Microsoft

Securing the Microsoft Cloud

Securing the Microsoft Cloud

Microsoft recognizes that trust is necessary for organizations and customers to fully embrace and benefit from cloud services. We are committed to providing customers with the information they need to have confidence in Microsoft as their preferred cloud provider. Our security policies and practices are based on leading industry standards and more than two decades of experience in delivering online services and managing datacenters.

This strategy brief discusses how Microsoft addresses the challenges of providing a trustworthy infrastructure for more than 200 cloud services, including Bing, Office 365, OneDrive, Microsoft Azure, Skype, and Xbox Live that are hosted in our global cloud infrastructure of more than 100 datacenters. It provides a review of our risk-based information security and related privacy controls, and describes the compliance framework we follow to ensure our cloud infrastructure helps customers meet their security and compliance related needs.

Cloud security challenges

Cloud computing offers both challenges and opportunities for organizations looking to harness the favorable economics and operational flexibility of an online services model. The growing interdependence of services, complex global compliance requirements, a dynamic hosting environment, and the growing sophistication of threats requires that cloud services providers employ robust policies, technologies, and processes to protect sensitive information and meet compliance needs.

All cloud customers and providers face these challenges. Many organizations are recognizing that the scale and scope of Microsoft's capabilities can help them take advantage of better security in cloud services than they can provide for themselves. Microsoft has been meeting the following challenges for more than 21 years:

Proliferation of legislation and standards. New laws and standards are being introduced at an accelerating rate, increasing complexity and sometimes limiting the ability of enterprises and public sector organizations to meet their compliance needs while using cloud services. Microsoft's compliance program, along with our sharing of third party audits and attestations, are key to meeting this challenge.

Consumer privacy and law enforcement transparency. Recent news about law enforcement agency practices has raised important privacy questions. In 2012, Microsoft made a commitment to transparency with legal demands by publishing our Law Enforcement Requests Report. We have also made a commitment to protect communication from unauthorized access by encrypting traffic between our customers and Microsoft. This includes our major communications, productivity, and developer services such as Outlook.com, Office 365, OneDrive and Microsoft Azure, and will provide protection across the full lifecycle of customer-created content.

Data sovereignty and localization of services. Microsoft offers enterprises and public sector organizations the ability to select geographic boundaries for many of our cloud services, such as Microsoft Azure. This helps our customers address new legislation and standards, along with consumer privacy and law enforcement transparency concerns, that have caused geographic constraints on the delivery of cloud services.

More persistent and sophisticated attacks. This represents a challenge for everyone involved with online and cloud services. Traditional attacks continue, while new attacks challenge traditional security practices. We bring together hundreds of subject matter experts across our cloud infrastructure, research, development, operations, and incident response teams to protect our customers from criminal and unlawful attacks, and intrusions. We also work with industry partners, peers, and research organizations to understand and respond to this evolving threat landscape. We also share recommended practices with consumers of cloud services so that they can also take action to protect themselves.

As a part of our defense-in-depth strategy, we maintain a state of readiness following a principle of "assumed breech" and tune our controls and operations to limit an attacker's lateral movement or escalation of privilege.

Most importantly, we are able to apply the critical updates necessary to protect our services more rapidly than most enterprise customers can do in a heterogeneous environment.

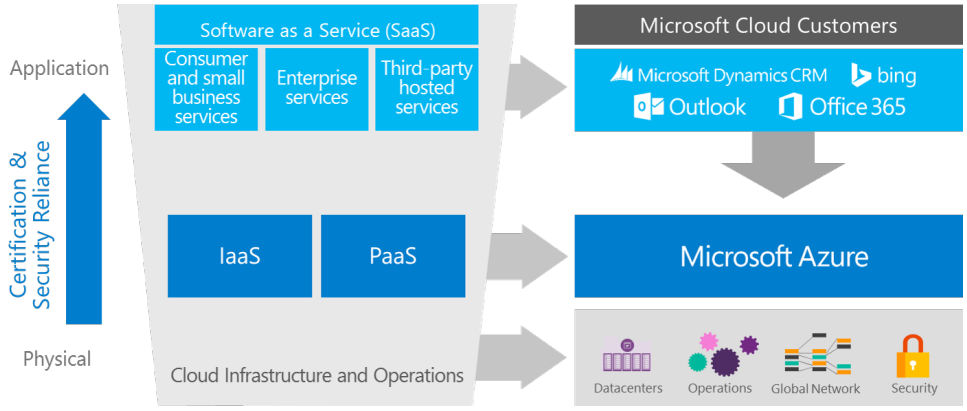
Cloud and on-premise interoperability. As customers adopt more cloud services, they typically do so alongside existing on premises workloads, and need to effectively interoperate in a hybrid model to maintain business operations. With these new dependencies come mutual expectations that services and hosted applications be secure and available, and that the cloud-based security controls work in conjunction with other on premises security controls. Microsoft provides guidance on how to use our services in a hybrid model to meet business goals, including controls like monitoring, resiliency targets, response, and configuration management.

Changing infrastructure form factors. New technologies requires us to create new types of security controls and our Information Security Program maintains strong internal partnerships among security, product, and service delivery teams. This allows us to meet our current needs while continually building capabilities for future demands. These changes include rapidly evolving technologies, massive scale, changing business models, and dynamic hosting environments which all represent challenges to security and compliance. The scale and continuing growth of our environment requires us to rely heavily on standardization and automation.

Cloud reliance

Reliance is the glue that holds the cloud security model together. A security model structures our security capabilities. These capabilities can be thought of as a stack starting from the physical layer at the base and working up through layers that include network, host, and application. Certifications and attestations are simply a verification of the sets of capabilities and are used to enable reliance.

The ability to rely and build upon security and compliance capabilities allows each component to focus on its most relevant and valuable security functions. By the nature of the cloud, there are always components that rely upon one another. At a minimum, there is the cloud service provider and the cloud service consumer. Reliance also exists between cloud services, such as the use of Microsoft Azure by Office 365. Reliance even exists at the infrastructure layer, for example, in cases where datacenters are leased from a third party. Each component of a cloud service must meet the security and compliance needs of each of the elements that rely on it, as well as ensure that the elements it relies upon can meet its needs.



Security at our foundation

Application security is a key element in Microsoft's approach to securing its cloud computing environment. The rigorous security practices employed by development teams at Microsoft were formalized into a process called the Security Development Lifecycle (SDL) in 2004.

The SDL process is development methodology agnostic and is fully integrated with the application development lifecycle from design to response. Various phases of the SDL process emphasize education and training, and also mandate that specific activities and processes be applied as appropriate to each phase of software development.

Starting with the requirements phase, the SDL process includes a number of specific activities that need to be considered for the development of applications to be hosted in the Microsoft cloud.

One of the key steps is threat modeling and attack surface analysis, where potential threats are assessed, exposed aspects of the service is evaluated, and the attack surface is minimized by restricting services or eliminating unnecessary functions. The later stages then ensure that the controls are fully tested to mitigate the potential threats, so customers can have confidence in the final service release.

In addition to SDL, Microsoft applies a framework called Operational Security Assurance (OSA) to online services, which takes over after code, which has been subject to SDL, moves to operations. Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively.

Information Security Management System

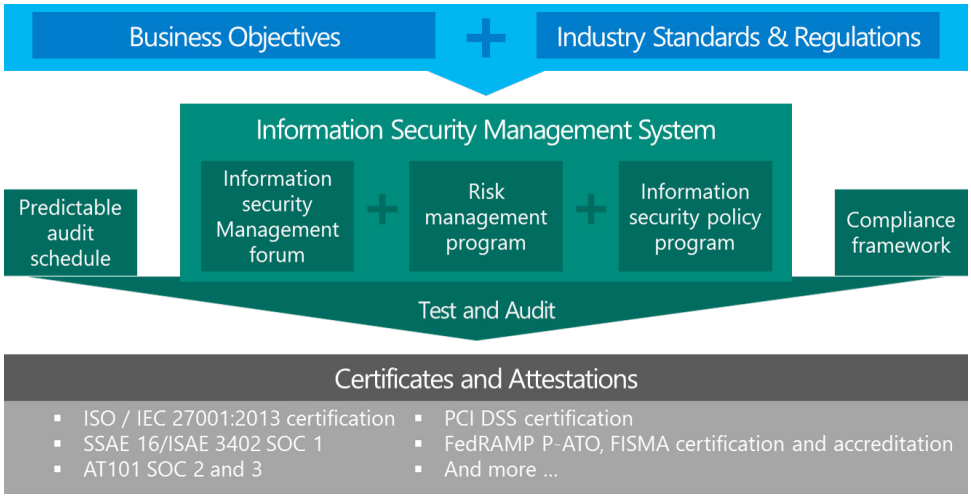
The Microsoft Information Security Management System (ISMS) guides how we make risk-informed decisions and drive them across our cloud infrastructure operations.

The system is built on business objectives and security requirements, and includes a compliance framework, and audit schedule that results in certifications and attestations. This provides an overall assurance that control objectives are being met while satisfying regulatory requirements.

The governance and controls framework is made up of four areas:

- The Microsoft Security Policy suite includes the policy, standards, baselines, and standard operating procedures. These are the Microsoft-specific security requirements that must be followed by all of the Microsoft teams.
- The Requirements are the collection of regulatory, statutory, and industry obligations, plus any additional business requirements that the cloud infrastructure must meet for Microsoft's cloud services.
- The Control Activities represent the operational work that the team performs in support of the security objectives. Each control activity has an owner and maps to both the policy suite and the requirements.
- Audits ensure that the performance of control activities meet the individual requirements.

This framework is connected by various governance workflows – for example, filing an exception when the policy cannot be met or creating and managing issues when gaps are identified between control activities and requirements.



Microsoft Information Security Management System

Visit one of the Microsoft Trust Centers for more detail on specific solutions:

- **Microsoft Azure Trust Center:** azure.microsoft.com/support/trust-center
- **Office 365 Trust Center:** trustoffice365.com
- **Dynamics CRM Trust Center:** microsoft.com/dynamics/crm-trust-center
- **Microsoft Intune Trust Center:** microsoft.com/intune-trust-center

Comprehensive compliance program

The Microsoft cloud services' environment must meet numerous government-mandated, regional- and country-specific data security standards, and industry-specific security requirements, in addition to Microsoft's own business-driven specifications.

Microsoft's compliance framework is based on security capabilities from sources such as the National Institute of Standards and Technology (NIST) Special Publication 800-53, ISO/IEC 27001:2013, AT 101 Service Organization Controls (SOC) 2 Trust Service Principles, the European Union Data Protection Directive, and the Payment Card Industry Data Security Standard (PCI DSS). It also uses the ISO/IEC 27001:2013 approach to provide a mechanism of continual improvement. Microsoft regularly monitors changes in regulatory needs and adjusts the compliance framework and audit schedule accordingly.

The compliance team works across operations, product, and service delivery teams, and with internal and external auditors to ensure Microsoft is in compliance with relevant regulatory, statutory, and industry obligations.

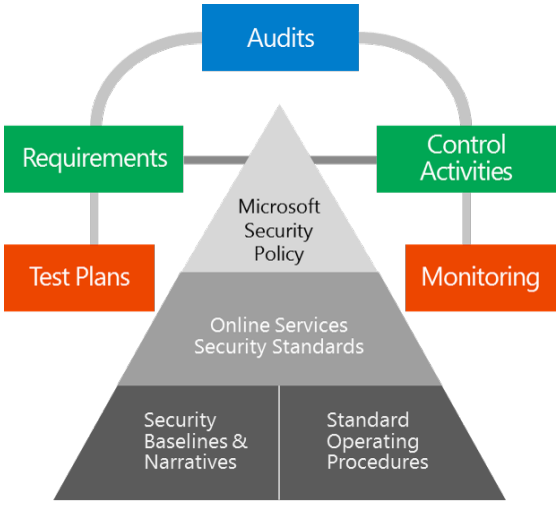
In addition to providing a high level of assurance that our controls are operating as expected, the compliance framework also results in several important certifications and attestations for Microsoft's cloud infrastructure, including ISO/IEC 27001:2013 certification, SSAE 16/ISAE 3402 SOC 1 Type I and Type II and AT Section 101 SOC 2 and 3 Type I and Type II attestations, as well as FedRAMP and FISMA Certification and Accreditation.

To help our customers comply with their own requirements, we build our services with common privacy and security requirements in mind. However, it is ultimately up to our customers to evaluate our offerings against their own requirements, so they can determine if the way they use cloud services satisfies their compliance needs. We are committed to providing our customers with detailed information about our cloud services to help them make informed decisions.

Controls framework

Customers evaluating Microsoft's cloud services often ask how our compliance framework is actually structured. Microsoft has a series of domains that are based on the ISO/IEC 27001:2013 standard, along with specific industry obligations, such as the Payment Card Industry Data Security Standard and the FISMA NIST SP 800-53 standard. Specifically, the control framework maps over 800 control activities performed by our operations teams to individual requirements. Through process and tooling, we are able to map these elements, and identify and address gaps or areas that may be duplicative. For example, a single control activity may map to similar requirements across multiple audits.

This mapping shifts the focus from individual, specific audit requirements to rationalized controls representing the work being performed, allowing teams to focus on the effectiveness and design of control activities. The control framework also helps us develop a predictable audit schedule. For example, we are able to use control activity performance data for pre-audit preparation, with a focus on key controls. Additionally, we are able to prepare for multiple audits with a single, annual control activity readiness review. These processes ensure that the Microsoft cloud infrastructure meets its obligations and we are able to share these results with our customers through certifications and attestations.



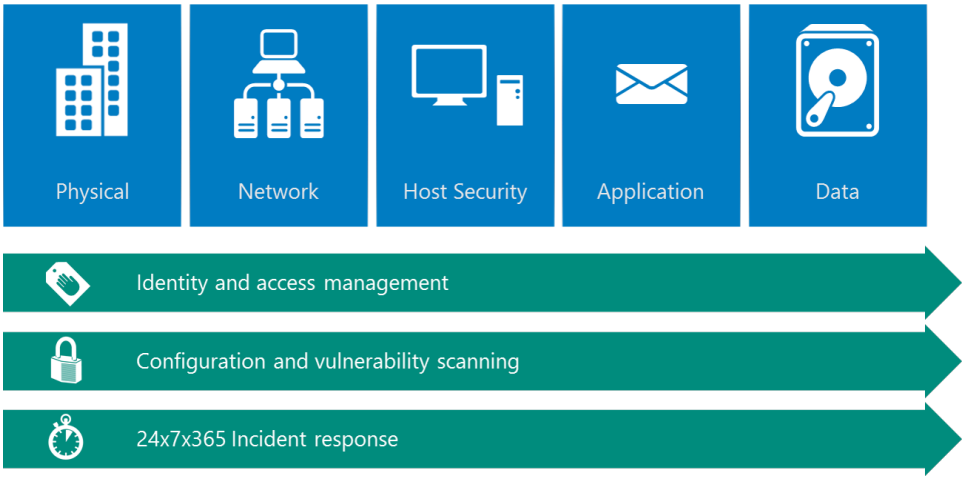
Defense-in-depth

Defense-in-depth is a security best practice and it is an approach Microsoft uses across our cloud services and infrastructure. Applying controls at multiple layers can involve sometimes employing overlapping protection mechanisms, developing risk mitigation strategies, and responding quickly and effectively to attacks when they occur. Using multiple security measures of varying strength—depending on the sensitivity of the protected asset—results in improved capacity to prevent breaches or to lessen the impact of a security incident.

When we deploy a service to our datacenters, we assess and address every part of the service stack – from the physical controls, to encrypting all data that moves over our network, to locking down the host servers, to keeping malware protection up-to-date, to ensuring applications themselves have appropriate safeguards in place. Maintaining a rich set of controls and a defense-in-depth strategy ensures that if any one area should fail, there are compensating protections in other areas.

Just in Time and Just Enough Administration is an important part of our approach. This technology enables organizations to present operators with only the amount of access required to perform specific tasks.

In addition, Microsoft has built unique assets in our Digital Crimes Unit and Malware Protection Center—the work they are doing around the cloud ecosystem is continuously applied to protecting customers and their data.



An example of Defense-in-Depth

Security incident response

An important part of Microsoft's security capabilities include our response processes. The Security Incident Management (SIM) team responds to potential security issues when they occur, operating around the clock. The SIM processes are aligned with ISO/IEC 18044 and NIST SP 800-61.

There are six phases to the SIM incident response process:

Preparation – SIM staff undergo ongoing training to be ready to respond quickly and effectively when a security incident occurs.

Identification – looking for the cause of an incident, whether intentional or not, often means tracking the issue through multiple layers of the Microsoft cloud computing environment. SIM collaborates with members from internal Microsoft teams to diagnose the origin of a given security incident.

Containment – once the cause of the incident has been found, SIM works with all necessary teams to contain the incident. Containment methods are based on the business impact of the incident.

Mitigation – SIM coordinates with relevant product and service delivery teams to reduce the risk of incident recurrence.

Recovery – continuing to work with other groups as needed, SIM assists in the service recovery process. This phase often includes suggestions and recommendations for additional monitoring and penetration testing to validate mitigation efficacy.

Lessons learned – after resolution of the security incident, SIM convenes a joint meeting with all involved personnel to evaluate the event and to record lessons learned during the incident response process.

Looking forward

The challenges for delivering secure and reliable cloud services will continue to evolve and Microsoft is continually adapting our strategies, policies, and practices to help customers stay protected and compliant.

Regulatory standards are proliferating around the world at an accelerating rate and organizations are challenged to stay abreast of the changing landscape, while maintaining compliance across all of the geographies in which they operate.

In addition, advances in technology are changing the way security is administered, such as moving from physical controls including locked racks and cameras, to logical controls including encryption and anti-malware technology, and improved monitoring and auditing.

In these cases, migrating to the cloud means more of the work and investments required to maintain a secure and compliant environment becomes the responsibility of the service provider. This will require continued transparency and regulations harmony to support a trustworthy cloud ecosystem.

Considerations for selecting cloud service providers

Microsoft's stringent security, privacy, and compliance controls help ensure customers can have confidence and trust in the cloud services we provide. As customers evaluate options for cloud services, it is important that the ability of a service provider to operate a protected, trusted environment be included in the selection criteria.

The following checklist can help assess the security, privacy, and compliance capabilities and requirements of a potential service provider:

- Require that the provider has attained third-party certifications and attestations.
- Understand the value of the data that you are considering putting in the cloud and the obligations that come with the data.
- Ensure a clear understanding of security and compliance roles, and responsibilities for delivered services.
- Understand the specific regional and industry compliance obligations that must be met, and the vendor's ability to accommodate changing security and compliance requirements as they happen around the world.
- Ensure data and services can be brought back in-house if necessary.
- Require transparency in security policies and operations.

What Microsoft's cloud security approach means for you

Adopting Microsoft cloud services provides many security and compliance benefits, including:

- Our investments in security technologies and procedures help protect information from unauthorized access, use, or disclosure.
- With the increasing sophistication and volume of attacks, our economies-of-scale- and risk-based controls help us to offer better protection to customers.
- Additionally, our compliance framework, certifications, and attestations can support you in designing a program to meet your compliance needs.
- Most important, these capabilities allow you to trust the cloud services we provide.

Microsoft has extensive experience operating a cloud services infrastructure since 1995. As Microsoft's cloud services portfolio and infrastructure continues to grow we are making thoughtful investments to answer customer needs for greater availability, improved performance, increased security, and lower costs.

Contributors:

Pete Boden

Monica Drake

Mark Estberg

Jeff Fellinge

For more information, please visit www.microsoft.com/datacenters