Microsoft Azure Microsoft Intune

Regulatory Compliance and Auditing with Microsoft Cloud Services

for Financial Services Customers

Published: January 2016

Introduction

Many businesses that use a cloud-based service such as Microsoft Office 365, Microsoft Azure, Microsoft Intune, and Microsoft Dynamics CRM Online must comply with strict regulations for ensuring the privacy, security, access, and continuity of their customer data in the cloud. Microsoft has designed its enterprise cloud services to deliver on these needs by being resistant to attacks, protecting against unauthorized access, and offering features and functionality that meet or exceed the requirements of industry-leading standards, such as NIST 800-53, ISO 27001/27018 and SSAE 16 SOC1 and SOC2. These standards govern all aspects of the service that are related to the storage, access, and operation of customer data. Adhering to their depth and breadth enables Office 365, Azure, Intune, and Dynamics CRM Online (collectively, "Microsoft Cloud Services") to help commercial organizations meet their regulatory obligations.[1]

Financial services customers are subject to stricter regulatory oversight than many commercial customers are. They typically need deeper insights into a cloud service's capabilities, risks, and performance, as well as contractual commitments related to meeting their unique regulatory obligations. To meet these needs, Microsoft extends the standard Microsoft Cloud Services service contracts with a special amendment for financial services customers, and offers an optional, fee-based Microsoft Regulatory Compliance Program for them (for more information, see the box on page 3).

This document describes how the core contract amendments and the Microsoft Regulatory Compliance Program work together to support financial services customers in meeting their regulatory obligations as they relate to the use of cloud services.

Assessing the Risk of Using the Service

Regulated organizations generally are required to conduct a full risk assessment and due diligence before committing to a cloud service, and they must maintain valid risk assessments and appropriate oversight of the cloud vendor for as long as they use it.

Through the Trust Center, Microsoft provides detailed information on the trust tenets that are relevant for all customers who are evaluating a move to the Microsoft cloud. These tenets cover the top concerns that customers face in reviewing the impact and risk of moving to a cloud service, namely:

- Data ownership, location, portability, and privacy
- Security
- Trust
- Communication
- Availability and Reliability
- Supervision and Control
- Data Loss Prevention
- Business Continuity

When validating the suitability of Microsoft Cloud Services, customers may request or access directly the most recent Office 365, Azure, Intune, and Dynamics CRM Online audit reports (ISO 27001 and SSAE 16)

[1] Microsoft validates the compliance capability of the service through independent testing and annual third-party reviews.

and the ISO Statement of Applicability[2] from Microsoft. Customers also have access to the detailed documentation available on the Trust Center, such as information about the location of primary and backup datacenters, subcontractor lists, and rules for when Microsoft service administrators have access to customer data.

Microsoft also provides deeper technical trust and compliance information via the Service Trust Portal (STP). The STP is freely accessible with the following service subscriptions:

- Office 365 for business (both trial and paid subscriptions)
- Microsoft Azure (Azure Active Directory accounts only)
- Dynamics CRM Online

Customers can use the STP to access documents that describe a variety of topics, such as Microsoft's security practices for customer data that is stored online and independent third-party audit reports about Microsoft online services. Customers can also find out how our online services can help them be compliant with standards, laws, and regulations across industries, such as the:

- International Organization for Standardization (ISO)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Financial Industry Regulation Authority (FINRA)
- Federal Risk and Authorization Management Program (FedRAMP)

For detailed steps to access the STP, see these instructions.

A contract amendment for financial services customers also assures that you will be able to access and maintain insight and oversight into the risks. This optional amendment is available through the account manager and worldwide licensing.

Once customers have signed up for the service, they may perform ongoing risk assessments by accessing the information maintained on the Trust Center and the audit reports associated with the services.

[2] This document identifies the ISO controls that Microsoft applies in the cloud environment, and explains how and why they are appropriate.

The Microsoft Regulatory Compliance Program

This optional, fee-based program extends the compliance functionality of the standard Office 365, Azure, Intune, and Dynamics CRM Online services to provide deeper, ongoing engagement with Microsoft through:

- *Ad hoc access to additional information from Microsoft subject matter experts (SMEs)*—for instance, participants can ask questions or seek help or clarification about the standard service documentation.
- Access to *additional compliance-related information* that Microsoft may develop over time—such as customer FAQs, compliance summits, or documents that provide insights into the underpinnings and plans for the compliance features of the Office 365, Azure, Intune, and Dynamics CRM Online services.
- The opportunity for *one-to-one discussions* with Microsoft third-party auditors, if required.
- Participation in an *annual, webcast walkthrough of ISO and SSAE audit reports* with Microsoft SMEs. A recording of this webcast will also be made generally available.
- The option to *view the Microsoft control framework for the service*. This can enable a customer's risk officers to better understand and assess the scope and coverage of the framework (subject to more than 900 controls).
- The *opportunity to recommend future additions to the audit scope of the service*. All participants will be allowed to suggest new audit controls; the program's Financial Services Executive Committee (composed of one program participant from each regulatory region) will agree on up to five controls for inclusion in future audits.
- Access to detailed reports of the *external annual penetration tests* conducted on the service.
- The option to assess overall service approach to risk management and the underlying risks associated with using the service.

Preserving Customer Data Confidentiality

Keeping customer data private is a fundamental requirement for any organization. In addition to applying industry-leading operational systems and frameworks to control physical access, Microsoft preserves the confidentiality of customer data in its enterprise cloud services by logically isolating one customer's data from other customers and users; enabling encryption of data at rest and in transit; and undergoing regular penetration testing.

Data Isolation

Microsoft continuously works to ensure that the multi-tenant architecture of Office 365 supports enterprise-level security, confidentiality, privacy, integrity, and availability standards. Multiple forms of protection have been implemented throughout Office 365 to prevent customers from compromising Office 365 services or applications or gaining unauthorized access to the information of other tenants or the Office 365 system itself. Together, these protections provide robust logical isolation controls that provides equivalent threat protection and mitigation to that provided by physical isolation alone.

All of the Office 365 services and workloads are built on top of Azure Active Directory and as a result they use the same authorization and role based access control (RBAC) model. All Office 365 requests are mediated through the authorization and access control features in Azure Active Directory. All Office 365 data sessions are either user-scoped or tenant-scoped, and users can't see outside the tenant scope. Access to Office 365 objects is controlled via user account permissions that are enforced by Azure Active Directory and operating system access control lists. The authorization stack prevents you from accessing data for which you don't have the appropriate credentials. Finally, there is no service code that allows a user from one tenant to execute commands against another tenant.

Azure also uses logical isolation to segregate each customer's environment and data from that of others. Data in Azure Storage is controlled with a Storage Access Key (SAK). Shared Access Signature (SAS) tokens can be generated using SAKs to provide more granular, restricted access. Network controls block customer-to-customer access to Azure services and no access from the internet is enabled by default.

Dynamics CRM Online provides customers with logical data isolation through separate SQL databases. Every Dynamics CRM Online customer also receives a unique identifier in the service, which restricts access by default to that customer's domain, for customer-to-customer data separation.

Encryption

Office 365 and Dynamics CRM Online encrypt client/server customer data in transit for all services using TLS. To encrypt customer data at rest, Office 365 supports Azure Rights Management Services, BitLocker, S/MIME encryption, and per-file encryption, among others, and soon Advanced Encryption. Together, these technologies minimize the risk of information leakage by encoding content, allowing access only by intended users, extending protection beyond the initial publication location, and encrypting Office document attachments. Customers control the encryption infrastructure and manage encryption keys from their own premises.

Azure uses encryption to help secure communications between datacenters. Customers can also configure encrypted communications TLS and have a number of options for encrypting their data stored in Azure. These include BitLocker for full disk encryption and data import/export, EFS and cryptographic services in Windows Server, Microsoft StorSimple cloud-integrated storage, .NET cryptographic services, Rights Management Services (RMS), as well as partner solutions.

Dynamics CRM Online encrypts client/server data in transit using TLS. Dynamics CRM also offers SQL based Transparent Data Encryption as an option to encrypt all of customer data when at rest.

Microsoft Intune customer software packages are encrypted, all data in transit is encrypted using TLS.

For more information on the cryptography and encryption features in Office 365, see Data Encryption Technologies in Office 365, available for download from the STP.

Penetration Testing

Microsoft regularly conducts penetration testing and vulnerability assessments as one of the activities required by the Microsoft Security Development Lifecycle (SDL), Payment Card Industry, FedRAMP and/or ISO 27001 certification. Microsoft security practices and the ongoing SDL processes enable the service to rapidly mitigate new threats and attacks and protect customer data. Testing standards have also included Open Web Application Security Project Top 10 and CREST-certified testers. As part of the ongoing risk management program, test results are resolved and the resolution is validated as part of the compliance program. In addition, customers can conduct authorized penetration testing on their Office 365 properties and applications in Azure.

Maintaining Customer Data Availability

Microsoft enterprise cloud products, services, and controls have been designed to address failures at hardware, network, and data center levels. Customers may access their service availability reports at any time via the Microsoft administrator portal.

Microsoft's service commitments, financially backed by Service Level Agreements (SLAs) of at least 99.9% availability, are made possible by several core design principles for its architecture. Redundancy is built in at every layer for greater failure protection and recovery. Service resiliency is achieved via active load balancing, dynamic task prioritization, and constant recovery testing. By distributing service functionality among many different components, Microsoft helps limit the scope, impact, and recovery times of a failure. Similarly, simplification of the service, such as using standardized components and processes, makes for more predictable, less complex deployment and maintenance. Continuous monitoring, automated and manual service recovery, and 24/7 human staffing make the detection, investigation, and resolution of issues more efficient. In Azure, customers can architect applications for high availability using its global network of datacenters. Storage is replicated locally and at minimum to a second data center in the same geography. Customers can view where data is stored at the Trust Center.

Dynamics CRM Online provides a robust a high-availability and disaster recovery for customer data that is based off SQL Server "Always-On" technologies. With local and remote redundancy of customer data and regular simulation of these scenarios ensures a high level of data availability and reliability for customers.

Ensuring Customer Data Integrity

Microsoft helps maintain customer data integrity by providing automated protections against external threats, plus native features for managing cloud content.

Automated Protections

Office 365 uses Microsoft Exchange Online Protection to scan all email messages that enter the service. The multiple antivirus and antispam engines of this tool capture known and new threats against the system. We regularly test, verify, and update these tools and systems to validate performance and address new threats that arise. If files ever do become corrupted, the service stops using the corrupted data source and restores to an earlier time to keep the corruption from spreading through backups and the infrastructure. Azure offers anti-malware features with a simple checkbox when provisioning solutions, both native Microsoft as well as trusted partners.

Features for Customer Control

Office 365 provides many tools that help customers do their part to protect the integrity of their customer data in the cloud. These include Data Loss Prevention, enhanced Rights Management Services, legal holds, and eDiscovery. Configurable filters and permissions enable customers to process junk mail system-wide and/or by user. The service also supports deploying localized antivirus protection at every workstation (a recommended practice). Other security measures for which customers are responsible are described in the box on the page below. At the storage level, Azure allows customers to configure MD5 signature checking with each read/write operation.

Managing Data Stored in the Cloud

Microsoft Cloud Services are designed to ensure customers have full control over their customer data. Core Office 365 features for managing, monitoring, finding, removing, and handling content include eDiscovery, Data Loss Prevention, legal holds, and transport rules. In Azure, customers can implement operating system level logging to provide full visibility into their data stored in the cloud.

We also offer customers the ability to download a complete copy of their data to on-premises.

Controlling Access to the Service

By default, no one has access to customer data without authorization. Customers remain in control of all users' access, and Microsoft provides contractual guarantees for how administrative access is handled (for instance, when providing technical support or responding to a subpoena).

Customer Login Controls and Visibility

Through Active Directory federation, customers can configure the service to limit Office 365 logons to specific IP addresses, so that devices can connect only through the customer's corporate network. Customers also have direct access to a subset of in-service logs to verify who has accessed which data, and what they did with it. This includes viewing mailbox usage, administration activities, and SharePoint Online sites. Other core service features that provide visibility for compliance purposes include Exchange Online, SharePoint Online, and Dynamics CRM auditing, the eDiscovery Center console, and the Microsoft administrator portal. Microsoft Intune administrative portal can be accessed after authorization from Azure Active Directory (or Azure Active Directory Premium for EMS License holders). Microsoft Intune has the ability to do a two factor authentication during the device enrollment process.

Administrator access to the Azure portal can be managed using Azure Active Directory. Customers can also enable Azure Active Directory to control user access to applications they run in Azure and enable single sign-on to world of other cloud applications. All access is logged and reports are readily available from the Azure portal. Microsoft provides customer guidance for hardening their administrator environment. Azure offers a multi-factor authentication (MFA) service for customers to secure on-premises, cloud and hybrid solutions.

A Secure Cloud Is a Shared Responsibility

Because Microsoft enterprise cloud services support a high degree of customer configuration, some of the responsibility for secure management of the service lies with the customers. At a minimum, customers must complete the following tasks to help ensure the security of their customer data:

- *Account management*—Configure account setup and deletion; password complexity, expiry, and history; account lockout; and/or online user IDs.
- *Access control*—Ensure that an access control policy and monitoring is implemented for the cloud service and in each application, including granting, revoking and reviewing each user's access rights, as well as denying "Guest" users, "anonymous" users, and users who cannot be authenticated.
- *Segregation of duties*—Configure the level of access for each user according to job function, including appointing appropriate staff to manage access control.
- *Application/infrastructure security* – Customers are responsible for securing their applications and infrastructure in Azure. This includes the use of secure development, deployment, and operational practices.
- *Awareness and training*—Train employees in how to configure and control access to the service and data, and how to protect data confidentiality. Monitor employee actions to ensure compliance with your corporate policies.
- *Support requests*—As with support for on-premises software, manage sensitive or restricted data in any support request to reduce distribution of sensitive information over open channels.

Microsoft Access Controls

Microsoft engineers do not have default access to your customer data. Instead, they are granted access only when necessary under management oversight. The operational processes and controls that govern access to and use of customer data in the Microsoft cloud are regularly verified by accredited audit firms. These firms, and Microsoft, regularly perform sample audits to attest that access is only for legitimate business purposes. Strong controls and authentication, including the use of multi-factor authentication, help limit access to customer data to authorized personnel only. When access is granted, whether to Microsoft personnel or our subcontractors, it is carefully controlled and logged, and revoked as soon as it is no longer needed.

For Office 365 and Azure, this access is also time-limited. Cardkey and biometric protections are in place to restrict physical access to datacenters. All Microsoft subcontractors are subject to the same access controls. Restricted access to customer data by Microsoft personnel is enforced through technical and operational controls which are subject to ongoing monitoring and recurring audit by independent third parties for certifications such as ISO, SSAE16, and others.

Regulator's Right to Examine the Service

The contract amendment for financial services organizations gives a customer's external regulators the right to access and examine the Office 365, Azure, Dynamics CRM Online, and Intune service. As required, regulators may engage with Microsoft to help them understand the systems that are relevant to their regulatory domain. Microsoft reserves the right to charge the customer if the regulator's scope exceeds the existing audits and certifications.

Customer's Right to Examine the Service

As explained in the section Controlling Access to the Service, Microsoft provides many built-in features to help customers examine and verify access, control, and service operation. They may also examine all public information about the service on the Trust Center, as well as request the latest audit reports through their account manager or Microsoft support.

The contract amendment for financial services customers adds the ability for a company's internal compliance officers to examine the service more deeply to meet regulatory requirements. This examination is first fulfilled through the standard audit reports that are available in the service. Further detail is available through participation in the optional Microsoft Regulatory Compliance Program (for more information, see the box on page 3). Through this program, customers may invoke the right to examine the control framework of the service, review its risk management framework, hold one-to-one discussions with SOC auditors, and obtain other in-depth views into the service directly with Microsoft subject matter experts. Together, this additional level of oversight ensures that customers can meet their own audit requirements, that they can maintain supervision of the service and have ongoing accountability with the service provider.

Additional Information

Customers who have additional concerns related to the auditing and compliance features of Microsoft enterprise cloud services or the Microsoft Regulatory Compliance Program may:

- Consult their account manager

- Request the ISO Statement of Applicability from their account manager, Microsoft support, or download it directly from the Service Trust Portal
- Visit the Microsoft Security Development Lifecycle web site
- Review the white paper, Security Management in Microsoft Azure
- Download the service descriptions for Office 365 and Dynamics CRM Online
- Visit the Microsoft Trust Center
- Visit the Microsoft Transparency Hub

Summary

Microsoft has designed its enterprise cloud services to deliver on these needs by being resistant to attacks, protecting against unauthorized access, and offering features and functionality that meet or exceed the requirements of industry-leading standards, such as NIST 800-53, ISO 27001/27018 and SSAE 16 SOC1 and SOC2. Adhering to their depth and breadth enables Office 365, Azure, Intune, and Dynamics CRM Online to help commercial organizations meet their regulatory obligations.

Microsoft engineers do not have default access to your customer data. Instead, they are granted access only when necessary under management oversight. The operational processes and controls that govern access to and use of customer data in the Microsoft cloud are regularly verified by accredited audit firms.

Further detail is available through participation in the optional Microsoft Regulatory Compliance Program. Through this program, customers may invoke the right to examine the control framework of the service, review its risk management framework, hold one-to-one discussions with SOC auditors, and obtain other in-depth views into the service directly with Microsoft subject matter experts.