Security in the Business Productivity Online Standard Suite from Microsoft Online Services

White Paper

Published: June 2009

The services in the Microsoft Business Productivity Online Standard Suite from Microsoft® Online Services offer efficient, economical, and scalable communication and collaboration services for your business.

Along with reliability, continuity, and data privacy, the security of their online environment is high on the list of customer requirements. This paper describes how security has been a central principle designed into all aspects of the Business Productivity Online Standard Suite.

The Microsoft approach to continuing to safeguard its services and customer data characterizes its Risk Management Program (RMP). The RMP focuses on continuing to extend and mature into the services world the practices defined by the Microsoft Trustworthy Computing Initiative, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone.

Microsoft provides customers with confidence in the Online Services by demonstrating compliance with industry-standard practices for service operations, through regular audits and third-party certification.

For the latest information about the Business Productivity Online Standard Suite and other Microsoft Online Services, visit Microsoft Online Services.

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, it 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.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Exchange, Forefront, SharePoint, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

Executive Summary 1

Why Online Services? 2
- Why Online Services from Microsoft? 3
- The Foundation of Microsoft Online Services: Trustworthy Computing 4
  - The Trustworthy Computing Initiative 4
- Developing Secure Services: The Security Development Lifecycle 5

Building and Maintaining Trust: The Microsoft Online Services Risk Management Program 6
- Risk Management Program Objectives 6
- Risk Management Program Success Criteria 6
- Risk Management Core Disciplines 7

Security 7
- A Comprehensive, Ongoing Process 8
- Physical Security 8
  - Carrier-Class Data Centers 9
  - Worldwide Data Center Locations 9
  - Security for Data Center Personnel 9
  - Secure Network Design and Operations 9
  - Best-of-Breed Hardware 10
- Logical Security 10
  - Features of the Microsoft Online Services 10
  - The Microsoft Online Services Infrastructure 11
  - *Systems Management and Access Control* 11
  - The Microsoft Online Services Network 12
  - Protection Against Malicious Software 12
- World-Class Operations 13
  - Monitoring and Risk Reduction 14
  - Integrating Security with Operations 15
- Incorporating Risk Management Principles 16
  - Security Incident Management 17
  - Security Investigation 17

Privacy in Microsoft Online Services 18
- Data Privacy by Design 18
  - Specific Privacy Practices: Marketing and Advertising, and Testing 18
- Vendors and Partners 19
  - Vendors 19
  - Partners 19
- Access, Security, Data Integrity, and Enforcement 19
- Customer Guidance 19
- International Data Transfer 20

Service Continuity Management 21

Archiving for Messaging Continuity 21
Data Storage 21
Availability and Continuity 22
99.9-Percent Reliability 22
Avoiding Resource Constraints Through Scalability 22
Dedicated Support 22
Self-Help, Backed by Continuous Staff Support 23

Compliance 24
Standards-Driven Compliance Management 24
Microsoft Online Services Compliance Management Program 24
The Microsoft Online Services Compliance Framework 25
Compliance Assessments and Audits 26
Independent Certification 27
Demonstrating Compliance 27
Statement of Auditing Standard (SAS) 70 27
ISO 27001 27
Verizon Security Management Program – Service Provider Certification 28
Current and Future State of Online Services Third-Party Certifications 28

Further Information 29
Microsoft Online Services 29
Security and Service Continuity 29
Privacy 29
Compliance 29

Executive Summary

This paper's goal is to answer your questions about the security and reliability of the Business Productivity Online Standard Suite from Microsoft® Online Services. It describes the capabilities, technologies, and processes that build trust in the Business Productivity Online Standard Suite, providing world-class online services for your business. It examines how the considerable experience of Microsoft in building and operating enterprise software has led to the demonstrated reliability and trustworthiness of its Microsoft Online Services offerings. This paper describes how Microsoft:

- Manages security, privacy, and continuity of the Online Services through a robust and mature compliance management program.
- Aligns with industry standards for security and reliability.
- Periodically obtains independent validation and testing through accredited third-party organizations.

In the right hands, your messaging and collaboration applications are more secure, more available, and more scalable than if you were bearing the expense and effort of operating those services yourself.

Why Online Services?

Ask your online service provider:

How secure?

How private?

How available?

… And how do you prove it?

Key applications such as messaging, worker and group collaboration tools, and online conferencing services provide the foundation for businesses of all sizes and in all markets. Though necessary to the day-to-day operation of your business, these applications can be expensive to purchase and operate. These important communication tools require staff with specialist skills outside the key requirements for your business, can represent a significant overhead, and must be regularly maintained and monitored to ensure that they are securely and reliably operated.

Until recently, there were few alternatives to running your own on-site IT applications and services. But with the developments in Web-based technologies that enable service providers to host them for you, there are now opportunities to access just those applications and services that you need, when you need them, and without deploying and operating them yourself.

Immediate benefits to using Web-based or online services include lower total cost of ownership: you have no specialized staff to hire, no equipment to house, no server software to maintain and operate. Services scale readily to match your business requirements; you're never under-provisioned or over-provisioned and your online "virtual" IT department grows and responds to your changing needs.

But handing over control of your IT service to an online service provider requires due diligence, and most likely raises immediate questions:

- How experienced is my online service provider?
- How do I know my data is kept private and can only be accessed by the appropriate people?
- How secure is my data?
- Will my data be available to me when I need it?
- Will my e-mail and collaboration services be up and running when I need them?
- How can I be sure that my service is as reliable and safe as my service provider claims it is?

Why Online Services from Microsoft?

Microsoft Online Services offer a selection of hosted communication and collaboration services designed to deliver flexibility and low overhead costs.

The Business Productivity Online Standard Suite is a set of Microsoft Online Services, subscription-based enterprise software services hosted by Microsoft and sold with partners. The Online Services operate within a complete ecosystem of features and capabilities that are designed to meet and in many cases to exceed the security and availability goals that you have for your business applications. Best-of-breed data centers host highly secure servers that are operated using verified, industry-leading best practices. These are among the features of the Business Productivity Online Standard Suite that help secure your data from the desktop to the data center, and world-class support staff are fully trained and ready to provide help.

When you sign up to use the Business Productivity Online Suite, you can select from a set of mature enterprise-class applications that offer key features such as e-mail, collaboration, instant messaging, and Web-based conferencing services.

Microsoft has many years' experience designing hosting deployments for Internet service providers, in which these mature enterprise applications are run as Web-based services and offered to business clients. This experience feeds into the overall design of the Microsoft Online Services architecture.

The Business Productivity Online Standard Suite from Microsoft includes the following services:

- **Microsoft Exchange Online** – A hosted enterprise messaging solution based on Microsoft Exchange Server 2007. Exchange Online helps give businesses the e-mail security they demand, the anywhere access that employees want, and the operational efficiency that IT staff need.
- **Microsoft SharePoint® Online** – A hosted enterprise collaboration solution based on Microsoft Office SharePoint Server 2007. SharePoint Online gives businesses a secure, central location where employees can efficiently collaborate with team members, find organizational resources, manage content and workflow, and gain business insight to make better-informed decisions.
- **Microsoft Office Communications Online** – A Microsoft-hosted instant messaging (IM) and presence solution based on Microsoft Office Communications Server 2007. Office Communications Online helps give businesses a more secure environment than public IM tools for real-time collaboration and working within teams that are increasingly dispersed around the world.
- **Microsoft Office Live Meeting** – A Microsoft-hosted Web conferencing solution that enables businesses to collaborate from virtually anywhere. Using only a PC with an Internet connection and basic software, employees can connect internally and engage customers and partners externally through real-time meetings, training sessions, and events.

The result is a set of enterprise-ready Microsoft Online Services that can easily be scaled and that have clear and calculable cost. And the services are delivered complete with ongoing improvements and technology upgrades at no extra cost.

The Foundation of Microsoft Online Services: Trustworthy Computing

Microsoft Online Services, including the Online Services that are included with the Business Productivity Online Standard Suite, have at their foundation mature software design, development, testing, operations, and maintenance practices based squarely on core principles that have come to characterize the Microsoft approach to security, privacy, and overall business practices.

The Trustworthy Computing Initiative

In 2002, Bill Gates set out the basis for the Trustworthy Computing Initiative, a company-wide effort aimed at *"...building trust into every one of our products and services."* Bill set out the key aspects of the initiative that would embody the Microsoft approach to building software and services:

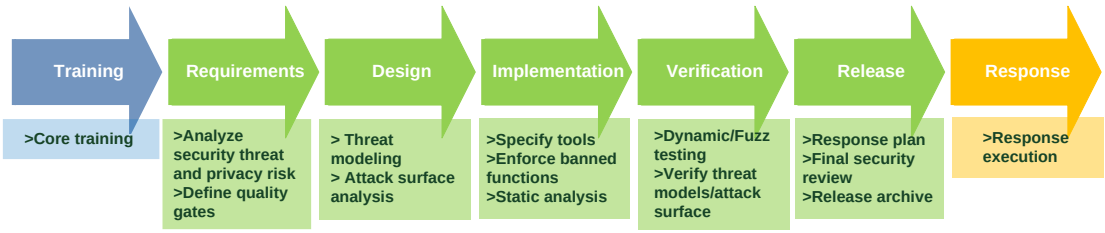
Security is embedded in the long Microsoft history of software development and business culture.

- "***Availability:*** *Our products should always be available when our customers need them. System outages should become a thing of the past because of a software architecture that supports redundancy and automatic recovery. Self-management should allow for service resumption without user intervention in almost every case.*
- ***Security:*** *The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and built into their applications.*
- ***Privacy:*** *Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information, including controlling the use of e-mail they send.*"

The overall goal of trustworthy computing, now a corporate tenet at Microsoft, is to deliver secure, private, and reliable computing experiences for everyone. Trustworthy computing involves not only making the computing experience inherently safer, but also making it more reliable and available while at the same time protecting customers' privacy.

Developing Secure Services: The Security Development Lifecycle

The Microsoft Security Development Lifecycle (SDL), the industry-leading Microsoft software security assurance process, is applied to Microsoft Online Services development, deployment, and maintenance. Like the Trustworthy Computing Initiative, the SDL is a Microsoft-wide initiative and has been a mandatory policy since 2004. The SDL has played a critical role in embedding security and privacy into Microsoft software and culture, introducing security and privacy early and throughout the development process.



Microsoft Security Development Lifecycle

All Microsoft software and services used in the Online Services are built according to the SDL process. SDL develops threat models for each component, evaluating each identified threat according to one or more risk categories:

- **Spoofing identity –** Attacks that allow a user or server to pose as a valid user or device within the environment.
- **Tampering with data –** Attacks that maliciously modify data or add erroneous data to a dataset.
- **Repudiation –** Threats that make it possible for a user to deny a specific action.
- **Information disclosure –** Attacks that expose information to individuals who are not supposed to have access to it.
- **Denial of service –** Attacks that prevent valid users from accessing the system and system data.
- **Elevation of privilege –** Threats that make it possible for unprivileged users to escalate their privileges.

Threat models categorize risks and assess severity before assigning priority and arriving at appropriate countermeasures.

Based on these evaluations, appropriate countermeasures are built into each product to mitigate the identified risks. In prioritizing these countermeasures, the severity of each risk is judged according to a set of factors that provide an assessment of the overall threat:

- **Damage potential –** The potential for damage is related to the overall quantity of data as well as to the impact on data confidentiality, integrity, and availability.
- **Reproducibility –** The effectiveness of an attack increases if it can be repeatedly executed.
- **Exploitability –** An attack can be characterized by how much expertise is required to create and execute it.
- **Affected users –** The more system users that are affected by the attack, the more dangerous that attack may be.
- **Discoverability –** A measure of the availability of information and the visibility of code that may assist in executing an attack. A key input to the software design and review process.

Building and Maintaining Trust: The Microsoft Online Services Risk Management Program

Service security is more than a feature, it is an ongoing effort that combines experienced and qualified personnel; software and hardware technologies; and robust processes to design, build, deploy, operate, and support the service. Security must be vigilantly maintained, regularly enhanced, and routinely verified through testing.

An effective risk-based information security strategy is necessary to protect the confidentiality, integrity, and availability of Microsoft Online Services and the data processed through the services.

Threats to the security or availability of the service are characterized by the generic term "risk." How likely is it that your data will be intact and available to your chosen application when you need it? The Microsoft Online Services Risk Management Program (RMP) focuses on ensuring that Microsoft Online Services, including the Business Productivity Online Standard Suite, are developed and operated in a manner that exceeds industry best practices for security, privacy, and continuity. The RMP also validates ongoing compliance with those practices through third-party audits.

An equally important priority of the RMP is to ensure that the Online Services in the Business Productivity Online Standard Suite provide the functionality and features that allow customers to manage the services and their own data in accordance with their own policies and requirements.

Risk Management Program Objectives

The RMP goal is to ensure that services are developed and operated in a manner that exceeds industry best practices for security, privacy, and continuity.

The Risk Management Program objectives are threefold:

- **Help to ensure the security and privacy** of Microsoft Online Services by providing an efficient, robust, and mature risk management program that is designed to meet or exceed industry best practices and, where possible, accommodate customers' regulatory or legal obligations.
- **Meet customer expectations** by ensuring that Online Services features and functionality are available to support applicable security and compliance obligations, providing expertise in meeting key vertical market or geo-location requirements, and facilitating transparency into the security, privacy, and continuity health of Online Services.
- **Continually mature and enhance** Online Services capabilities by contributing to product and service innovations, driving feedback into the product release cycle, and providing solution accelerators to extend the applicability and usability of Online Services worldwide.

Risk Management Program Success Criteria

The success criteria for the Microsoft Online Services Risk Management Program include:

- **Visible support and commitment** from Online Services executive management.
- **The establishment and implementation of an information security policy** and related objectives and activities that reflect business objectives.
- **Distribution of guidance** on information security policy and associated standards to all employees and contractors.
- **Effective promotion of security to all managers and employees,** and an effective user education and training plan to update staff on changes to the existing policy, supporting infrastructure, and processes.

- **A comprehensive and balanced system of measurement** that is used to evaluate performance in information security management and feedback suggestions for improvement.

Risk Management Core Disciplines

The Risk Management Program is designed to provide tried and tested design, development and operations practices that are applied across the complete Microsoft Online Services solution, from software running on your premises, through the network, to the services infrastructure and the data centers in which it is hosted.

The Risk Management Program focuses on four core areas to provide secure and available services, with demonstrated compliance to industry standards for services provision:

- **Security –** The environment must include features that secure it from intentional and unintentional attack.
- **Privacy –** A customer's data and operations must be regarded as private and restricted to that customer.
- **Continuity –** The services and related data must be available when required, and robust capabilities must exist to ensure recoverability from catastrophic events.
- **Compliance –** The services must operate in demonstrable compliance with Microsoft security policies and relevant industry standards.

Security

Service security must be proactively designed into all aspects of the online experience, from the software itself to the supporting infrastructure, from the day-to-day best practices for your own information workers to the buildings that house the data centers.

The security architecture for Microsoft Online Services embodies the key principles of the company's Trustworthy Computing Initiative: security created by design, by default, and by deployment. Developed for global enterprises, the multifaceted Microsoft security program applies a common set of security policies to manage risk and mitigate threats to customer data. Microsoft seeks to improve security by working to standardize the way it tests, implements, and monitors policies for all of its customers. In turn, each Business Productivity Online Standard Suite customer benefits from Microsoft experience with the security concerns of customers all over the world—and from the practices that Microsoft applies to address them.

Microsoft Online Services create security by design, by default, and by deployment.

A Comprehensive, Ongoing Process

A complete online services solution addresses security and availability at all points in the chain from your users to the staff and facilities that operate your services. To resist attack and safeguard customer data effectively, Microsoft Online Services apply the principle of "defense in depth," a layered security strategy that independently defends the various components of a service: the application, the supporting infrastructure and hardware, the network, and the data center facility.

Security measures can be generally divided into two main areas:

- **Physical** security measures are applied to the buildings that house the hosted services, the computer and other specialized hardware, and the staff who run those facilities.
- **Logical** security measures are applied through software at the operating system, infrastructure, and application layers of the system.

Physical Security

Physical security is often regarded as the poor relation of logical or software-based security; when customers consider security and availability, they often think first of viruses and malware attacks or crashed disks. However, it's every bit as important to consider physical security, and it's a tough problem to ensure that your data is physically secure even on your own premises.

The same rigorous physical and logical security practices are applied to datacenters hosting Microsoft Online Services throughout the world.

You need to be confident that only authorized staff have access to the hardware on which you run your business. You need to know that power outages, staff vacation, or physical relocation of your computers will not affect your operations or expose your data to unmanaged risks.

Moving to an online service in some respects simply shifts that responsibility to the service provider; now you need to be confident that the service provider has thought through these issues on your behalf, and has incorporated solutions and mitigations to physical security issues into the data center that houses your data.

Carrier-Class Data Centers

Microsoft enforces physical security controls as part of a broad set of carrier-class data center operations. Carrier-class means very high availability, allowing only a few minutes' downtime per year. The data centers in which Business Productivity Online Standard Suite services are operated achieve carrier-class performance through features such as:

- Physical building security.
- Secure physical access for authorized personnel only.
- Redundant power supplies:
    - Two main power supplies from separate providers.
    - Battery backup.
    - Diesel generators (with alternative fuel delivery contracts in place).
- Multiple fiber trunks connecting the data centers for redundancy.
- Climate control to ensure that equipment runs at optimal temperature and humidity.
- Seismically braced racks where required.
- Fire prevention and extinguishing systems that cause minimal disruption to computer equipment.
- Motion sensors, 24-hour secured access, as well as video camera surveillance and security breach alarms.

Worldwide Data Center Locations

The Online Services are deployed in data centers worldwide, offering geographically local hosting with global availability.

Security for Data Center Personnel

An additional layer of security within the data center is applied to personnel that operate the facility. Access is restricted by job function so that only essential personnel are authorized to manage customers' applications and services. Authorization requires:

- Badge and smartcard restricted access.
- Biometric scanners.
- On-premises security officers.
- Continuous video surveillance.

In addition, authorized personnel must have prior approval for all operations and actions within the data center. Any operations that are not already part of established process and procedures are reviewed before they can be executed.

Two-Factor Authentication

Data centers are "lights-out" deployments and require remote support and administration. Remote support and administrative access to Online Services environments is conducted over a 128-bit encrypted communication channel and requires two-factor authentication. Two-factor authentication provides a physical, tamper-resistant security layer by requiring access with the use of a physical device, such as a smart card and a personal identification number (PIN).

Secure Network Design and Operations

Multiple separate network segments provide physical separation for critical back-end servers and storage devices from the public-facing interfaces. Networks within data centers that

operate Online Services have full N+1 redundancy, and full failover features help protect all network equipment.

Best-of-Breed Hardware

Servers that run your applications and services are fully redundant with dual network interfaces, dual power supplies, and full lights-out management capability. Servers are custom configured for the Online Services architecture for maximum efficiency, availability, and scalability. Hardware can be added and removed without interrupting service, and servers can be accessed only by authorized personnel using physically secured networks with dedicated network connections.

Custom Hardware

Microsoft data centers use hardware that is specifically designed and configured to support the software and services that form the Online Services. Just as the software is tailored and hardened to enable only the necessary and eliminate the unnecessary functions, so is hardware designed to operate as efficiently, effectively, and securely as possible. This process increases the speed and effectiveness of configuring, deploying, and securing new servers, and ensures that security requirements are continually met. In the process, it also eliminates unnecessary cost, power consumption, and space consumption, savings that can be passed on to Online Services customers.

Logical Security

Logical security in Microsoft Online Services means securing the software that is already running on physically secure hardware, in secured data centers. The holistic Microsoft approach to software security is driven by thorough risk assessment and mitigation processes.

Features of the Microsoft Online Services

The applications that make up the Online Services share many features that help secure the confidentiality, integrity, and availability of your data in the Online Services environment. Whether on your premises or operating within the Online Services architecture, these features provide effective and proven means of increasing availability and reducing risk.

Hosted Applications Security Features

- **Sign-in client** that supports strong user passwords, making it easy to provide users with secured access to multiple applications.
- Support for **authenticated and encrypted communications** that help identify messaging participants and prevent message tampering.
- Support for **Secure / Multipurpose Internet Mail Extensions (S/MIME) and rights management** technologies that add digital signatures and encryption technologies to e-mail messages.
- **Client-side attachment blocking** to prevent potentially dangerous e-mail attachments.
- **Restricted message relaying** to reduce unwanted messaging and spam.
- **Real-time block lists (RBL)** and safe lists to restrict messages from known sources of spam.
- Multilayered **antivirus filtering** to help protect your organization’s incoming, outgoing, and internal e-mail messages and shared files.
- **Flexible device policies** to help secure mobile device communications (such as PIN lock and remote or local wipe).

The Microsoft Online Services Infrastructure

The Online Services infrastructure consists of the hardware, the software, and the networks that are required to run the Online Services within the physical data center premises.

Security measures within the services infrastructure are likely to be more stringent than those an enterprise might provide within its own network. Infrastructure-level security measures include:

- **Security trimmed user interfaces** that filter available features to only those actions, links, and content that a specific user is authorized to access.
- **Extensive server monitoring support**, integrated with the overall service-wide Microsoft System Center Operations Manager monitoring architecture.
- **Secure remote access** via Windows Server® 2008 Terminal Services.
- **Multi-tier administration**, using a three-tier administration model that isolates administrative tasks and controls access to them based on the user's role and the level of administrative access to which the user is authorized.
- **Server-level antivirus scanning** for protection against viruses that target the server operating system.
- **Environmental security scanning** to monitor for vulnerabilities and incorrect configuration.
- **Intrusion detection systems** to provide continuous 24-hour monitoring of all access to the Online Services. Sophisticated correlation engines analyze this data to alert staff immediately of any connection attempts that are classified as suspicious.

Operating System Security Standards

To help protect Online Services from attack by malicious users or malicious code, special care is taken in hardening the operating system. The hardening of the operating system includes disabling nonessential services, securing file shares to require authorization, and implementing the Data Execution Prevention (DEP) feature. DEP is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running.

Microsoft Online Services practice "defense in depth," a layered security strategy that defends components of a network by using multiple mechanisms, procedures, and policies.

All servers within the Online Services environment are regularly updated with the appropriate security updates for the software that they use. The time when updates are applied is based on a schedule derived by the criticality, scope, and impact of the security vulnerability associated with each update.

Systems Management and Access Control

Management of the networks and component servers that run the Online Services is provided by the Active Directory® service. Applications that provide the Online Services are designed to operate efficiently and effectively within the Active Directory environment.

Staff manage and enforce security policies centrally, from secured servers that are dedicated to controlling and monitoring network-wide systems. A delegated management model enables administrators to have only the access they need to perform specific tasks, reducing the potential for error and allowing access to systems and functions strictly on an as-needed basis.

New servers can be quickly and safely configured, and template-based server hardening ensures that new capacity is brought online with security measures already in place.

The Microsoft Online Services Network

Network connections from your business to the Online Services are secured by certificates using the Secure Sockets Layer protocol (SSL).

Communications are protected with 128-bit encryption. Microsoft intends to ensure that not only is the data that is stored within the Online Services protected, but also that when you're using the Online Services, any transmission of that data is also secure.

Connections that arrive at the Online Services platform itself must pass scrutiny by rigorous security policies before they can cross filters and firewalls to enter the network. Full N+1 redundancy throughout the network offers full failover capability and helps ensure 99.9-percent network availability.

Firewalls and Filtering Routers

Firewalls and filtering routers at the edge of the Online Services network provide well-established security at the packet level to prevent unauthorized attempts to connect to the Online Services. They help to ensure that the actual contents of the packets contain data in the expected format and conform to the expected client/server communication scheme. Firewalls also restrict data communication to known and authorized ports, protocols, and destination IP addresses. In this way, external access to the Online Services is restricted to the ports and protocols that are required for the communications between the Online Services and the Online Services customers.

Protection Against Malicious Software

The services in Business Productivity Online Standard Suite run multiple layers of antivirus software to help ensure protection from common malicious software. For example, all servers within the Business Productivity Online Standard Suite environment run antivirus software that scans the operating system for viruses. Furthermore, Microsoft Exchange Server mail servers run additional antivirus software that focuses on scanning e-mail messages for potential hazards.

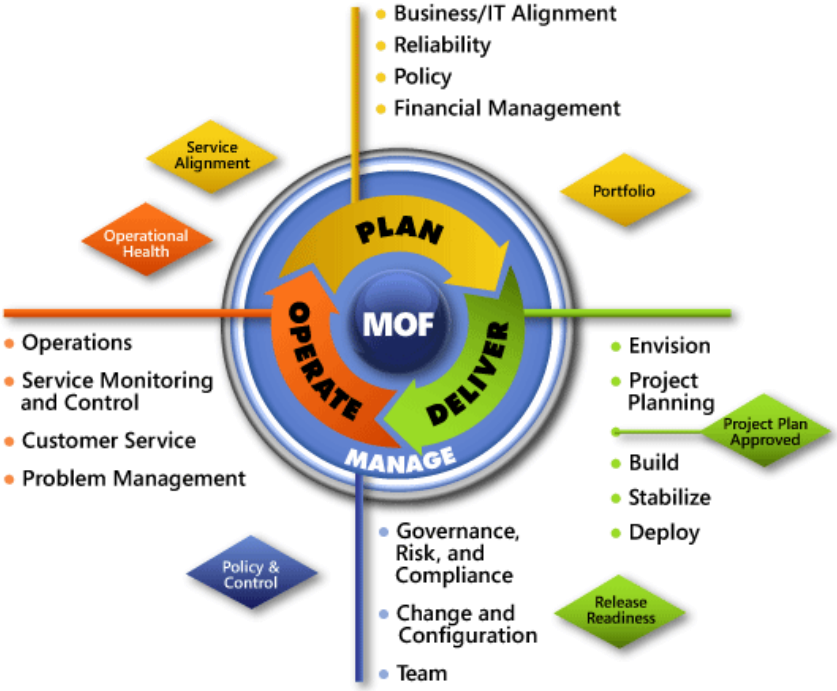
These measures also help prevent viruses that may have been inadvertently introduced into your data by your users.

World-Class Operations

Operations is a key component of the Microsoft Online Services, is central to overall security and availability of the Online Services, and is one of the core competencies that businesses look for in their online service providers. A significant part of the expense of owning and operating your own on-site software is the cost of administration and maintenance, compounded by the need to retain associated support staff. A key value of using Microsoft Online Services is the expertise of the dedicated, standards-driven Microsoft Online Services operations team.

For change management, incident management, and problem management, Microsoft staff follow industry standard principles of the Information Technology Infrastructure Library (ITIL). ITIL provides a framework of guidelines and best practices for managing software services and infrastructure. To this set of requirements, Microsoft has added its own Microsoft Operations Framework (MOF), a prescriptive set of procedures that results in a standardized implementation of ITIL recommendations. MOF provides an integrated set of best practices, principles, and activities that help organizations achieve reliability for their IT solutions and services.

MOF codifies and standardizes procedures for timely and low-risk change management, and helps to define a path for problem management from customer through operations and on to product engineering teams.



Microsoft Online Services Use Microsoft Operations Framework for Service Deployment and Operations

Monitoring and Risk Reduction

To proactively minimize risk and ensure applications and data availability, the Online Services make significant investments in tools and services for monitoring.

Microsoft System Center Operations Manager

Servers within the Online Services environment are configured to maximize the security events from the operating system and the applications. This produces a rich audit trail of how applications are being used, and includes logging of security exceptions should they occur. The Online Services operations team utilizes latest technology and optimized processes to harvest, correlate, and analyze information as it is received.

The Online Services hosting environment uses Microsoft System Center Operations Manager, an end-to-end service management environment that integrates with platform and services hardware and software to provide continuous, 24-hour health monitoring.

Staff monitor both internal network and services performance, and external Web conditions that may affect Microsoft Online Services customer experience.

Custom management packs are layered above the Online Services platform to provide operations staff with very specific information that helps identify trends and predict behavior that may require proactive intervention. The System Center Operations Manager management packs provide internal transaction monitoring, capabilities for looking at service threshold models, and CPU utilization analysis that is tailored to the Online Services applications.

Integrated Infrastructure and Web Performance Monitoring

The wealth of data that is provided from System Center Operations Manager is combined with feeds from additional specialized tools and services to capture, aggregate, and analyze not only the network that operates Online Services, but also the behavior of key sites on the Internet. For example, if connectivity begins to degrade, staff can identify whether the problem is internal to one of the Online Services, or caused by conditions on the Internet that may represent a risk to Business Productivity Online Standard Suite customers.

Hardware and Software Subsystems Monitoring

Proactive monitoring continuously measures the performance of key subsystems in the Online Services platform. Online Services have established thresholds that represent boundaries for acceptable service performance and availability. When a threshold is reached or an anomalous event occurs, the monitoring system generates warnings so that operations staff can address the anomalous event. Examples of specific thresholds include:

- **CPU utilization** – A non-critical alert threshold is established at 80-percent utilization. A critical alert threshold is established at 90 percent.
- **Service utilization** – Various service components including service licenses, capacity for e-mail, and Microsoft SharePoint Online are all monitored.
- **Storage utilization** – If storage reserves are reduced to 15 percent, a non-critical alert is displayed. If storage reserves reach 7 percent, a critical alert is displayed.
- **Network latency** – Non-critical alerts are displayed when network latency is at 100 milliseconds, and a critical alert is generated at 300 milliseconds.

Events and Activity Logging

Monitoring is a key component of the Online Services security strategy. Security monitoring provides two primary benefits for the Business Productivity Online Standard Suite: the ability to identify attacks as they occur, and the ability to perform forensic analysis on the events that occurred before, during, and after an attack.

Detecting attacks as they occur enables Microsoft staff to react quickly to help reduce substantive damage to the services and the supporting infrastructure. Forensic data also helps investigators identify the extent of the attack.

Access and activity logging is an important facet of security. Monitoring the creation or modification of objects provides a way to help track potential security problems, helps to ensure user accountability, and can provide evidence in the event of a security breach. The Online Services operations program monitors and logs information related to the following event types:

- Account logon events
- Account management
- Directory service access
- Logon events
- Object access
- Policy change
- Privilege use
- Process tracking
- System events

Microsoft constantly performs internal and external vulnerability assessment scanning against Microsoft Online Services networks.

Integrating Security with Operations

Microsoft Online Services maintain a dedicated security organization that is focused on constant security vigilance, with staff following principles defined in MOF. From a broad operations perspective, Microsoft structures internal operations based on the Information Technology Infrastructure Library (ITIL) framework. The security team follows the functions defined by ITIL, and applies them to the operation of the Online Services:

1. **Change management** -- Change Management is an important element in ensuring that your data is protected and always available. The Business Productivity Online Standard Suite team follows ITIL change management guidelines, which drive a regimented approach to how the environment is changed. As the software-plus-services paradigm grows in popularity, Microsoft keeps pace with this growth by adding networks, server capacity, and software functionality. Each change within the environment is scrutinized by the Microsoft Online Services security team for the possibility that it may cause downtime or other unintended consequences.

- **Incident management** – The Online Services operations group receives alerts from a variety of sources. These sources include customer e-mail messages, telephone calls, and system and security monitoring tools. Each alert is triaged to decide whether it represents an incident. In some cases, an alert may be classified as a security incident and appropriately escalated through internal Microsoft support groups. If the incident is security-oriented, Microsoft Online Services security personnel work with product experts to ensure rapid incident investigation, response, and closure.
- **Problem management** – If an incident occurs frequently, the appropriate response may be service configuration change or a recommendation to a Microsoft product group to introduce a new feature. Microsoft Online Services security staff help with defining and testing the appropriate service or product change.

Segregation of Duties for Staff

Microsoft Online Services require distinct and separate hosted services development, deployment, and operations staff to adhere to the principle of segregation of duty. This includes controlling access to the source code, controlling access to the build servers, and controlling access to the production environment.

Access to the Business Productivity Online Standard Suite production environment is restricted to operations personnel. Development and test teams may be granted temporary access to help troubleshoot issues. However, this access is granted on a case-by-case, as-needed basis.

Access to Online Services source code control is restricted to development personnel; operations personnel cannot change source code.

Incorporating Risk Management Principles

The operations strategy incorporates the following set of risk management principles that help manage service delivery risks:

- **Defense-in-depth** – Overall security does not rely on a single defense mechanism. Each layer of the Business Productivity Online Standard Suite infrastructure, from the perimeter of the network through the servers and services that make up the infrastructure and hosting customer data, implements controls to help resist an attack.
- **Identity management** – Effective access controls depend on proper identity management and role-based authorization.
- **Compartmentalization** – The Online Services customer, applications, services, and management systems reside in isolated security zones. Accessibility and communications among systems in different zones are carefully managed to help prevent data leakage and make it difficult for an intruder in one zone to attack systems in other zones.
- **Redundancy** – Online Services are designed to help ensure availability by using redundant servers, network components, and geographically dispersed facilities.
- **Simplicity** – Business Productivity Online Standard Suite deployments are optimized for simplicity. The more complex systems are, the more difficult they are to secure; simplicity reduces the potential for configuration or operational error.
- **Least-privilege** – Users and systems are granted only the minimal level of access necessary to perform their defined function.
- **Accountability** – The actions of individuals within the Business Productivity Online Standard Suite environment are traceable to individual users or staff.
- **Auditing** – Systems are designed with audit mechanisms to detect unauthorized use and to support incident investigations.
- **Fail to a secure state** – Systems are designed so that system failures do not reduce the effectiveness of current security controls.
- **Operational excellence** – Microsoft maintains a trained operations staff and well-defined procedures for administering and maintaining Online Services systems, and responding to outages and incidents.
- **Universal participation** – A strong security infrastructure requires the cooperation of all parties in the environment. Attacks can originate from anywhere, and therefore all Microsoft Online Services staff, partners, and vendors, as well as customers, must be active participants in the security program.

Security Incident Management

Security incidents are rare within the Online Services environment. However, Microsoft has developed robust processes to facilitate a coordinated response to incidents if they occur.

Security incidents may include, but are not limited to, e-mail viruses, root kits, worms, denial of service attacks, unauthorized access, inappropriate use of network resources, and any other type of unauthorized, unacceptable, or unlawful activity involving Online Services–based computer networks or data processing equipment.

The Online Services security incident response process follows the following phases:

- **Identification** – System and security alerts are collected, correlated, and analyzed. Events are investigated by Microsoft operations and security teams. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists.
- **Containment** – The escalation team evaluates the scope and impact of the incident. The immediate priority of the escalation team is to ensure that the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In cases where in-depth investigation is required, content is collected from the affected systems using best-of-breed forensic software and industry best practices.
- **Eradication** – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause of the security issue. If vulnerability is determined, the escalation team reports the issue to product engineering.
- **Recovery** – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity.
- **Lessons Learned** – Each security incident is analyzed to ensure the appropriate mitigations are applied to help protect against future recurrence.

Security Investigation

If a significant security event occurs, Microsoft Online Services security staff will launch an investigation to find the facts surrounding the incident, form opinions as to what may have occurred, and perform any experimentation required to form a conclusive description.

Some incidents require forensic investigation. Forensic investigation involves the proper collection and analysis of evidence from a security incident. The process involves the recreation of an incident in a reconstructed environment, to prove or disprove the various theories that arise from the investigative process. In some cases, Online Services security staff may draw upon the deep experience of other Microsoft teams to provide assistance and analysis.

The Online Services security team may also help customers with security matters that they cannot investigate using only the available logs and tools from the Online Services platform. This activity is performed on a case-by-case basis, based on the situation and extent to which Online Services resources are required.

Privacy in Microsoft Online Services

Microsoft recognizes that privacy is a critical element of a highly secure computing experience. Customers have high expectations about how Microsoft collects, uses, and stores their data. Privacy is one of the four pillars of the Microsoft Trustworthy Computing Initiative, along with security, reliability, and business integrity. Microsoft commits significant resources to enhancing privacy protection, and as a result, privacy has been woven into the culture at Microsoft as an automatic priority in every area of the company.

Data Privacy by Design

Privacy efforts are focused around three key areas: technology, partnership and collaboration, and customer guidance and engagement. Microsoft creates policies and processes to ensure that we:

- Engineer privacy into our products during the product life cycle.
- Implement privacy-based technology throughout our internal processes.
- Execute our global privacy practices properly throughout the company.
- Provide leadership for the industry.

No matter where our customers live or work, Microsoft strives to help them protect their data.

To create a trusted environment for our customers, Microsoft develops software, services, and processes with privacy in mind. Microsoft is vigilant in its compliance with global privacy laws; its 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.

Additionally, Microsoft employs technical and organizational security measures to ensure appropriate handling of customer data.

Specific Privacy Practices: Marketing and Advertising, and Testing

Two areas of Microsoft information handling practices are of specific interest to customers: marketing and advertising, and testing.

Marketing and Advertising

Microsoft markets only to the business customer who registered and purchased the service (or to a successor as the designated contact and representative of the customer). Microsoft will not contact a customer's users, or use any personal information collected for providing the service, for marketing or advertising purposes except with the explicit consent of the customer.

Testing

To improve the Online Services, Microsoft may automatically compile a sample set of data from across the Online Services to run through servers before planned updates. This helps to ensure that problems are identified early, that your service experience remains uninterrupted, and that there are fewer support incidents in the future.

Additionally, if Microsoft identifies spam or malware originating from your account, this information may be isolated and used to improve the security of the Microsoft network for all users.

Vendors and Partners

To help provide our services, we occasionally provide information to other companies that provide limited services on our behalf. These companies are required to maintain the confidentiality of personal information and are prohibited from using it for any other purpose.

Vendors

All Microsoft vendors are required to join the Microsoft Vendor Privacy Assurance Program, which requires them to meet Microsoft standards for privacy. Microsoft enforces vendors' compliance by contract and by vendor audits.

Partners

If a customer requests Microsoft partner features or support, Microsoft will share personal information with those partners in response to that request. Microsoft is not responsible for the privacy and information-handling practices of such partners. However, Microsoft will always provide clear notice that personal information will be transferred, when a customer signs up to link an account with a Microsoft partner. Additionally, a customer may choose not to share information with a partner at any time, at which point information sharing will stop.

Access, Security, Data Integrity, and Enforcement

To ensure that customers maintain control over their own data, the Microsoft Online Services are designed to provide the customer's administrators or representatives with complete access to the customer environment, including their users' mailboxes and Web sites so that they can enforce their own company's security and privacy policies.

Either on request or on a periodic basis, Microsoft will provide records that detail administrator access to users' mailboxes to help customers audit and enforce their policies regarding appropriate behavior for their service administrators. These records will also detail access by support partners and by Microsoft support personnel, except when prohibited by legal process.

Customer Guidance

Security and privacy starts on your premises. Therefore, Business Productivity Online Standard Suite services include documentation, applications, and utilities to make it easy for your users and administrators to join Microsoft to help keep your data secure and private.

Online Web interfaces or portals provide simple, straightforward guidance for users and administrators. Administrators can provision users and services, and monitor usage of Business Productivity Online Standard Suite services throughout your organization. Users can access and manage their assigned services, and a single sign-on application makes it easy to create and use a strong password with minimal effort. The goal is for the online experience to be more secure and private by default, because the most effective safeguards are those that are the most transparent and easily followed.

As a Business Productivity Online Standard Suite customer, you are responsible to ensure your own compliance with applicable policies, practices, and regulations by tailoring our feature set appropriately to suit your unique needs. For example, you should interpret relevant privacy laws and regulations; notify and obtain consent, as appropriate, from employees and other users about data location and processing; and you should define the appropriate level of protection for different classes of your organization's personal information.

Personal information within the Online Services will only be collected, processed, and transferred with the consent of the customer or as required under applicable law. We use personal information only to provide, operate, and improve Microsoft products and services.

The Privacy and Trust in a Connected World white paper offers further information about how Microsoft is helping customers protect individual and organizational privacy through a combination of technology innovation and investments, leadership and collaboration, and customer guidance and engagement.

International Data Transfer

A goal of Microsoft Online Services is to be available to users in as many markets as possible.

Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country/region in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities.

For customers in the European Union, Microsoft is Safe Harbor–certified with the U.S. Department of Commerce and abides by the Safe Harbor Framework regarding the collection, use, and retention of data from the European Union. This allows for legal transfer of data to Microsoft for processing from within the European Union, as well as countries that have aligned their data protection laws with those of the European Union.

Service Continuity Management

Data can be accidentally or maliciously deleted. The management of security and availability go hand in hand to create services and data that are available whenever you need them, but service continuity management adds the ability to proactively avoid outages or data losses, and to recover from such disasters if they do occur.

Continuity helps keep services ready, data available, and your business running.

Many generations of services hosting platform software and hardware design, deployment and training experience are now applied to the Business Productivity Online Standard Suite. That industry-leading experience is applied at all points in the Microsoft Online Services design, provisioning, operations, and support to help protect your business from downtime due to unavailable applications or lost data.

Archiving for Messaging Continuity

Access to the e-mail service and to historical e-mail transactions is important both to business continuity and for legal compliance requirements.

The Business Productivity Online Standard Suite has an available hosted archive option, which offers advanced message archiving and compliance tools for e-mail, instant messages, and Bloomberg mail. The hosted archive has the following features:

- **Convenient access:** As a business continuity tool, the archive can be accessed by e-mail administrators and end users, to recover messages that may have been lost or deleted from the primary e-mail environment.
- **Continuous receipt of mail:** If normal delivery of e-mail is blocked because the primary mail environment is down or the corporate network is unavailable, the hosted archive continues to copy messages to the archive. The original messages are queued, and are then delivered after the primary e-mail environment is restored.
- **Fully indexed database:** As messages are archived, each one is full-text indexed with the metadata, message body, and any attachments that are stored in the database. All database servers have fully functioning standby databases secured in a separate facility. Each primary database regularly ships transaction logs to the corresponding secondary database via Secure Shell protocol (SSH), and a regular, formal backup schedule ensures redundancy for customers' archived data.

Data Storage

Specialized storage servers provide redundant, mirrored storage for customer data. Continuous offsite mirroring—to geographically diverse data centers—helps ensure that data is secure and current even in the unlikely event of a complete local data center failure. All data is stored on disks rather than tape for rapid, error-free recovery, on clustered servers with redundant backup services provided by Microsoft System Center Data Protection Manager. Data Protection Manager provides byte-level replication and automatically validates replicated data against known-good production servers to maintain data integrity. Data protection is near-continuous, and real-time monitoring provides administrators with current backup status.

In addition to the normal backup and restore procedures, Business Productivity Online Standard Suite services allocate approximately 30 percent of all raw disk space for redundancy. A combination of RAID5 and RAID1 provides rapid, reliable disk access and disk arrays maintain spare drives to eliminate any single point of failure in the configuration.

Along with avoiding data loss, a goal of the service is to maintain data performance. Databases are regularly checked for:

- Blocked processes.
- Packet loss.
- Queued processes.
- Query latency.

Preventative maintenance includes running database consistency checks, periodic data compression, and error log reviews.

Availability and Continuity

High availability requires proactive procedures to ensure that problems are addressed as they arise, and before they affect customers. The goal is to discover issues and provide mitigations before customers experience any problems.

Minimizing data loss, maximizing data availability: the two go hand in hand.

99.9-Percent Reliability

Microsoft Online Services have a measured 99.9-percent reliability. N+1 redundancy means that critical components throughout the service—at the network, data storage, and applications server levels—are duplicated to protect against failures. Details such as dual power supplies and network interfaces further increase uptime for key components. In addition, configurations are replicated offsite among data centers so that the data centers themselves are protected.

Avoiding Resource Constraints Through Scalability

Excess capacity is built into the Business Productivity Online Standard Suite. All users are pre-allocated the resources that they need, and additional capacity can be brought online proactively, in advance of current resources becoming constrained. The result is that you can add users, storage, or services at any time and get immediate results.

To help prevent unscheduled capacity bottlenecks, advanced capacity modeling techniques implement capacity enhancements at least three months ahead of forecasts. Capacity is reviewed regularly against demand, to help prevent resource constraints from affecting overall service.

Dedicated Support

The Microsoft Online Services development and operations teams are complemented by a dedicated Online Services support organization, which plays a key role in providing customers with business continuity. Support staff have a deep knowledge of the service and its associated applications, and direct access to Microsoft company-wide experts in architecture, development, and testing.

Tightly aligned with operations and product development, the support organization offers fast resolution times and provides a channel for customers' voices to be heard. Feedback from customers provides input to the planning, development, and operations processes.

Customers need to know that their issues are being addressed, and they need to be able to track timely resolution. The Microsoft Online Services Administration Center provides a one-stop Web-based interface to support, from which customers can add and monitor tickets and receive feedback from support personnel.

The portal makes it easy for customers to manage their Online Services, because it combines administration functions—adding and removing users and services, for example—with support functions—entering and monitoring trouble tickets.

Self-Help, Backed by Continuous Staff Support

The goal for Microsoft and for Business Productivity Online Standard Suite customers is self-sufficiency, avoiding the need for support if possible. Before they enter a ticket, customers can access Knowledge Base articles and FAQs that provide immediate help with the most common problems. These resources are updated continuously with the latest information, which helps avoid delays by providing solutions to well-understood issues.

However, when an issue arises that needs the help of a support professional, staff are available for immediate assistance by telephone and via the administration portal 24 hours a day, every day.

Compliance

All companies face significant legal and regulatory challenges in areas such as information security, privacy, reliability, and business integrity. Compliance, in broad terms, means satisfying all of the legal and business requirements that an organization faces during the course of running its business. The increasing number of regulations—along with greater-than-ever enforcement activity—highlights the importance of having in place appropriate internal governance policies and procedures, directly and through an organization's service providers. Numerous embedded internal policies (such as procurement, quality assurance, and recruiting) add another layer of complexity to the compliance requirements that an organization needs to manage.

The Business Productivity Online Standard Suite compliance strategy is based on a proactive continual compliance approach to minimize risk and secure the environment. This is backed up by independent third-party audits on a periodic basis to provide greater assurance to Microsoft customers.

The Microsoft Online Services approach to compliance is to proactively identify non-compliance risk, and create a culture of continual compliance within the Microsoft Online Services organization.

The Business Productivity Online Standard Suite compliance goals include ensuring that:

- Online Services comply with Microsoft security policies and relevant industry standards.
- Online Services meet contractual security and compliance obligations to customers.

Standards-Driven Compliance Management

The Business Productivity Online Standard Suite compliance team follows the risk-based approach and continual improvement process of the International Standards Organization (ISO). The team assesses compliance of security implementations using a methodology based on the guidelines provided within ISO 27001.

A central, standardized source of audit controls is an essential component of a coordinated compliance management program. The Business Productivity Online Standard Suite compliance team uses a common control framework based on ISO 27001 as the basis for extensible Business Productivity Online Standard Suite security controls, allowing Business Productivity Online Standard Suite engineers to quickly implement new controls as needed.

Microsoft Online Services Compliance Management Program

Typically, there is a high degree of commonality among seemingly distinct regulatory and policy requirements, which can span processes, policies, controls, and technology. Making efficient use of these commonalities creates competitive advantage for the compliance function within an organization.

To make the process of managing multiple technical controls more efficient, Microsoft identifies overlap in the technical or process-based controls that these requirements drive, and where possible, implements a single control to address those requirements. In this manner, Microsoft builds an integrated set of specific control objectives, and drives those control objectives into a consolidated framework.

These common controls are categorized into the following domains or competencies:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Microsoft regularly reviews its common control framework in light of changes in industry standards and the various legal or regulatory environments in which customers do business.

The Microsoft Online Services Compliance Framework

Microsoft has implemented a framework-based approach to managing compliance-related controls. This approach enables Microsoft staff to:

- Efficiently plan, deliver, operate, and continually manage compliance requirements.
- Build technical and process controls to address customer requirements that stem from various regulatory standards, such as SOX and HIPAA.
- Address and plan for evolving customer requirements.
- Prevent duplication of work, redundancy, or conflicts within Microsoft Online Services by providing effectively planned compliance solutions that communicate across the organization.
- Update current compliance requirements more efficiently through controlled delivery of incremental changes to the existing controls.
- Establish and maintain a common ground between Microsoft Online Services, customers, and auditors.

Compliance Assessments and Audits

The internal Microsoft compliance team is responsible for auditing, monitoring, managing, and closing audit issues. Therefore, the team periodically conducts assessments of people, processes, and technology controls to assess operational effectiveness.

Ongoing internal and external auditing maintains customer confidence in the Microsoft compliance process.

The compliance assessment involves several phases:

1. **Planning.** In the planning phase of the assessment, scope and applicable controls are defined.
2. **Assessment.** The effectiveness of controls is measured and reported. Microsoft compliance assessment processes include people, processes, and technology controls. Depending on the control, the control effectiveness is assessed using the following common auditing practices:
    - **Inquiry.** Auditors seek information from knowledgeable persons throughout the organization or outside the organization.
    - **Inspection.** Auditors examine records or documents, whether internal or external, in paper form, electronic form, or other media.
    - **Observation.** Auditors look at a process or procedure that is being performed by the Microsoft Online Services operations teams.
3. **Remediation.** The team develops a remediation plan to address the findings discovered during the audit. Findings are tracked until they are addressed. Business Productivity Online Standard Suite service teams own and execute the remediation plan, and any residual risks are communicated to senior management.
4. **Reporting.** When all testing is complete, Microsoft compiles the findings in a report. This report details any deficiencies discovered during the audit. Typically, deficiencies belong to one of the following categories:
    - **Design deficiencies.** These deficiencies are situations in which Microsoft finds a complete or partial lack of controls for a given risk, or finds that the controls are insufficient to adequately accomplish their goal. An example of a design deficiency is if the organization handles confidential customer information, such as a name, address, and driver's license number, but has no process defined for how it protects this personally identifiable information.
    - **Operational deficiencies.** These deficiencies are situations in which Microsoft finds that the controls are not applied as designed. These situations could occur if the control was documented but never put into production, or if the control is in production but not followed. For example, a control might state that managers must approve a user access request for a particularly sensitive resource before the user is granted access. This control would constitute an operational deficiency if access is routinely granted without such approval.

Independent Certification

In addition to internal assessment as described above, the Microsoft Online Services organization undergoes various independent third-party compliance audits to provide a greater level ofguarantee to our customers. Such independent, objective audits may also help satisfy customers' legal, regulatory, and compliance obligations.

Demonstrating Compliance

There are a number of ways to demonstrate standards compliance. Two of the most prevalent methods are the Statement of Auditing Standard (SAS) 70 Type II and the ISO 27001 certification.

SAS 70 also helps Microsoft and its customers comply with the Sarbanes-Oxley Act (SOX) legislation for the management of electronic records.

The Microsoft strategy is to undergo independent unbiased third-party compliance audits and certifications of Online Services to validate control design and operational effectiveness, from service development to physical deployment of infrastructure and operations. This third-party assurance enables our customers not only to be confident about the security of the Business Productivity Online Standard Suite services, but in some cases it also enables them to satisfy their own legal, regulatory, and compliance obligations.

These third-party audits also save customers money by eliminating the need for customers to conduct their own audits, while at the same time providing a better control validation of Business Productivity Online Standard Suite services via an independent third-party entity.

Microsoft develops compliance strategies based on the nature of the service offering. In the current service line, a service may have one or more of the following:

- Statement of Auditing Standard (SAS) 70 Type II
- ISO 27001 certification
- Verizon Security Management Program – Service Provider Certification (formerly Cybertrust)

Statement of Auditing Standard (SAS) 70

SAS 70 is an acronym for Statement on Auditing Standard Number 70; it was developed and is maintained by the American Institute of Certified Public Accountants (AICPA).

Specifically, SAS 70 is a "Report on the Processing of Transactions by Service Organizations." SAS 70 is a thorough audit that demonstrates transparency to the service organization's customers and partners. Although SAS 70 audits and reports can be costly and time-consuming, they have definite advantages for service organizations that use them.

SAS 70 compliance demonstrates that a service provider has been thoroughly checked by an independent third party and deemed to have satisfactory controls and safeguards when hosting or processing data belonging to its customers. In this way, it provides transparency and builds trust with customers.

ISO 27001

ISO 27001 is the formal standard against which organizations may seek independent certification of their information security management systems (ISMS). It specifies requirements for the implementation of security controls that are customized to the needs of individual organizations or parts thereof. It does not mandate specific information security controls.

The ISO 27001 standard is well established and internationally recognized for the management of information security. It has become the most widely adopted standard in the field of information security. A number of certification bodies are accredited by national standards bodies (such as the British Standards Institution and the National Institute of Science and Technology) to review compliance with ISO 27001 and issue certificates.

Your Microsoft Online Services purchases are protected by Payment Card Industry (PCI) Compliance.

Verizon Security Management Program – Service Provider Certification

Customers who are considering an online service need to have confidence that the claims the service provider makes are in fact implemented, in place, and working to help keep customer data safe.

The Microsoft Online Services environment has been certified by third-party independent audit standards supplied and performed by the Verizon Security Management Program (Service Provider Certification), formerly known as Cybertrust.

It is impossible to guarantee that a service is 100-percent secure, because threats develop and change over time; however, Microsoft tracks threats at a very aggressive level, with quarterly audits and monthly scans by internal security operations.

Current and Future State of Online Services Third-Party Certifications

The Microsoft third-party compliance strategy involves achieving ISO 27001 certification across all Microsoft Online Services.

To achieve that goal, Online Services started with ISO 27001 certification for the facility management and physical security of its data centers, as well as associated data center and infrastructure services. The Business Productivity Online Standard Suite services themselves currently either undergo SAS 70 assessment or maintain Verizon Security Management Program certification, both of which require that a subset of ISO controls be implemented and in operation.

In the future, Microsoft intends to undergo end-to-end ISO certification of the Online Services.

Further Information

For more information about topics raised in this white paper, visit the following links.

Microsoft Online Services

- Online Services from Microsoft (www.microsoft.com/online)
- About Microsoft Online Services (www.microsoft.com/resources/technet /en-us/MSOnline/Microsoft Online Services/html/99d9ede5-ce15-476c-9a3f-d42a481d287e.htm)
- Microsoft Solutions for Hosting Providers (www.microsoft.com/serviceproviders /hostingproviders.mspx)
- Microsoft Datacenters blog (blogs.technet.com/msdatacenters/)

Security and Service Continuity

- Microsoft Security Central (www.microsoft.com/security/default.mspx)
- Microsoft Operations Framework (www.microsoft.com/technet/solutionaccelerators /cits/mo/mof/default.mspx)
- Windows Server 2003 Security Services (www.microsoft.com /windowsserver2003/technologies/security/default.mspx)
- Microsoft Forefront™ (www.microsoft.com/forefront/default.mspx)
- Best Practices for Service Continuity (technet.microsoft.com/en-us/library /bb633282.aspx)

Privacy

- The Microsoft Trustworthy Computing Privacy Overview (www.microsoft.com /mscorp/twc/privacy/default.mspx)
- Microsoft Trustworthy Computing Security Development Lifecycle (msdn2.microsoft.com/en-us/library/ms995349.aspx)
- Microsoft Online Services Privacy Statement (go.microsoft.com/fwlink /?LinkId=143471)
- Privacy Guidelines for Developing Software Products and Services (go.microsoft.com /fwlink/?LinkId=143469)

Compliance

- Security Compliance Management Toolkit (www.microsoft.com/downloads /details.aspx?FamilyId=5534BEE1-3CAD-4BF0-B92B-A8E545573A3E&displaylang=en)