Microsoft

EXECUTIVE STRATEGY BRIEF

Securing the Cloud Infrastructure

A DAY IN THE MICROSOFT CLOUD

Cloud

Resources

Securing the Cloud Infrastructure

Microsoft recognizes that trust is necessary for the cloud to reach its full potential. Microsoft is committed to giving customers the information they need to have confidence in Microsoft as a cloud provider. Although the cloud can be abstract, our security policies and practices are not. They are based on industry best practices and years of experience.

This strategy brief discusses the challenges of providing a trustworthy infrastructure for cloud services, reviews Microsoft's risk-based information security and privacy controls, and describes the compliance framework we follow to ensure our data centers and other infrastructure elements meet our commitments and help customers meet their security and related compliance needs.

Cloud Security Challenges

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

All cloud customers and providers face these challenges and Microsoft has been meeting them for more than 24 years:

Growing Interdependence – Organizations, whether cloud providers or cloud consumers, and their customers become interdependent on each other through use of the cloud. With these interdependencies come mutual expectations that cloud services be secure and available. Microsoft provides a trustworthy infrastructure, a base upon which public and private sector entities and their partners can build a trustworthy experience for their employees, customers and partners. Microsoft actively encourages these groups as well as the development community at large to adopt processes to manage security and reliability risk.

Complex Global Compliance Requirements – Regulatory, statutory, and industry compliance is a highly complex area because worldwide each region maintains its own requirements that govern the provisioning and use of online services. Microsoft must be able to comply with myriad complex obligations because it has data centers in many countries and offers online services to a global customer base. Microsoft has implemented a compliance framework to more easily manage and communicate its various compliance obligations and capabilities without creating undue burden on its business.

Dynamic Hosting Environment – Keeping pace with new technologies and anticipating future needs is essential to running an effective security program. The latest wave of change has already begun with the rapid move to virtualization and a growing adoption of Microsoft's cloud services strategy, which combines the power and capabilities of computers, mobile devices, online services, and enterprise software. The advent of cloud platforms enables custom applications to be developed by third-parties and hosted in the Microsoft cloud. Microsoft maintains strong internal partnerships among security, product, and service delivery teams to provide a trustworthy Microsoft cloud environment that can robustly deliver service while these changes occur.

Growing Sophistication of Threats – While domain squatting, man-in-the-middle and other common attacks still occur, more sophisticated malicious attempts aimed at obtaining identities or blocking access to sensitive business data have emerged, along with a more organized underground market for stolen information. Microsoft works closely with law enforcement, industry partners and peers, and research groups to understand and respond to this evolving threat landscape. Additionally, the long-standing Microsoft Security Development Lifecycle introduces security and privacy early and throughout the development process.

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.

Information Security Management System

The Microsoft Information Security Management System (ISMS) guides how we make risk-informed decisions. Security is part of the Microsoft culture and the ISMS is how we drive it 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 controls are being met while satisfying regulatory requirements.

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

- The Microsoft Security Policy suite which 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 online services.
- The control activities represent the operational work that the operations teams perform. Each control activity has an owner and maps to both the policy suite and the requirements.
- Audits ensure that the control activities that are being performed 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.

Comprehensive Compliance Framework

The Microsoft online services environment must meet numerous government-mandated and industry-specific security requirements in addition to Microsoft's own business-driven specifications. As Microsoft's online businesses continue to grow and change

and new online services are introduced into the Microsoft cloud, additional requirements are expected that could include regional and country-specific data security standards.

The compliance framework is based on the ISO/IEC 27001:2005 approach of plan-do-check-act. 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 27001:2005 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 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 our services satisfy their compliance needs. We are committed to providing our customers detailed information about our cloud services to help them make informed assessments.

Control 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 27001:2005 standard along with specific industry obligations, such as the Payment Card Industry Data Security Standard and the FISMA NIST SP 800-53 standard.

The control framework maps the control activities performed by 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 across the industry, and it is an approach Microsoft takes across our online services and infrastructure. Applying controls at multiple layers involves employing protection mechanisms, developing risk mitigation strategies, and responding 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 data centers, we assess and address every part of the service stack – from the physical controls to prevent unauthorized access to equipment, to encrypting data moving over the network, to locking down the host servers and keeping

Cloud Infrastructure Certifications and Attestations (as of January 2013)	
ISO / IEC 27001:2005 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	✓
HIPAA/HITECH	✓
PCI Data Security Standard Certification	✓
FISMA Certification & Accreditation	✓
Various State, Federal, and International Privacy Laws (95/46/EC—aka EU Data Protection Directive; California SB1386; etc.)	✓

malware protection up-to-date, to ensuring applications themselves have appropriate safeguards in place. Maintaining a rich set of controls and defense-in-depth strategy ensures that if any one area should fail, there are compensating protections in other areas.

Security Incident Response

An important part of Microsoft's security capabilities includes our support and 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 in order to be ready to respond 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 other 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 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.

Security and Privacy Considerations for Selecting Online Services Providers

Microsoft's stringent security, privacy, and compliance controls helps ensure customers can have confidence and trust in the online services we provide. As customers evaluate options for online services, it is important that the ability of a service provider to ensure 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 audits, such as ISO/IEC 27001:2005
- Consider the vendor's ability to accommodate changing security and compliance requirements
- Understand the specific regional and industry compliance obligations that must be met
- Ensure a clear understanding of security and compliance roles and responsibilities for delivered services
- Ensure data and services can be brought back in-house if necessary
- Require transparency in security policies and operations

Microsoft has extensive experience operating a cloud services' infrastructure, with a history of innovation, operational excellence and industry leadership. As Microsoft's cloud services portfolio and infrastructure continues to grow, and with new services and applications launching on a rapid basis, the Global Foundation Services team is making thoughtful investments to answer our customer's needs for greater availability, improved performance, increased security, and lower costs.

For more information, please visit www.globalfoundationservices.com

A DAY IN THE MICROSOFT CLOUD