microsoft helps customers meet compliance obligations by providing an extensive repository of resources that include tools, documentation, and guidance.

Microsoft helps customers meet compliance obligations by providing an extensive repository of resources that include tools, documentation, and guidance.

Microsoft Trust Center

The Microsoft Trust Center is your resource for learning how we implement and support security, privacy, compliance, and transparency in all our cloud products and services. The Trust Center features a comprehensive set of all current certifications, attestations, and other compliance offerings.

Service Trust Center

The Service Trust Portal contains additional guidance and tools to help meet your security, compliance, and privacy needs when using Azure and other Microsoft Cloud services. These audit reports, Azure Security and Compliance Blueprints, and trust documents to help you understand cloud features, and to verify technical compliance and control requirements.

Azure Blueprints

The Azure Blueprint service helps customers build Azure applications that are secure and comply with many regulations, including the GDPR and HIPAA, both internally and externally. They also help simplify large scale Azure deployments by packaging key environment artifacts, such as Azure Resource Manager templates, resource groups, role-based access controls, and policies, in a single blueprint definition.

This free service provides you with templates to create, deploy, and update fully governed cloud environments to consistent standards and comply with regulatory requirements. It differs from Azure Resource Manager (ARM) and Azure Policy in that Blueprints is a package that contains different types of artifacts—including Resource Manager templates, resource groups, policy assignments, and role assignments—all in one container, so you can quickly and easily deploy all these components in a repeatable configuration.

You can use the built-in blueprints or create your own custom blueprints. Blueprints can be created in the Azure portal or using the REST API with tools such as PowerShell. If the latter method is used, you can define blueprint parameters to prevent conflicts when reusing certain blueprints.

Implementation guidance

Organizations face many challenges in achieving their compliance goals. Microsoft provides guidance to help Azure customers reach those goals and comply with industry and government regulations in the cloud:

- Overview of Microsoft Azure Compliance
- How Microsoft Azure Can Help Organizations Become Compliant with the EU GDPR
- A Practical Guide to Designing Secure Health Solutions using Microsoft Azure
- Microsoft Azure HIPAA/HITECH Act Implementation Guide

Microsoft