Securing Microsoft's Cloud Infrastructure

This paper introduces the reader to the Online Services Security and Compliance team, a part of the Global Foundation Services division who manages security for the Microsoft cloud infrastructure. Readers will gain an understanding of what cloud computing at Microsoft means today and how the company delivers a trustworthy cloud computing infrastructure.

Published: May 2009



Table of Contents

Executive Summary	
Cloud Computing Security Challenges	4
How Microsoft Handles These Challenges	5
What Is the Microsoft Cloud Computing Environment?	6
Online Services Security and Compliance Team	6
Trustworthy Computing at Microsoft	7
Privacy	8
Security	9
Information Security Program	9
Risk Management Processes	
Business Continuity Management	
Security Incident Management	
Global Criminal Compliance	
Operational Compliance	14
Taking a Defense-in-Depth Approach	
Physical Security	
Network Security	
Data Security	
Identity and Access Management	
Application Security	
Host Security Auditing and Reporting	20
Conclusion	22
Additional Resources	23

Executive Summary

Recent research on the emerging definitions of "Cloud," "cloud computing," and "cloud environment" has attempted to identify what customers expect from cloud providers and to find ways to categorize what such providers say they will offer. The idea that purchasing services from a cloud environment may allow technology business decision makers (BDMs) to save money and allow companies to focus on their core business is an enticing proposition in the current economic climate. Many analysts view the emerging possibilities for pricing and for delivering services online as disruptive to market conditions. These market studies and the ensuing dialogue among prospective customers and service providers show certain themes have emerged as potential barriers to rapid adoption of cloud services. Concerns about security, privacy, reliability, and operational control top the list of potential barriers. Microsoft recognizes that BDMs have many questions about these issues including a need to know how they are addressed in the cloud computing environment at Microsoft and the implications to their own risk and operations decisions.

This paper shows how the coordinated and strategic application of people, processes, technologies, and experience results in continuous improvements to the security of the Microsoft cloud environment. The Online Services Security and Compliance (OSSC) team within the Global Foundation Services (GFS) division builds on the same security principles and processes Microsoft has developed through years of experience managing security risks in traditional development and operating environments.

Cloud Computing Security Challenges

The information technology industry faces the challenges that accompany the opportunities of cloud computing. For over 15 years, Microsoft has been addressing the following online service delivery challenges:

- Emerging cloud business models create a growing interdependence amongst public and private sector entities
 and the people they serve Such organizations and their customers will become more interdependent on each
 other through use of the cloud. With these new dependencies come mutual expectations that platform services
 and hosted applications 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 users.
 Microsoft actively works with these groups and the development community at large to encourage adoption of
 security-centric risk management processes.
- Acceleration of adoption of cloud services, including the continuing evolution of technologies and business
 models, creates a dynamic hosting environment, which is of itself a security challenge Keeping pace with
 growth 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 Softwareplus-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. Through the online services Information Security Program described
 in more detail later in this paper, Microsoft maintains strong internal partnerships among security, product, and
 service delivery teams to provide a trustworthy Microsoft cloud environment while these changes occur.
- Attempts to infiltrate or disrupt online service offerings grow more sophisticated as more commerce and business occurs in this venue – While pranksters still seek attention through a variety of techniques including domain squatting and man-in-the-middle attacks, 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 Microsoft Security Development Lifecycle, described later in this paper, introduces security and privacy early and throughout the development process.
- Complex compliance requirements must be addressed as new and existing services are delivered globally Regulatory, statutory, and industry (referred to simply as "regulatory" for the remainder of this paper) compliance is a highly complex area because worldwide each country can and does pass their own laws that can govern the provision and use of online environments. Microsoft must be able to comply with a myriad of regulatory obligations because it has data centers in a number of countries and offers online services to a global customer base. In addition, many industries impose requirements. Microsoft has implemented a compliance framework (described later in this paper) whereby it efficiently manages its various compliance obligations without creating undue burden on the business.

How Microsoft Handles These Challenges

Since the launch of MSN[®] in 1994, Microsoft has been building and running online services. The GFS division manages the cloud infrastructure and platform for Microsoft online services, including ensuring availability for hundreds of millions of customers around the world 24 hours a day, every day. More than 200 of the company's online services and Web portals are hosted on this cloud infrastructure, including such familiar consumer-oriented services as Windows Live[™] Hotmail[®] and Live Search, and business-oriented services such as Microsoft Dynamics[®] CRM Online and Microsoft Business Productivity Online Standard Suite from Microsoft Online Services.

Whether a consumer's personal information is stored on their own computer or in an online setting, or whether an organization's mission-critical data is stored in-house or is on a hosted server and sent across the Internet, Microsoft recognizes that all of these environments must provide a Trustworthy Computing experience. As a company, Microsoft is in a unique position to provide both guidance and technology solutions that can offer a safer online experience. To help customers avoid financial loss and other consequences of opportunistic and targeted online attacks, and as part of a steadfast commitment to Trustworthy Computing, Microsoft ensures that the people, processes, and technologies the company employs provide more secure and privacy-enhancing experiences, products, and services.

Microsoft provides a trustworthy cloud through focus on three areas:

- Utilizing a risk-based information security program that assesses and prioritizes security and operational threats to the business
- Maintaining and updating a detailed set of security controls that mitigate risk
- Operating a compliance framework that ensures controls are designed appropriately and are operating effectively

This paper describes how Microsoft protects customer data and business operations through a comprehensive Information Security Program and a mature methodology for policy and compliance management, frequent internal and external evaluation of practices and capabilities, and robust security controls across all service layers. These processes and mechanisms are how Microsoft complies with industry standards and sustains regulatory compliance with all applicable laws, directives, statutes, and regulations while delivering services online to a global customer base.

While privacy policies are mentioned in this paper, the intent is not to provide an in-depth discussion of privacy policies nor will it be a privacy operations guide. Information about how Microsoft addresses privacy needs can be found at the <u>Microsoft Trustworthy Computing Privacy</u> page.

What Is the Microsoft Cloud Computing Environment?

The Microsoft cloud computing environment is the physical and logical infrastructure as well as the hosted applications and platform services. GFS provides the physical and logical cloud infrastructure at Microsoft including many platform services. The physical infrastructure includes the data center facilities themselves, as well as the hardware and components that support the services and networks. At Microsoft, the logical infrastructure consists of operating system instances, routed networks, and unstructured data storage, whether running on virtual or physical objects. Platform services include compute runtimes (such as Internet Information Services, the .NET Framework, Microsoft® SQL Server®), identity and directory stores (such as Active Directory® and Windows Live ID), name services (DNS), and other advanced functions consumed by online services. Microsoft cloud platform services, such as infrastructure services, may be virtualized or actual.

Online applications running in the Microsoft cloud include simple and complex products designed for a range of customers. These online services, and the corresponding security and privacy requirements, can be broadly grouped as offerings for:

- Consumer and Small Business Services Examples include Windows Live Messenger, Windows Live Hotmail, Live Search, Xbox LIVE[®], and Microsoft Office Live.
- Enterprise Services Such as Microsoft Dynamics CRM Online and the Microsoft Business Productivity Online Standard Suite, including Exchange Online, SharePoint[®] Online, and Office Live Meeting.
- Third-party hosted services Includes Web-based applications and solutions that are developed and operated by third parties using platform services provided through the Microsoft cloud computing environment.

Online Services Security and Compliance Team



The OSSC team within GFS is responsible for the Microsoft cloud infrastructure Information Security Program, including policies and programs used to manage online security risks. The mission of OSSC is to enable trustworthy online services that create a competitive advantage for Microsoft and its customers. Placing this function at the cloud infrastructure layer allows all Microsoft cloud services to take advantage of economies of scale and reduced complexity through use of shared security solutions. Having this standard approach also enables each of the Microsoft service teams to focus on the unique security needs of their customers.

The OSSC team drives the effort to provide a trustworthy experience in the Microsoft cloud through the Microsoft Information Security Program using a risk-based operating model and a defense-in-depth approach to controls. This includes regular risk management reviews, development, and maintenance of a security control framework, and ongoing efforts to ensure compliance in activities ranging from data center development to responding to requests from law enforcement entities around the world. The team applies best practice processes, including a variety of internal and external reviews, throughout the lifecycle of online services and each element in the infrastructure. Close working relationships with other Microsoft teams result in a comprehensive approach to securing applications in the Microsoft cloud.

Operating a global cloud infrastructure across many businesses comes with the need to comply with compliance obligations and to withstand the scrutiny of outside auditors. Auditable requirements come from government and industry mandates, internal policies, and industry best practices. The OSSC program ensures that compliance expectations are continuously evaluated and incorporated. As a result of the Information Security Program, Microsoft is able to obtain key certifications such as International Organization for Standardization / International Society of Electrochemistry 27001:2005 (ISO/IEC 27001:2005) and Statement of Auditing Standard (SAS) 70 Type I and Type II attestations, and to more efficiently pass regular audits from independent third parties.

Trustworthy Computing at Microsoft

The core driver to creating an effective security program is having a culture that is aware of and highly values security. Microsoft recognizes that such a culture must be mandated and supported by company leaders. The Microsoft leadership team has long been committed to making the proper investments and incentives to drive secure behavior. In 2002, the company formed the Trustworthy Computing initiative with Bill Gates committing Microsoft to fundamentally changing its mission and strategy in key areas. Today, Trustworthy Computing is a core corporate value at Microsoft, guiding nearly everything the company does. At the foundation of this initiative are these four pillars: Privacy, Security, Reliability, and Business Practices. For more information on Trustworthy Computing, see the <u>Microsoft Trustworthy</u> <u>Computing</u> page.

Microsoft understands that success in the rapidly changing business of online services is dependent upon the security and privacy of customers' data and the availability and the resiliency of the services Microsoft offers. Microsoft diligently designs and tests applications and infrastructure to internationally recognized standards in order to demonstrate these capabilities and compliance with laws and with internal security and privacy policies. As a result, Microsoft customers benefit from more focused testing and monitoring, automated patch delivery, cost-saving economies of scale, and ongoing security improvements.

Privacy

Microsoft endeavors to protect the privacy and security of customers, including complying with all applicable privacy laws, and following the stringent privacy practices detailed in Microsoft's Privacy Statements.

To create a trusted environment for customers, Microsoft develops software, services, and processes with privacy in mind. Microsoft teams are vigilant in maintaining compliance with global privacy laws and the company's privacy practices are derived, in part, from privacy laws from around the world. Microsoft follows the lead of these privacy laws, and applies those standards globally.

Microsoft is committed to protecting the security of personal information. The online service delivery teams use a variety of security technologies and procedures to help protect personal information from unauthorized access, use, or disclosure. Microsoft software development teams apply the PD3+C principles, defined in the Security Development Lifecycle (SDL), throughout the company's development and operational practices:

- **Privacy by Design** Microsoft uses this principle in multiple ways during the development, release, and maintenance of applications to ensure the data collected from customers is for a particular purpose and that the customer is given appropriate notice in order to enable informed decision-making. When data to be collected is classified as highly sensitive, additional security measures such as encrypting while in transit, at rest, or both, may be taken.
- **Privacy by Default** Microsoft offerings ask customers for permission before collecting or transferring sensitive data. Once authorized, such data is protected by means such as access control lists (ACLs) in combination with identity authentication mechanisms.
- **Privacy in Deployment** Microsoft discloses privacy mechanisms to organizational customers as appropriate to allow them to establish appropriate privacy and security policies for their users.
- **Communications** Microsoft actively engages the public through publication of privacy policies, white papers, and other documentations pertaining to privacy.

For more information about Microsoft's commitment to privacy, see the Microsoft Trustworthy Computing Privacy page.

Security

Microsoft has continued to adapt the company's cloud infrastructure to take advantage of emerging technologies, such as virtualization. These advances result in a decoupling of information assets from a common physical infrastructure for many types of customer objects. Combine this with the fact that the software development process for applications hosted online is often more agile with more frequent releases, and the result is that information security risk management has had to adapt in order to deliver a Trustworthy Computing experience.

The following sections of this paper provide an in-depth look at how the Microsoft OSSC team applies security fundamentals and the efforts made across the company to manage risks in the Microsoft cloud infrastructure. It also introduces what a defense-in-depth approach to online service security means and how the cloud computing environment results in new approaches to security measures.

Information Security Program

Microsoft's online Information Security Program defines how OSSC operates. The program has been independently certified by British Standards Institute (BSI) Management Systems America as being compliant with ISO/IEC 27001:2005. To view the ISO/IEC 27001:2005 certificates, see the <u>Certificate/Client Directory Search Results</u> page.

The Information Security Program organizes security requirements into three top-level domains: Administrative, Technical, and Physical. The criteria in these domains represent the basis from which risk is managed. Starting with the safeguards and controls identified in the domains and their subcategories, the Information Security Program follows the ISO/IEC27001:2005 framework of "Plan, Do, Check, Act."



OSSC further defines the four steps in the traditional Plan, Do, Check, Act structure of an ISO information security program as follows:

- Plan
 - a. **Risk-based decision making** Driving the prioritization of key activities and allocation of resources, OSSC creates a security action plan based on risk assessments. The organizational and individual objectives captured in this plan address updates for policies, operating standards, and security controls in GFS and many product groups.
 - b. **Document requirements** OSSC sets clear expectations that set the stage for obtaining third-party attestations and certifications through a documented control framework. This framework provides requirements in a clear, consistent, and concise manner.
- Do
- a. **Implement appropriate controls** Controls based on the security action plan are put in place by operation, product, and service delivery teams.
- b. **Operate controls** OSSC implements and operates many controls directly, such as those used to ensure global criminal compliance, to manage threat to the infrastructure, and to physically secure data centers. Other measures are enacted and maintained by operation, product, and service delivery teams.
- Check
 - a. **Measure and improve** OSSC evaluates control activity on a continuous basis. Additional controls may be added or existing ones modified to ensure the objectives detailed in the Information Security Policy and control framework are met.
- Act
 - a. Validate program effectiveness Both internal teams and external auditors periodically review the Information Security Program as part of ongoing efforts to validate program effectiveness.
 - b. Adjust to remain relevant OSSC evaluates the Information Security Program and its control framework against applicable legislative, regulatory, business, and industry requirements and standards to identify areas for improvement and to validate objectives are being met. As a result, Microsoft technology and business plans are updated to address the impact of operational changes.

No security program is complete without addressing the need to train staff. Microsoft produces and delivers security training to ensure that all groups involved in creating, deploying, operating, and supporting online services hosted on the cloud infrastructure understand their responsibilities as they relate to the Information Security Policy for Online Services at Microsoft.

This training program teaches key guiding principles that should be applied when considering each layer of Microsoft's defense-in-depth approach to securing online services. Microsoft also encourages business customers and third-party software developers to apply these same principles when developing applications and delivering services using Microsoft's cloud infrastructure.

Risk Management Processes

The analysis and resolution of security vulnerabilities in interdependent online systems is more complex and can be more time intensive than those found in traditional IT systems. Risk management and corresponding reviews must be adapted to this dynamic environment. Microsoft uses mature processes based on long-term experience delivering services on the Web for managing these new risks.

OSSC staff works in partnership with operations teams and business owners in many product and service delivery groups within Microsoft to manage these risks. The Information Security Program establishes the standard processes and documentation requirements for performing continuous risk-based decision making.

Through the Security Risk Management Program (SRMP), risk assessments occur at a variety of levels and inform prioritization in areas such as product release plans, policy maintenance, and resource allocation. Each year, a comprehensive assessment of threats to the Microsoft cloud infrastructure occurs that leads to additional reviews throughout the year. This ongoing work focuses on those threats that could be highly disruptive. Through this process, Microsoft prioritizes and guides development of security controls and related activities. The SRMP methodology evaluates control effectiveness against threats by:

- Identifying threats and vulnerabilities to the environment
- Calculating risk
- Reporting risks across the Microsoft cloud environment
- Addressing risks based on impact assessment and the associated business case
- Testing remediation effectiveness and residual risk
- Managing risks on an ongoing basis

Business Continuity Management

Many organizations considering use of cloud applications are asking questions about service availability and resiliency. Hosting applications and storing data in a cloud environment offers new service availability and resiliency options as well as data backup and recovery options. The Microsoft Business Continuity Program uses industry best practices to create and adapt capabilities in this area to address new applications as they become available in the Microsoft cloud environment.

Microsoft uses an ongoing management and governance process to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services. Knowing all the resources—the people, equipment, and systems—needed to execute a task or perform a process is essential to creating a relevant plan for when disaster strikes. The failure to review, maintain, and test the plan is one of the biggest risks associated with having a disastrous loss occur, therefore the program does more than simply record recovery procedures. Microsoft uses the Business Continuity Management Plan Development Lifecycle to create and maintain disaster recovery plans through application of six phases, as shown in the following illustration:



Microsoft addresses service and data recovery after having completed a dependency analysis by identifying two objectives in relation to the recovery of the assets:

- **Recovery Time Objective (RTO)** The maximum amount of time that the loss of a critical process, function, or resource can be withstood before a serious adverse business impact would result.
- **Recovery Point Objective (RPO)** The maximum amount of data loss that can be sustained during an event, usually thought of in terms related to the time between the last data backup and when the outage occurred.

Because the process of identifying and classifying assets is ongoing as part of managing risks to the Microsoft cloud computing infrastructure, the disaster recovery plan means these objectives can be more readily applied to evaluating whether or not to implement recovery strategies during a disaster situation. Microsoft further validates these strategies through conducting exercises that involve rehearsal, testing, training, and maintenance.

Security Incident Management

The security controls and risk management processes Microsoft has in place to secure the cloud infrastructure reduce the risk of security incidents, and yet it would be naïve to think future malicious attacks will not happen. The Security Incident Management (SIM) team within OSSC responds to these issues when they occur and operates 24 hours a day, every day. SIM's mission is to quickly and accurately assess and mitigate computer security incidents involving Microsoft's Online Services, while clearly communicating relevant information to senior management and other concerned parties within Microsoft.

There are six phases to the SIM incident response process:

- **Preparation** SIM staff undergo ongoing training in order to be ready to respond 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. How containment occurs depends 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.
- **Lessons learned** After resolution of the security incident, SIM convenes a joint meeting with all involved personnel to evaluate what happened and to record lessons learned during the incident response process.

SIM is able to detect issues early and to mitigate disruption of services thanks to cross-team alliances. For example, SIM is closely aligned with operations teams, including the Microsoft Security Response Center (for more information, see the <u>Microsoft Security Response Center</u> page). This relationship enables SIM to quickly gain a holistic operational view of an incident as it happens. SIM responders also consult with asset owners to determine severity of the incident based on a variety of factors including potential or additional disruptions to service and risk of reputational damage.

Global Criminal Compliance

OSSC's Global Criminal Compliance (GCC) program is involved in setting policy and providing training on Microsoft's response process. GCC also responds to valid legal requests for information. GCC has legal agents available in many countries to validate and, if necessary, translate the request. One reason that GCC is considered a "best response program" by many international authorities is that GCC provides a law enforcement portal that offers guidance in multiple languages to authenticated law enforcement personnel about how to submit a legal request to Microsoft.

GCC's training mission includes providing training to law enforcement professionals. GCC also provides training to all levels of personnel at Microsoft about responsibilities for data retention and privacy. Internal training and policy work continues to evolve as Microsoft adds data centers in international locations, thereby expanding the scope of

international regulatory requirements. GCC plays a crucial role in understanding and implementing processes that take into account various international laws and how they apply to consumer or business customers who rely on Microsoft online services.

Operational Compliance

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 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 Operational Compliance team works across operation, product, and service delivery teams and with internal and external auditors to ensure Microsoft is in compliance with relevant standards and regulatory obligations. The following list presents an overview of some of the audits and assessments that the Microsoft cloud environment undergoes on a regular basis:

- **Payment Card Industry Data Security Standard** Requires annual review and validation of security controls related to credit card transactions.
- Media Ratings Council Relates to the integrity of advertising system data generation and processing.
- Sarbanes-Oxley Selected systems are audited annually to validate compliance with key processes related to financial reporting integrity.
- Health Insurance Portability and Accountability Act Specifies privacy, security, and disaster recovery guidelines for electronic storage of health records.
- Internal audit and privacy assessments Assessments occur throughout a given year.

Meeting all these audit obligations became a considerable challenge at Microsoft. Upon studying the requirements, Microsoft determined that many of the audits and assessments required evaluation of the same operational controls and processes. Recognizing the significant opportunity to eliminate redundant efforts, streamline processes, and proactively manage compliance expectations in a more comprehensive manner, OSSC developed a comprehensive compliance framework. This framework and associated processes are based on a five-step methodology represented in the following illustration:



- Identify and integrate requirements Scope and applicable controls are defined. Standard Operating Procedures (SOP) and process documents are gathered and reviewed.
- Assess and remediate gaps Gaps in process or technology controls are identified and remediated.
- Test effectiveness and assess risk Effectiveness of controls is measured and reported.
- Attain certifications and attestations Engagement with third-party certification authorities and auditors occurs.
- Improve and optimize If non-compliance is found, the root cause is documented and assessed further. Such findings are tracked until fully remediated. This phase also involves continuing to optimize controls across security domains to generate efficiencies in passing future audit and certification reviews.

One of the successes of having implemented this program is that Microsoft's cloud infrastructure has achieved both SAS 70 Type I and Type II attestations and ISO/IEC 27001:2005 certification. This achievement demonstrates Microsoft's commitment to delivering a trustworthy cloud computing infrastructure because having:

- The ISO/IEC 27001:2005 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard, and
- The SAS 70 attestations illustrate Microsoft's willingness to open up internal security programs to outside scrutiny.

Taking a Defense-in-Depth Approach

Having a defense-in-depth approach is a fundamental element in how Microsoft provides a trustworthy cloud infrastructure. Applying controls at multiple layers involves employing protection mechanisms, developing risk mitigation strategies, and being capable of responding 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. The advent of cloud computing does not change this principle—that the strength of the controls derives from the sensitivity of the asset—or how essential it is to managing security risks. The fact that in a cloud computing environment most assets can be virtualized results in shifts in the analysis of risk and how to apply security controls to the traditional defense-in-depth layers (physical, network, data, identity access, access authorization and authentication, and host).

Online services, including the infrastructure and platform services provided by GFS, take advantage of virtualization. As a result, customers using services hosted on the Microsoft cloud may have assets that can no longer be easily associated with a physical presence. Data may be stored virtually and distributed across many locations. This basic fact means identifying security controls and determining how to use them to implement a layered approach to protecting assets must evolve. Physical and network security measures must, of course, still be taken. However, the focal point of risk management shifts closer to the object level, closer to the elements in use in the cloud environment: for example, the static or dynamic data storage containers, the virtual machine objects, the run-time environments in which computations occur.

The various controls in place make use of many traditional physical and network security methods and devices to ensure that the entity, be it a person wanting access to a data center building or a compute process requesting access to customer data stored dynamically in the Microsoft cloud environment, is authentic and authorized for the requested access. Measures are also in place to ensure the servers and operating system instances running on the Microsoft cloud infrastructure are hardened against attacks.

This section provides an overview of some of the processes and controls Microsoft uses to address security of data centers, network hardware and communications, and services hosts.

Physical Security

Use of technical systems to automate authorization for access and authentication for certain safeguards is one way that physical security has changed as security technology advances. The shift from using traditional enterprise applications, deployed on computing hardware and software physically located within the business, to utilization of Software-as-a-Service and Software-plus-Services is another. These changes necessitate additional adjustments to the way organizations ensure their assets are secured.

OSSC manages the physical security of all of Microsoft's data centers, which is critical to keeping the facilities operational as well as to protecting customer data. Established, precise procedures in security design and operations are

utilized for each facility. Microsoft ensures the establishment of outer and inner perimeters with increasing controls through each perimeter layer.

The security system applies the combined use of technology solutions including cameras, biometrics, card readers, and alarms with traditional security measures such as locks and keys. Operational controls are incorporated to facilitate automated monitoring and early notification if a breach or problem occurs, and enables accountability through the provision of auditable documentation of the data center's physical security program. The following list provides additional examples of how Microsoft applies controls to physical security:

- Restricting access to data center personnel Microsoft provides security requirements upon which data center employees and contractors are reviewed. In addition to contractual stipulations about site staff, a further layer of security within the data center is applied to personnel that operate the facility. Access is restricted by applying a least privilege policy, so that only essential personnel are authorized to manage customers' applications and services.
- Addressing high business impact data requirements Microsoft has developed more stringent minimum requirements for assets categorized as being highly sensitive than for those of low or moderate sensitivity within the data centers used to provide online services. Standard security protocols regarding identification, access tokens, and logging and surveillance of site entry clearly state what type of authentication is needed. In the case of access to highly sensitive assets, multifactor authentication is required.
- Centralizing physical asset access management As Microsoft continues to expand the number of data centers used to provide online services, a tool was developed to manage access control to physical assets, which also provides auditable records through the centralization of workflow for the process of requesting, approving, and provisioning access to data centers. This tool operates using the principle of providing the least access needed and incorporates workflow for gaining approvals from multiple authorization parties. It is configurable to site conditions and enables more efficient access to history details for reporting and compliance with audits.

Network Security

Microsoft applies many layers of security as appropriate to data center devices and network connections. For example, security controls are used on both the control and management planes. Specialized hardware such as load balancers, firewalls, and intrusion prevention devices, is in place to manage volume-based denial of service (DoS) attacks. The network management teams apply tiered access control lists (ACLs) to segmented virtual local area networks (VLANs) and applications as needed. Through network hardware, Microsoft uses application gateway functions to perform deep packet inspection and take actions such as sending alerts based on—or blocking—suspicious network traffic.

A globally redundant internal and external DNS infrastructure is in place for the Microsoft cloud environment. Redundancy provides for fault tolerance and is achieved through clustering of DNS servers. Additional controls mitigate distributed denial of service (DDoS) and cache poisoning or pollution attacks. For example, ACLs within DNS servers and DNS zones restrict write access to DNS records to authorized personnel. New security features, such as randomization of query identifiers, from the latest secure DNS software is used on all DNS servers. DNS clusters are continuously monitored for unauthorized software and DNS zone configuration changes as well as for other disruptive service events. DNS is part of the globally connected Internet and requires participation of many organizations to provide this service. Microsoft participates in many of these such as the DNS Operations Analysis and Research Consortium (DNS-OARC), which is comprised of DNS experts worldwide.

Data Security

Microsoft classifies assets to determine the strength of security controls to apply. The categories take into account the relative potential for financial and reputational damage should the asset be involved in a security incident. Once classified, a defense-in-depth approach is taken to determine what protections are needed. For example, data assets falling into the moderate impact category are subject to encryption requirements when they are residing on removable media or when they are involved in external network transfers. High impact data, in addition to those requirements, is subject to encryption requirements for storage and for internal system and network transfers as well.

All Microsoft products must meet the SDL cryptographic standards, which list the acceptable and unacceptable cryptographic algorithms. For example, keys longer than 128-bits are required for symmetric encryption. When using asymmetric algorithms, keys of 2,048 bits or longer are required.

Identity and Access Management

Microsoft uses a need-to-know and least-privilege model to manage access to assets. Where feasible, role-based access controls are used to allocate logical access to specific job functions or areas of responsibility, rather than to an individual. These policies dictate that access that has not been explicitly granted by the asset owner based upon an identified business requirement is denied by default.

Individuals who are authorized to access any asset must use the appropriate measures to gain access. Highly sensitive assets require multifactor authentication, including such measures as password, hardware tokens, smart cards, or biometrics. Reconciliation of user accounts against authorizations for use happens on an ongoing basis to ensure that use of an asset is appropriate and needed to complete a given activity. Accounts no longer needing access to a given asset are disabled.

Application Security

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, and is not a replacement for software development methodologies such as waterfall or Agile. 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.

Senior leadership within Microsoft continues to support the mandate that SDL be applied during the development process of Microsoft products, including delivery of online services. OSSC plays a pivotal role in ensuring the SDL is and continues to be applied to the creation of applications to be hosted on the Microsoft cloud infrastructure.

The SDL process is represented in the following illustration:



Starting with the requirements phase, the SDL process includes a number of specific activities when considered with development of applications to be hosted in the Microsoft cloud in mind:

- Requirements The primary objective in this phase is to identify key security objectives and otherwise maximize software security while minimizing disruption to customer usability, plans, and schedules. This activity may include an operational discussion when dealing with hosted applications that focuses on defining how the service will utilize network connections and message transports.
- **Design** Critical security steps in this phase include documenting the potential attack surface and conducting threat modeling. As with the requirements phase, environmental criteria may be identified when going through this process for a hosted application.
- Implementation Coding and testing occur in this phase. Preventing the creation of code with security vulnerabilities and taking steps to remove such issues, if present, are the key practices during implementation.
- Verification The beta phase is when new applications are considered functionally complete. During this phase, close attention is paid to determining what security risks are present when the application is deployed in a real-world scenario and what steps can be taken to eliminate or mitigate the security risks.
- **Release** The Final Security Review (FSR) happens during this phase. If needed, an Operational Security Review (OSR) also occurs before the new application can be released into Microsoft's cloud environment.
- Response For Microsoft's cloud environment, the SIM team takes the lead in responding to security incidents and works closely with product, service delivery teams, and members of the Microsoft Security Response Center to triage, research, and remediate reported incidents.

For more information about SDL, see <u>The Microsoft Security Development Lifecycle (SDL)</u> page.

OSSC manages the FSR process, a mandatory SDL review, for Microsoft online services to ensure appropriate security requirements have been met before new applications are deployed to the Microsoft cloud infrastructure. The FSR is a

review of a team's adherence to SDL throughout the development process. During the FSR, OSSC manages the following tasks:

- **Product Team Coordination** Questionnaires and other documentation must be completed by the product development team. That information is used by OSSC to ensure that SDL has been applied correctly during development.
- Threat Models Review Microsoft considers threat models to be critical to developing secure software. OSSC analyzes the threat models produced by product teams to verify they are complete and current. Validation that mitigating controls have been implemented to address all identified risks also takes place as part of this review.
- Security Bugs Review All bugs identified during design, development, and testing are reviewed to ensure that bugs that will impact the security or privacy of customers' data are addressed.
- Tools Use Validation Microsoft development and test teams use software security tools and documented code
 patterns and practices as part of the development process. This can greatly enhance software security through
 elimination of common vulnerabilities. OSSC ensures that product teams have correctly and appropriately made
 use of the tools, documented code, and patterns and practices available to them.

In addition to managing the FSR process, OSSC also manages a process called the Operational Security Review (OSR). The OSR consists of reviewing associated network communications, platform, system configuration, and monitoring capabilities against established security standards and baselines. The OSR process ensures appropriate security controls are part of the operational plans before permission is granted to deploy into the cloud infrastructure.

Host Security Auditing and Reporting

Growing environmental size and complexity must be managed in order to deliver reliable, well-managed, secure, and patched services.

Daily scanning of the infrastructure assets provides a current view of host system vulnerabilities and allows OSSC to work in partnership with product and service delivery groups to manage the associated risks without causing undue interruptions to Microsoft's online services operations.

Penetration testing performed by internal and external parties provides important insight into the effectiveness of security controls for the Microsoft cloud infrastructure. The outcome of these reviews and ongoing evaluation of the resulting controls are used in subsequent scanning, monitoring, and risk remediation efforts.

Automated deployment of standard hardened operating system images along with active use of host policy controls such as Group Policy allows Microsoft to control the addition of servers to the Microsoft cloud infrastructure. Once deployed, the Microsoft operational review processes and patch management program provide ongoing mitigation of security risks to the host systems.

OSSC relies on auditing and reporting as a detective control, and to provide insight and forensic evidence when incidents occur. Logs generated by perimeter firewalls, intrusion prevention systems, and network devices are collected centrally via the SYSLOG protocol and stored as files. The individual event records contained within these files are parsed and uploaded to a centralized SQL Server database. The uploaded records are analyzed using automated tools for patterns that may be indicative of anomalous behavior or malicious activity within the monitored environment and will trigger an alert to the SIM team when an investigation of the activity may be warranted. After each log file is processed, a cryptographic hash is generated on the file and stored along with relevant file statistics in the same database. Once hashed, the individual log files are compressed and stored on redundant file archive servers. The hash values allow auditors and investigators to validate the integrity of the original log files stored in the archive should those files be needed for additional analysis.

The audit logs of critical servers within the Microsoft cloud infrastructure, such as domain controllers, security servers, and servers containing sensitive information are collected near real-time via the Microsoft System Center Operations Manager 2007 Audit Collection Services (ACS) feature and stored in a SQL Server database. Due to the large amount of data collected for these environments, important and relevant events (referred to as "Events-of-Interest") are extracted and forwarded to another SQL database where OSSC uses automated tools to perform detailed analysis looking for suspicious activity. The information collected from the event logs includes user logon, security policy configuration changes, and unauthorized access to system or application files. As with the records generated by perimeter and network devices, the Events-of-Interest extracted from the audit logs are reviewed for evidence of control failure, unauthorized modification of server configuration, and other malicious activity.

In addition, customized management packs created for Microsoft Operations Manager (MOM) and Microsoft System Center Operations Manager provide real-time alerting and health monitoring. This allows for additional visibility into security violations, changes that affect system integrity, and policy infractions on individual systems. These MOM and System Center Operations Manager events are integrated into standard operational frameworks. The appropriate operations teams within Microsoft also use them to remediate less urgent issues.

Information extracted from the various log files is used for incident creation, report generation, and historical trending; all of which are used to validate the efficacy of controls in the control framework.

Conclusion

By building on the same security principles used to manage risks to Microsoft software development and operating environments, OSSC has created an online Information Security Program—one that results in continuous improvements to security for the Microsoft cloud computing environment. The coordinated and strategic application of people, processes, and technology allows Microsoft to adapt to the rapid changes happening within the cloud infrastructure and in the marketplace for online services while still maintaining Microsoft's commitment to delivering a Trustworthy Computing experience for customers.

The framework that enabled Microsoft to earn the ISO 27001:2005 accreditation and SAS Type I and Type II attestations for the Microsoft cloud infrastructure sets the stage for product and service delivery teams to more efficiently obtain additional certifications and attestations as appropriate. Security training, continuous review and management of risks, rapid response to security incidents and legal requests—having all of these elements in place—enables Microsoft to deliver on a firm commitment to Trustworthy Computing while simultaneously setting the stage for partners and customers to also reap the benefits of these mature and flexible processes.

Through this Information Security Program, Microsoft maintains a comprehensive compliance framework and a detailed set of security controls and policies to provide the reliability and privacy customers expect while complying with applicable regulatory obligations and industry standards. Microsoft's proven record of accomplishment, combined with its independently certified programs, shows the continued relevance of these programs to the continuing evolution of challenges and opportunities in the changing online services marketplace. Microsoft product teams are using these practices to establish trust and an appropriate level of transparency for new offerings as part of the Software-plus-Services strategy for agile and cost-effective development. Having a trustworthy cloud infrastructure enables Microsoft, partner, and customer teams to build more secure applications for this dynamic cloud environment.

Additional Resources

Microsoft Trustworthy Computing, home page: <u>http://www.microsoft.com/twc</u>

Microsoft Online Privacy Notice Highlights: http://www.microsoft.com/privacy

The ISO 27001:2005 certificate for the Global Foundation Services group at Microsoft: <u>http://www.bsi-global.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search-Results/?pg=1&licencenumber=IS+533913&searchkey=companyXeqXmicrosoft</u>

Microsoft Global Foundation Services, home page: http://www.globalfoundationservices.com

The Microsoft Security Development Lifecycle (SDL): <u>http://msdn.microsoft.com/en-us/security/cc448177.aspx</u>

Microsoft Security Development Lifecycle (SDL) – version 3.2, process guidance: <u>http://msdn.microsoft.com/en-us/library/cc307748.aspx</u>

Microsoft Security Response Center: <u>http://www.microsoft.com/security/msrc</u>

The Microsoft SDL Threat Modeling Tool: <u>http://msdn.microsoft.com/en-us/security/dd206731.aspx</u>

Microsoft Online Services: http://www.microsoft.com/online

Terms & Conditions

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, this document should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Hotmail, Microsoft Dynamics, MSN, SharePoint, SQL Server, Windows Live, and Xbox LIVE are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.