

The Microsoft Approach to Compliance in the Cloud

Microsoft
Reactive Security
Communications

Contents

Executive summary	1
Introduction	2
Helping customers meet compliance needs	7
Partnering with industry leaders	10
Microsoft cloud services create customer choice	10

Executive summary

Microsoft recognizes that trust is necessary for organizations and individuals to fully embrace and benefit from cloud services. Microsoft is committed to providing customers the compliance information they need in order to have confidence in Microsoft as their preferred cloud service provider (CSP). Although the cloud can be abstract, the Microsoft approach to delivering a trustworthy cloud is not. It is based on many years of experience, a commitment to security, privacy, and transparency principles, and on leading industry practices.

The term “compliance” has been used frequently as cloud adoption has increased. It is used in several different ways in relation to cloud services, especially as a tool in the evaluation of cloud services and as a way to describe expectations about how cloud services are operated. Several factors make compliance important when customers are evaluating Microsoft cloud services:

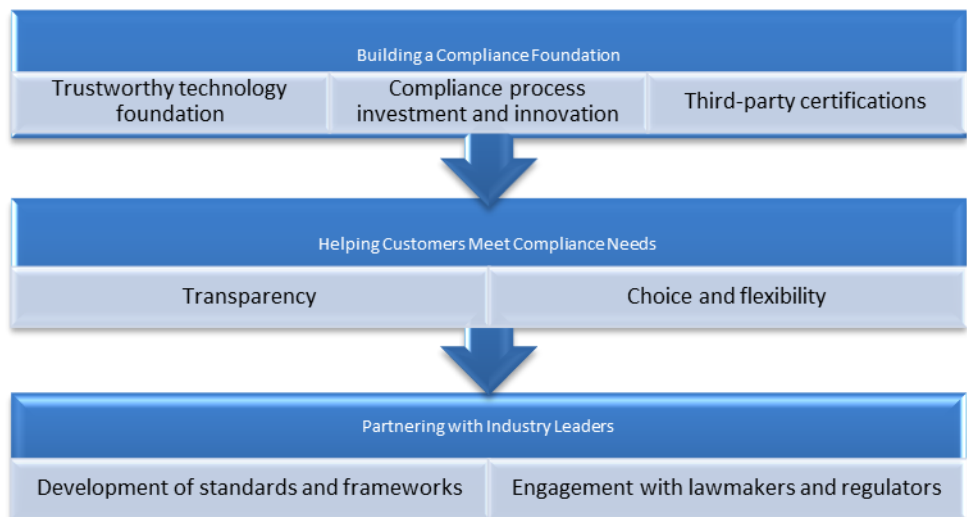
- **Customers must meet their own compliance needs.** Customers retain their own compliance obligations when they use cloud services. These obligations might arise from internal mandates or external regulations and industry standards, and they rely on the capabilities of the CSP. The CSP’s capabilities become a portion of the full set of compliance capabilities, which the customer represents. This compliance is supported through third-party validation of stated Microsoft capabilities, which are exposed in the form of certifications and attestations.
- **Compliance is sometimes viewed as a proxy for Microsoft claims about the trustworthiness of its cloud services.** Most Microsoft customers have the option to verify claims of Microsoft’s trustworthy cloud services as one way to inform their decisions about the adoption and ongoing operations of Microsoft’s cloud services.

- **Some Microsoft services may comply with certain requirements because of the markets and industries that Microsoft operates in.** Microsoft may elect to establish whether a service meets certain industry standards and regulations because of the markets and industries it operates in. For example, customers and the credit card industry expect Microsoft to meet the Payment Card Industry Data Security Standard (PCI DSS) because Microsoft processes their credit cards when they use cloud services to make purchases.
- **Microsoft must verify its environment against policy and business requirements.** Microsoft uses compliance for internal purposes—for example, to evaluate whether the company operates in a manner that matches its own policy and business requirements. Compliance in this sense is a tool that Microsoft uses for internal risk management.

This paper describes the Microsoft approach to compliance in the cloud to meet all of the aforementioned needs.

Microsoft cloud compliance practices can be divided into three main areas as shown in the following diagram:

- Building the right compliance foundation.
- Helping customers meet specific compliance needs when possible.
- Partnering with relevant industry leaders, regulators, and lawmakers.



Introduction

Cloud computing has many benefits. For example, [Microsoft research](#) shows that seventy percent of small and medium-sized businesses using cloud services have reinvested money they saved by moving to the cloud in product development, innovation, marketing, and expansion. Ninety-one percent of those surveyed said security had been positively affected by the adoption of cloud technology. More broadly, the cloud enables organizations to increase agility, stay up-to-date with the latest technology, scale to meet dynamic needs, and empower an increasingly mobile workforce to be productive anywhere, anytime.

A wide variety of private and public sector organizations have adopted Microsoft cloud services while continuing to meet their compliance needs. These organizations benefit from significant investments Microsoft has made in security, privacy, and reliability that they are often unable to make on their own. This factor allows organizations that use Microsoft cloud services to reinvest resources in areas that are strategic to their missions.

For organizations with internal or external compliance requirements, the choice of a CSP requires careful consideration. In many cases, the CSP's services can become part of the customer's chain of compliance, so customers can determine whether the CSP services satisfy their needs. The CSP may even provide specific, contractual compliance mechanisms, such as the [Model Clauses in the European Union](#) that Microsoft offers, or when an organization requires a Health Insurance Portability and Accountability Act Business Associate Agreement (HIPAA BAA).

With the right CSP, almost any customer can benefit from cloud computing. Organizations should use a broad set of criteria when evaluating a CSP's security, privacy, and compliance capabilities, including the CSP's answers to the following questions:

- Do they have a proven record of delivering secure, reliable, cloud services built for privacy and data protection?
- Have they obtained independent third-party verification and validation that are relevant to its customers' compliance needs?
- Do their customers have the flexibility and choice of capabilities to meet the customer compliance needs?
- Do they invest in developing and improving security, privacy, and compliance processes and technologies to meet ever-changing standards across the world?
- Are they transparent about their cloud compliance capabilities and which responsibilities are owned by customers?

- Does the CSP help customers achieve their own compliance requirements?
- Do they demonstrate leadership by participating in the development and continuous improvement of industry standards that are relevant to cloud services?

This paper discusses how the Microsoft approach to cloud compliance enables it to meet these important criteria as a CSP committed to delivering trustworthy cloud services.

Building a compliance foundation

Microsoft cloud services prioritize the security, privacy, and reliability capabilities of its technology, people, and processes. By prioritizing these capabilities across all its offerings, Microsoft helps reduce business and technical risk for all of its customers and positions itself and its customers to more easily obtain key certifications and attestations.

Microsoft Trustworthy Computing

Trustworthy Computing (TwC) is long-term Microsoft collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone. Microsoft believes fundamentally that customer data and personal information must be protected. It adheres to business practices that promote trust and focuses on solid engineering and operational best practices to help ensure that products and services are continuously made more reliable, secure, and compliant. One key way that TwC directly affects the compliance readiness of cloud services is by developing frameworks and tools that guide the ways that Microsoft designs, builds, and operates its offerings, including cloud services.

The first of these tools is the Security Development Lifecycle (SDL), which was mandated across Microsoft in 2004 and shared freely with the industry and customers. The SDL embeds security requirements into the software development process from beginning to end. Every Microsoft cloud service uses the SDL to enhance compliance capabilities through security capabilities and reduce the potential loss of sensitive information. The SDL is reviewed and updated on a regular basis as new threats and requirements are identified. To address the rapid pace of cloud-based development and deployment, Microsoft developed a version of the SDL methodology called SDL for Agile. SDL for Agile guidance is available as a free download for developers creating cloud applications on Microsoft Azure and other cloud platforms, or on software development projects that use the agile development methodology.

Many threats target software vulnerabilities, but others attack operational weaknesses, which is why Microsoft uses the [Operational Security Assurance \(OSA\)](#) framework. OSA supports continuous monitoring, helps to identify operational risks, provides operational security guidelines, and validates that those guidelines are followed. OSA helps make Microsoft cloud infrastructure more resilient to attack by decreasing the amount of time needed to protect, detect, and respond to security threats.

Compliance investment and innovation

For many of our leading online services, Microsoft has invested in a controls framework that maps to key industry standards such as ISO/IEC 27001:2005, SOC 1 (SSAE 16/ISAE 3402), SOC 2 (AT 101), PCI DSS, FISMA/FedRAMP (NIST SP 800-53), and others.

Through process and tooling, Microsoft maps control elements to engineering and operations responsibilities, identifies and addresses gaps, and reduces duplicate effort when a single control activity might map to similar requirements across multiple standards. This mapping shifts the focus from specific audit requirements to rationalized controls, which allows teams to focus on designing effective control activities. The control framework enables Microsoft to better develop a predictable audit schedule; prepare for multiple audits with a single, annual control activity readiness review; and helps to streamline compliance across a range of regulations today and in the future.

Third-party certifications

Its foundation of trustworthy technology and compliance process innovation enable Microsoft to lead the cloud services industry in receiving third-party attestations. Its streamlined approach to compliance enables it to accelerate certification and helps to deliver services that are compliant with certain standards or requirements for more customers and in a broader range of regulatory environments. For example:

- Microsoft was the first major cloud provider to be certified for ISO 27001 for its Global Foundation Services (GFS), a broad international information security standard.
- The FISMA Authority to Operate (ATO) was first granted to the Microsoft cloud infrastructure, for GFS, in 2010. Since then, Office 365, Microsoft Azure, and GFS have received ATOs from multiple federal agencies.
- With Microsoft Azure and GFS, Microsoft has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board. The GFS General Support System P-ATO

covers shared services in nine Microsoft data centers located in the United States, including California, Illinois, Iowa, Texas, Virginia, and Washington.

- In 2012, Microsoft GFS became one of the first in the industry to successfully complete SOC 2 Type 2 and SOC Type 3 attestations. Microsoft Azure has attained a SOC 2 attestation.
- Microsoft was the first major productivity CSP to offer a HIPAA BAA to healthcare entities with access to protected health information (PHI) for many of our online services.
- The European Union's 28 data protection authorities, acting through their "Article 29 Working Party," have determined that the contractual privacy protections Microsoft offers to its enterprise cloud customers meets the current existing European Union standards for international transfers of data. Microsoft is the first and only cloud service provider to receive this type of approval. Europe's privacy regulators have said, in effect, that personal data stored in Microsoft's enterprise cloud is subject to Europe's rigorous privacy standards no matter where that data is located. This recognition applies to Microsoft's enterprise cloud services – in particular, Microsoft Azure, Office 365, Microsoft Dynamics CRM and Microsoft Intune.
- Microsoft Azure has been validated for PCI-DSS Level 1 compliance by an independent Qualified Security Assessor (QSA).
- Microsoft was the first CSP to complete a third-party assessment against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) as part of its SOC 2 Type 2 audit for Microsoft Azure.

Microsoft Global Foundation Services

The [Microsoft data center infrastructure](#) serves a broad range of industries around the world—including those with requirements such as PCI-DSS, certain ISO standards and FedRAMP. The Microsoft GFS team is responsible for Microsoft data centers, including networking, operations, security, and compliance. This infrastructure is used by all Microsoft cloud services and serves more than 20 million businesses worldwide. GFS combines many security technologies and processes into a unified, defense-in-depth approach, which enables it to deliver a foundation for Microsoft cloud services that is secure, reliable, private, and compliance-ready.

The success of this approach is demonstrated by the fact that GFS has attained ISO/IEC 27001:2005 certification, SSAE 16/ISAE 3402 SOC 1, 2 and 3 attestations, a Provisional Authority to Operate by the Federal Risk and Authorization Program (FedRAMP) Joint Authorization Board, and PCI-DSS

certification as an infrastructure provider. GFS operates hundreds of security controls based on more than 1,000 unique audit requirements.

Microsoft data centers are strategically located around the world to enhance performance and help ensure service resiliency. They are designed to help protect services and data and enhance availability, and are operated in accordance with best practices such as strict access control and 24-hour monitoring.

Privacy by Design

Microsoft recognizes that cloud services create unique privacy challenges, and that data control and privacy are often critical aspects of compliance. Microsoft is one of few CSPs to have enterprise cloud service-specific privacy statements and contract-backed data use limitations and security protections.

Privacy by Design ensures that privacy protections are consistently implemented across Microsoft products, services, operations, and team organizations.

For many customers, knowing and controlling the location of their data is an important element of compliance. Microsoft enables organizations to choose the geographic area in which their data resides. Customers may also have some options regarding their ability to locate their data across regions within a geographic area for purposes such as redundancy or performance.¹

Helping customers meet compliance needs

Transparency

Industry recognized third-party verifications are important, but customers also need CSPs to be transparent about their compliance activities. Transparency enables customers to make a more informed decision about whether a provider is right for their unique needs.

¹ For full details about how Microsoft limits use of customer data, refer to the Trust Center for the service in question.

Microsoft has created Trust Centers for [Microsoft Azure](#), [Office 365](#), [Microsoft Intune](#), and [Dynamics CRM](#) to help customers understand the compliance aspects of Microsoft cloud services. These Trust Centers provide access to compliance related documentation and information on how Microsoft handles data stored for its cloud services, including principles of privacy, transparency, independent verification, and security. Microsoft Azure, Office 365, Microsoft Intune, and Dynamics CRM Trust Centers provide links to dashboards for customers with up-to-date information on service availability and data location.

Microsoft also participates in industry-wide initiatives, including its association with the [Cloud Security Alliance](#) (CSA). An independent industry organization, the CSA has developed a controls framework called the [Cloud Controls Matrix](#) (CCM) and the [Security, Trust & Assurance Registry](#) (STAR) to capture detailed responses to more than 100 self-assessment questions that are posed to CSPs about cloud security controls. Microsoft participated in the development of the CCM, maps to the CSA guidance, and has completed its own detailed CCM-based audit, which is available in the STAR registry.

Organizations that want to evaluate their IT security state, evaluate the benefits of cloud computing, and plan for adoption and compliance can use the [Cloud Security Readiness Tool](#). Based on the answers to a few short questions, the tool generates a report tailored to the needs of the organization. For more information, read the white paper "[The Microsoft Approach to Cloud Transparency](#)."

Choice and flexibility

Recognizing that compliance is not a one-size-fits-all activity, Microsoft offers industry-leading choice and flexibility and helps customers to use cloud services in accordance with their security and compliance standards.

In highly regulated industries or those that handle sensitive customer data, organizations may be required by customers, auditors, or internal policies to keep some data on-premises. If a cloud offering is not compatible with on-premises technology, these organizations either cannot use it or must keep cloud and on-premises services separate. Microsoft offers hybrid solutions that seamlessly combine on-premises software and cloud services into unified solutions. This capability enables customers to move to the cloud at their own pace and helps to simplify compliance with a unified set of management and auditing tools.

Microsoft promotes interoperability to make it easier and less costly for customers to develop and manage mixed IT environments. In the cloud,

Microsoft supports key standards that help provide the building blocks for open, interoperable cloud services. It also supports developer choice of programming languages such as Java, Android, and Ruby; data portability; and customer ownership of data no matter where it resides.

Customer-controlled compliance features

In addition to the robust controls implemented in the infrastructure, Microsoft continues its long-established practice of building compliance-related features into specific products and cloud services. Examples include:

- **Rights Management Services (RMS)**. Now available in the cloud via Microsoft Azure, RMS enables the application of protection policies to sensitive documents and records. Unlike approaches that attempt to interrupt the flow of information at exit points in an organization, rights management software works at deep levels within data storage technologies. Documents are encrypted and control over who can decrypt them uses access controls that are defined in an authentication control solution such as a directory service.
- **Identity and access controls**. Microsoft offers federated identity and access management solutions for customers to use across [Microsoft Azure](#) and other services such as [Office 365](#), which helps to simplify the management of multiple environments and applications by controlling user access across a range of applications.
- **eDiscovery and archiving**. With powerful tools including in-place archiving, litigation hold, audit logs, and Multi-Mailbox Search, Office 365 helps organizations meet legal, regulatory, and industry compliance standards.
- **Data Loss Prevention (DLP)**. In [Exchange Online](#), transport rules can be used to control the flow of email messages within, into, and out of an organization. For example, transport rules can be used to detect and stop outgoing messages that contain personally identifiable information such as Social Security numbers.
- **Policy tips**. Exchange can automatically detect sensitive business information based on company policies and warn Outlook and Outlook Web Application users before they click Send.

Partnering with industry leaders


Microsoft stays abreast of new and upcoming changes to key compliance requirements and actively participates in the conversations that shape them for the benefit of its customers. It works with decision makers and regulators to shape policies in ways that meet evolving business needs while maintaining high standards of security, privacy, and reliability.

To promote a standards-based approach to cloud compliance, Microsoft is part of organizations such as CSA. Microsoft collaborates with other CSPs in the CSA and in other standards bodies to develop guidelines and best practices that inform future standards. Microsoft proactively engages with government customers, serving as a trusted advisor on the development and implementation of their cloud security policies and programs. Microsoft has extensive experience in security compliance assessments for its products and services for both U.S. and global government customers. As an architect and custodians of cloud systems, governments turn to Microsoft to inform them about how it ensures the confidentiality, reliability, and trustworthiness of its online services.

Microsoft works with government organizations such as the National Institute of Standards and Technology (NIST), European Network and Information Security Agency (ENISA), and others to evolve how they approach the security challenges associated with operating in a network-to-cloud-based environment. Microsoft is committed to building a constructive way forward to achieve consensus on the measures that are necessary to reduce risk and achieve desired security outcomes.

Microsoft cloud services create customer choice

Because of the comprehensive approach Microsoft takes to security, privacy, and reliability as well as compliance-specific processes, technologies, and certifications, it offers a comprehensive collection of trustworthy cloud services. Customers can choose to consume infrastructure, platforms, and software services as a complete package from Microsoft, ensuring a common control framework and consistency across the services. This approach helps to reduce the number of dependencies and compliance risks across providers that must be certified, which can simplify the process of achieving compliance and certifications.



At the same time, Microsoft believes in customer choice. Microsoft uses industry-standard technology to support interoperability with third-party solutions, and it delivers advanced hybrid capabilities so customers can move to the cloud at their own pace. With Microsoft, customers have the flexibility to adopt the components of cloud services that support their business goals and meet their compliance requirements today, with the flexibility to change the mix as their needs evolve.

Cloud services have the potential to create tremendous value. Microsoft cloud solutions help to reduce the risks and costs associated with compliance activities while improving security, reliability, and privacy. Microsoft uses all the resources at its disposal to help move toward a world in which any customer can benefit from the power of the cloud.

Acknowledgements

Contributors and Reviewers

Christine Aguirre
Kevin Allison
Mark Estberg
Sarah Fender
Adrienne Hall
Carlene Heath
Min Hyun
Vijay Kumar
Diane McDade
Michael Mattmiller
Chris Mullaney
Paul Nicholas
Tim Rains
Ben Ravani
Mike Reavey
Greg Roberts
Joe Scalone
Frank Simorjay
Shawn Veney
Stevan Vidich

© 2014 Microsoft Corp. 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.