Think Cloud Compliance

Microsoft Cloud Security for Legal and Compliance Professionals

Introduction to security in a cloud-enabled world

Security in the cloud is a partnership

The security of your Microsoft cloud services is a partnership between you and Microsoft.

Microsoft

Microsoft cloud services are built on a foundation of security, privacy and compliance. Microsoft provides you security controls and capabilities to help you protect your data and applications.

You

You own your data and identities and the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components you control (varies by service type).

Microsoft's Trusted Cloud principles

Security	Safeguarding your data with state-of-the-art technology, processes, and encryption is our priority.
Privacy & Control	Privacy by design with a commitment to use customers' information only to deliver services and not for advertisements.
Compliance	The largest portfolio of compliance standards and certifications in the industry.
Transparency	We explain what we do with your data, and how it is secured and managed, in clear, plain language.

The responsibilities and controls for the security of applications and networks vary by the service type.

SaaS
Software as a Service

Microsoft operates and secures the infrastructure, host operating system, and application layers. Data is secured at datacenters and in transit between Microsoft and the customer.

You control access and secure your data and identities, including configuring the set of application controls available in the cloud service.

PaaS
Platform as a Service

Microsoft operates and secures the infrastructure and host operating system layers.

You control access and secure your data, identities, and applications, including applying any infrastructure controls available from the cloud service.

You control all application code and configuration, including sample code provided by Microsoft or other sources.

IaaS
Infrastructure as a Service

Microsoft operates and secures the base infrastructure and host operating system layers.

You control access and secure data, identities, applications, virtualized operating systems, and any infrastructure controls available from the cloud service.

Private cloud

Private clouds are on-premises solutions that are owned, operated, and secured by you. Private clouds differ from traditional on-premises infrastructure in that they follow cloud principles to provide cloud availability and flexibility.

Keys to success

Enterprise organizations benefit from taking a methodical approach to cloud security. This involves investing in core capabilities within the organization that lead to secure environments.

Governance & Security Policy

Microsoft recommends developing policies for how to evaluate, adopt, and use cloud services to minimize creation of inconsistencies and vulnerabilities that attackers can exploit.

Ensure governance and security policies are updated for cloud services and implemented across the organization:

- Identity policies
- Data policies
- Compliance policies and documentation

Administrative Privilege Management

Your IT administrators have control over the cloud services and identity management services. Consistent access control policies are a dependency for cloud security. Privileged accounts, credentials, and workstations where the accounts are used must be protected and monitored.

Identity Systems and Identity Management

Identity services provide the foundation of security systems. Most enterprise organizations use existing identities for cloud services, and these identity systems need to be secured at or above the level of cloud services.

Threat Awareness

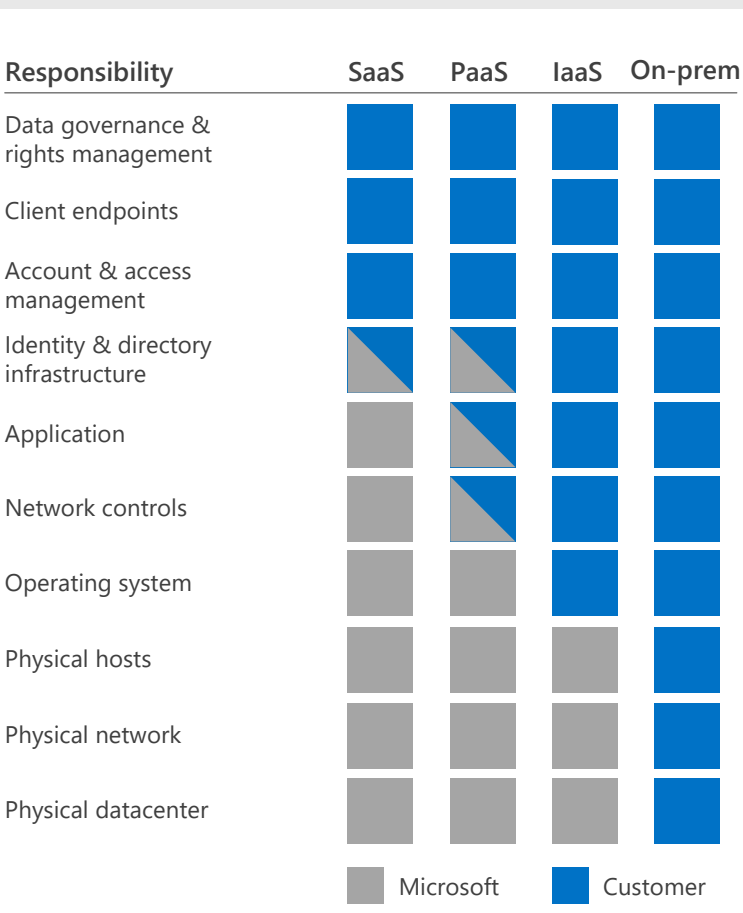
Organizations face a variety of security threats with varying motivations. Evaluate the threats that apply to your organization and put them into context by leveraging resources like threat intelligence and Information Sharing and Analysis Centers (ISACs).

Data Protection

You own your data and control how it should be used, shared, updated, and published.

You should classify your sensitive data and ensure it is protected and monitored with appropriate access control policies wherever it is stored and while it is in transit.

Your responsibility for security is based on the type of cloud service. The following chart summarizes the balance of responsibility for both Microsoft and the customer.



Top security certifications

Many international, industry and regional organizations independently certify that Microsoft cloud services and platforms meet rigorous security standards and regulatory requirements.

By providing customers with compliant, independently verified cloud services, Microsoft also makes it easier for you to achieve compliance for your infrastructure and applications.

This page summarizes the top certifications. For a complete list of certifications and more information, see the Microsoft Trust Center.

Learn more...

View compliance by service

	Regulatory and Compliance Domain	Office 365	Microsoft Azure	Microsoft Dynamics 365	Microsoft Intune
Broadly Applicable	ISO 27001	✓	✓	✓	✓
	ISO 27017		✓		✓
	ISO 27018	✓	✓	✓	✓
	SOC 1 / SOC 2 / SOC 3	✓	✓	✓	✓
	CSA Star	✓	✓	✓	✓
United States Government	FedRAMP	✓	✓	✓	
	CJIS	✓	✓	✓	
	DoD DISA	✓ Level 4	✓ Level 4	✓	
	FDA 21 CFR Part 11	✓	✓	✓	
	ITAR	✓	✓		
	IRS 1075	✓	✓		
Industry Specific	HIPAA / HITECH	✓	✓	✓	✓
	PCI DSS Level 1	N/A	✓	N/A	N/A
	FERPA	✓	✓	✓	N/A
	CDSA	N/A	✓	N/A	N/A
Region/Country Specific	EU Model Clauses	✓	✓	✓	✓
	UK G-Cloud v6	✓	✓	✓	✓
	Australia CCSL (IRAP)	✓	✓	✓	
	Singapore MTCS	✓	✓	✓	
	Japan FISC	✓	✓		
	New Zealand GCIO	✓	✓	✓	✓
	Spain ENS	✓	✓		
	China DJCP	✓	✓		

Microsoft

How Microsoft builds a trusted cloud platform

Microsoft is committed to the privacy and security of your data and applications in the cloud

Through industry-leading security practices and unmatched experience running some of the largest online services around the globe, Microsoft delivers enterprise cloud services customers can trust.

Decades of engineering experience have enabled Microsoft to develop leading-edge best practices in the design and management of online services. This section summarizes Microsoft's comprehensive approach, starting with your data and drilling down to the physical media and datacenters.

Learn more...

Microsoft Trust Center

Data Privacy

Data ownership

It's your data.

We define "customer data" as all the data (including all text, sound, software, or image files) that a customer provides, or that is provided on customers' behalf, to Microsoft through use of the Online Services.

Data use

We do not use customer data for purposes unrelated to providing the service, such as advertising. We have a "No Standing Access" policy — access to customer data by Microsoft personnel is restricted, granted only when necessary for support or operations, and then revoked when no longer needed.

Disclosure of government request for data

If a government approaches us for access to customer data, we redirect the inquiry to you, the customer, whenever possible. We have and will challenge in court any invalid legal demand that prohibits disclosure of a government request for customer data.

Learn more . . .

Transparency Center

Data access

You are in control of your data. You have control over who can access your data and how it is securely accessed and deleted. Depending on the service, you choose where your data is stored geographically.

Privacy reviews

As part of the development process, privacy reviews are performed to verify that privacy requirements are adequately addressed. This includes verifying the presence of privacy-related features that allow customers to control who can access their data and configure the service to meet the customer's regulatory privacy requirements.

Data portability

It's your data, so if you ever choose to leave the service, you can take your data with you and have it deleted permanently from our servers.

Read more...

Protecting Data and Privacy in the Cloud

Data encryption and rights management

Data in transit

Best-in-class encryption is used to help secure data in transit between datacenters and you, as well as at Microsoft datacenters. Additionally, customers can enable Perfect Forward Secrecy (PFS). PFS uses a different encryption key for every connection, making it more difficult for attackers to decrypt connections.

Encryption for Azure-based solutions

For Azure-based solutions, you can choose to implement additional encryption using a range of approaches — you control the encryption method and keys. Built-in TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.

Azure Key Vault

Safeguard cryptographic keys and other secrets used by cloud apps and services. Microsoft does not see or extract your keys.

Data at rest

Office 365 and other SaaS services use encryption at rest to protect your data on Microsoft servers.

Azure Rights Management (Azure RMS)

Azure RMS uses encryption, identity, and authorization policies to help secure your files and email. Protection stays with the files and emails — independently of the location inside or outside your organization, networks, file servers, and applications.

- You can use Azure RMS with Office 365: SharePoint Online and Exchange Online.
- You can configure Azure RMS for your entire organization.
- You can bring your own key to comply with your organization policies.

Learn more...

Azure Rights Management

Identity and access

You control access to your data and applications

Microsoft offers comprehensive identity and access management solutions for customers to use across Azure and other services such as Office 365, helping them simplify the management of multiple environments and control user access across applications.

Azure Active Directory and Multi-Factor Authentication

Azure Active Directory enables customers to manage access to Azure, Office 365, and a world of other cloud apps. Multi-Factor Authentication and access monitoring offer enhanced security.

Third-party SaaS identity management

Azure AD enables easy integration and single sign-on to many of today's popular SaaS applications, such as Salesforce.

Microsoft

Software and services

Secure Development Lifecycle (SDL)

Privacy and security considerations are embedded through the SDL, a software development process that helps developers build more secure software and address security and privacy compliance requirements. The SDL includes:

- Risk assessments
- Attack surface analysis and reduction
- Threat modeling
- Incident response
- Release review and certification

Secure development across the Microsoft cloud

Microsoft Azure, Office 365, Dynamics 365, and all other enterprise cloud services use the processes documented in the SDL.

Learn more...

Security Development Lifecycle

Proactive testing and monitoring

Learn more...

MICROSOFT DIGITAL CRIMES UNIT

Microsoft Digital Crimes Unit

Microsoft's Digital Crimes Unit (DCU) seeks to provide a safer digital experience for every person and organization on the planet by protecting vulnerable populations, fighting malware, and reducing digital risk.

Microsoft Cyber Defense Operations Center

The Microsoft Cyber Defense Operations Center is a 24x7 cybersecurity and defense facility that unites our security experts and data scientists in a centralized location. Advanced software tools and real-time analytics help us protect, detect, and respond to threats to Microsoft's cloud infrastructure, products and devices, and our internal resources.

Prevent Breach, Assume Breach

In addition to the "prevent breach" practices of threat modeling, code reviews, and security testing, Microsoft takes an "assume breach" approach to protecting services and data:

- Simulate real-world breaches
- Live site penetration testing
- Centralized security logging and monitoring
- Practice security incident response

Read more...

Microsoft Enterprise Cloud Red Teaming

Datacenter infrastructure and networking security

Operational Security Assurance (OSA)

OSA is a framework that focuses on infrastructure issues to help ensure secure operations throughout the lifecycle of cloud-based services.

Learn more...

Operational Security Assurance (OSA)

Private connection

Customers can use ExpressRoute to establish a private connection to Azure datacenters, keeping their traffic off the Internet.

Learn more...

Microsoft Azure ExpressRoute

Physical datacenter security

24-hour monitored physical security

Datacenters are constructed, managed, and monitored to physically shelter data and services from unauthorized access as well as environmental threats.

Zero standing privileges

Microsoft maintains a "No Standing Access" policy on customer data. We've engineered our products so that a majority of service operations are fully automated and only a small set of activities require human involvement. Access by Microsoft personnel is granted only when necessary for support or operations; access is carefully managed and logged, then revoked when no longer needed. Datacenter access to the systems that store customer data is strictly controlled via lock box processes.

Data destruction

When customers delete data or leave a service, they can take their data with them and have it deleted permanently from Microsoft servers. Microsoft follows strict standards for overwriting storage resources before reuse, as well as for the physical destruction of decommissioned hardware. Faulty drives and hardware are demagnetized and destroyed.

Learn more...

For more information on Microsoft's Trusted Cloud visit the Microsoft Trust Center

Microsoft