Microsoft Global Foundation Services

Information Security Management System for Microsoft Cloud Infrastructure

Online Services Security and Compliance

Published: November 2010

Table of Contents

Executive Summary

Organizations considering using cloud services face making a decision similar to the choice of outsourcing key services. Choosing to place information in the cloud requires an informed decision to transfer operational risk to the cloud provider. Meanwhile, risks to information security and concerns about privacy remain high on the list of issues cloud customers are evaluating. Unlike contracting with a payroll or software development firm, the business processes and standards for cloud services will continue to change for the near future. This flux is due to the relative newness of cloud business models and the ongoing revision of statutes and regulations that govern information security globally. Weighing the benefits and costs of operational risk transference involves closely reviewing trustworthiness of a cloud provider.

Although some change in information security requirements due to the advent of cloud computing was inevitable, a mature internationally recognized standard that details what a robust information security system looks like exists. Having such a program in place is the central element of establishing trust with customers and partners. The Online Services Security and Compliance (OSSC) Information Security Management System (ISMS) uses the ISO/IEC 27001:2005 *Information technology — Security techniques — Information security management systems — Requirements* (ISO/IEC 27001:2005) as its basis because it provided a well-established framework for integrating risk evaluation into the daily operations of running a cloud infrastructure. (For a copy of this standard, see http://www.iso.org.) The OSSC ISMS has been developed through many years of experience in online and traditional information systems with an ongoing focus on improving information security. Microsoft uses third parties to validate that the program is both relevant and effective. This validation from independent entities results in findings cloud customers can use while engaging in making an informed risk transference decision.

Since the launch of MSN network Internet services in 1994, Microsoft has been building and hosting familiar consumer-oriented services such as Windows Live Hotmail web-based email service and Bing search engine services, enterprise-oriented services such as Microsoft Dynamics CRM Online business software and Microsoft Business Productivity Online Standard Suite from Microsoft Online Services, and many behind-the-scenes services that handle online billing and advertising functions for Microsoft customers. Global Foundation Services (GFS) provides the cloud infrastructure for these services with a focus on adherence to numerous regulatory, statutory, and industry standards. The OSSC team within GFS fulfills its mission to provide trustworthy, available online businesses that create a competitive advantage for Microsoft by working with partners and other teams throughout the company to manage security risks to global online services at Microsoft.

Microsoft teams continue to improve the processes they use to identify, assess, and manage security risks with the objectives of increasing efficiency while responding to their customers' needs and to changing legal and industry requirements. The OSSC ISMS is how Microsoft operates its information security program for the Microsoft Cloud Infrastructure. This paper describes this program as well as some of the processes and benefits realized from operating this model, including an overview of the key certifications and attestations Microsoft maintains to prove to cloud customers that information security is central to Microsoft cloud operations.

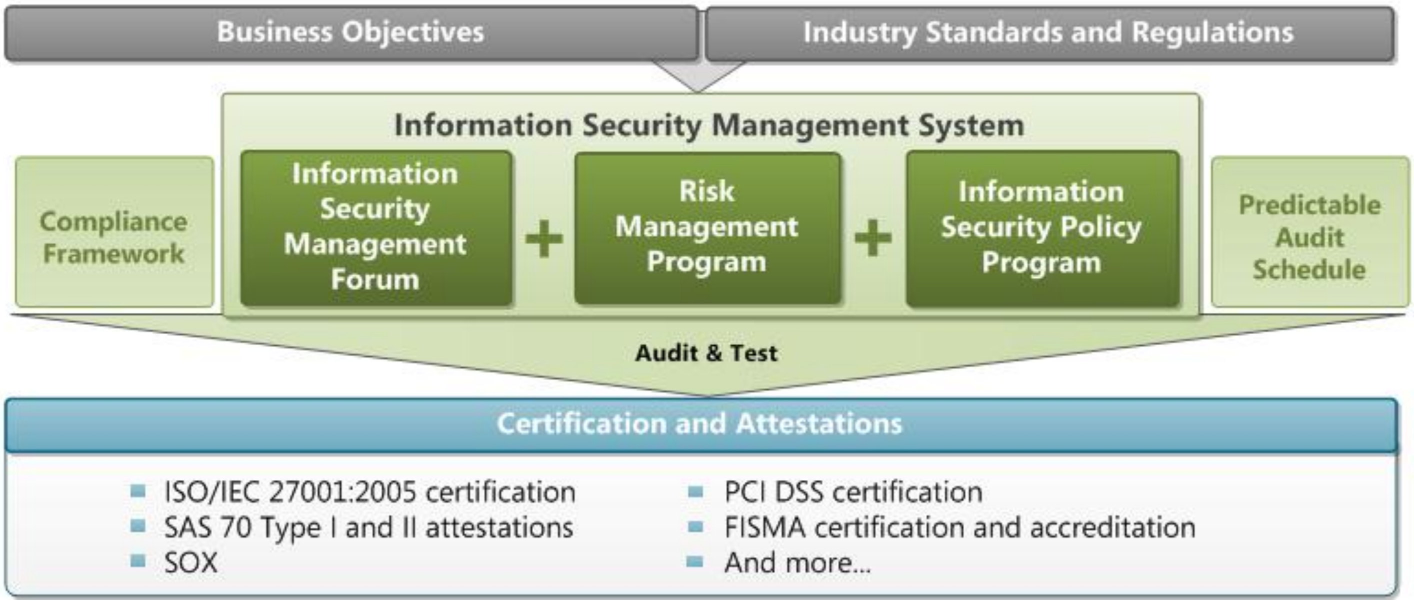
Information Security Management System

Several teams throughout Microsoft are involved in identifying risks to information security, developing policies to protect the infrastructure on which data is hosted and the networks through which it is accessed, and adapting existing policies and controls to address such risks. OSSC within GFS is responsible for coordinating these processes for the network, server, and data infrastructure upon which many well-known Microsoft services rely. Two previously published papers, Securing the Cloud Infrastructure at Microsoft and the Microsoft Compliance Framework for Online Services, introduced some of the teams and processes involved in managing information security at the infrastructure level of the Microsoft cloud. Where these papers described the comprehensive approach to information security and the framework for testing and monitoring the controls used to mitigate threats, this paper covers how the organization operates with an emphasis on these three key programs from the OSSC ISMS:

- **Information Security Management Forum** – A structured series of management meetings in specific categories for managing the ongoing operations of securing the cloud infrastructure.
- **Risk Management Program** – A sequence of processes for identifying, assessing, and treating information security risks and for enabling informed risk management decisions.
- **Information Security Policy Program** – A structured process for reviewing information security policy and for making changes when deemed necessary.

The ISMS components work in conjunction with each other and the framework outlined in the Microsoft Compliance Framework for Online Services paper (Compliance Framework). All of these information security processes can be more readily synchronized with each other because of having the ISMS. As shown in the following illustration, this approach also allows Microsoft to more efficiently and effectively operate in alignment with a variety of certification and attestation obligations, which include the following:

- ISO/IEC 27001:2005
- Statement on Auditing Standards No. 70 (SAS 70) Type I and II
- Sarbanes-Oxley (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Security Management Act (FISMA)


Business Objectives
Industry Standards and Regulations
Information Security Management System
Compliance Framework
Information Security Management Forum
+
Risk Management Program
+
Information Security Policy Program
Predictable Audit Schedule
Audit & Test
Certification and Attestations
ISO/IEC 27001:2005 certification
SAS 70 Type I and II attestations
SOX
PCI DSS certification
FISMA certification and accreditation
And more…

By combining the program elements of multiple regulations and compliance obligations into this singular OSSC ISMS program, the teams involved are able to improve their organization and focus. The results include more coordinated executive decision-making, policy analysis and revision with clear accountability for acceptance of exceptions, and rigorous compliance testing that ensures effectiveness of the controls in use. This level of maturity in information security management helps GFS to meet certification and attestation obligations. Being able to earn and maintain such credentials gives proof to cloud customers that Microsoft runs an effective information security program.

Continuing Challenges for Cloud Providers

Many experts in government and commerce still consider the greatest barrier to adoption of cloud services to be concerns about information security and privacy. While these risks exist across the entire cloud ecosystem, every cloud customer retains responsibility for assessing and understanding the value and sensitivity of the data they may choose to move to the cloud. As the owners of that information, cloud customers also remain accountable for decisions regarding the protection of that data wherever it may be stored. Organizations considering moving services to the cloud should keep these information security challenges in mind as they determine cloud adoption strategies:

- A growing interdependence amongst public and private sector entities and the people they serve continues to develop as government, industry, and commercial groups work to establish more widely accepted definitions of cloud computing. While those definitions and the associated standards continue to be created, one cloud requirement is clear—that platform services and hosted applications be secure and available.
- The cloud—however it is defined—is a dynamic hosting environment in which technologies and business models continue to evolve. This continuous change is a security challenge that cloud providers must address through an effective and dynamic security program.

- Sophisticated malicious attempts aimed at obtaining identities or blocking access to sensitive business data threaten to undermine the willingness of organizations to adopt cloud services. Cloud providers must prove that they have put into place and constantly evaluate the effectiveness of the technologies, controls, and processes used to mitigate such disruptions.
- In addition to these challenges, cloud providers must also address the myriad requirements related to delivering services globally online including those coming from governments, legal rulings, and industry standards.

In short, cloud service providers need to manage information security risks in a way that engenders trust with their customers—the government organizations or businesses that do provide such services to end users, as well as directly with end users.

Cloud customers, having decided to transfer some risk to a cloud provider by consuming a cloud service, should understand what their cloud provider has done and is doing to protect their information. OSSC completed a careful review of the existing information security regulations and standards while also considering the needs of Microsoft customers. A core set of certifications and attestations were selected and attained so that Microsoft could clearly communicate how it addresses operational information security for the Microsoft Cloud Infrastructure. The core set shown in the following table was chosen because they represent a broad set of requirements, many of which are internationally recognized, and that emphasize the need to continuously track and evaluate effectiveness of an overall information security program.

Industry Standards and Regulations	Description
ISO/IEC 27001:2005	Internationally recognized specification of standards for an ISMS that includes processes for examining, controlling, and managing threats to information security.
SAS 70 Type I and II	Standards used by auditors to evaluate and report on the controls (Type I) and the effectiveness of control activity over a period of time (Type II) for a service organization, including data hosting companies.
SOX	U.S. securities law that dictates specific requirements for financial reporting by public companies. The titles cover areas such as corporate responsibility, auditor independence, analyst conflicts of interest, and other subjects related to financial disclosures. The SOX program at Microsoft is based on the Control Objectives for Information and related Technology (COBIT) 4.1 framework.
PCI DSS	Security controls for credit card transactions.
FISMA	U.S. Federal law that mandates security standards for information technology systems in the federal government. The FISMA program at Microsoft is based on the National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*.

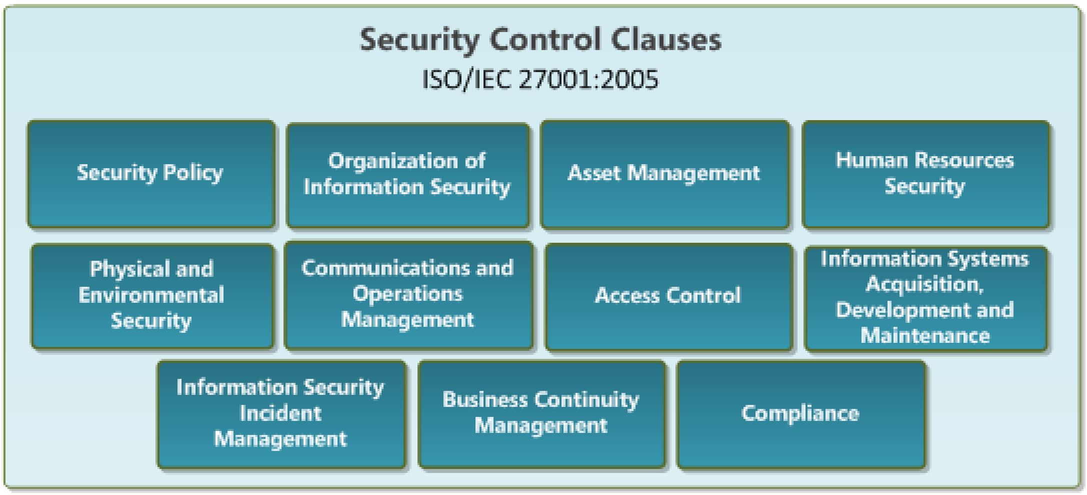
Microsoft has built a robust and responsive information security program by aligning to these standards and regulations. Cloud customers are able to rely on third-party validation of the effectiveness of the OSSC ISMS and therefore make informed risk transference decisions.

Alignment with Accepted Standard as a Solution

Addressing compliance is but one aspect of keeping information security central to conducting business. A successful information security program also:

- Incorporates risk-based decision-making processes into day-to-day business activities.
- Integrates information security into core IT and business practices.
- Ensures adequate resource allocation for the projects and programs designed to reduce risk.
- Dedicates resources to focus on key elements of the information security program.

OSSC introduced the ISMS into the existing information security program to increase efficiency and improve the ability to consistently repeat processes with greater clarity about responsibilities, improved internal coordination, and efficiency. The ISMS is aligned with the ISO 27001 security control clauses listed in the following table.



Security Control Clauses

ISO/IEC 27001:2005

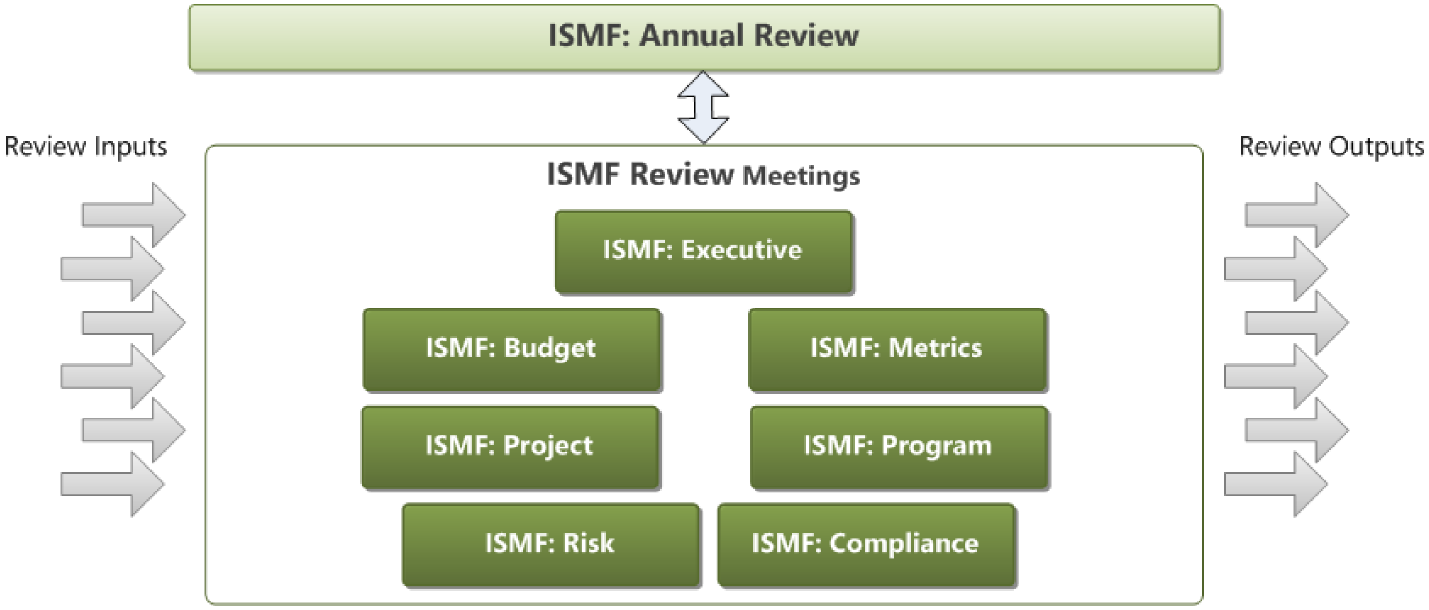
Security Policy	Organization of Information Security	Asset Management	Human Resources Security
Physical and Environmental Security	Communications and Operations Management	Access Control	Information Systems Acquisition, Development and Maintenance
Information Security Incident Management	Business Continuity Management	Compliance	

Aligning the ISMS program elements to the ISO 27001 security control clauses allows OSSC to more easily communicate security obligations and risk mitigation strategies to control owners and performers, as well as provide evidence to auditors and customers that Microsoft has a mature and rigorous program for managing information security, one that is continuously improving. Each ISMS area described in this paper also provides an efficient management context that allows GFS to adapt to changes in information security regulations and standards.

Information Security Management Forum

The Information Security Management Forum acts as the governance program within the GFS ISMS and is the mechanism by which the OSSC ISMS operates. As with the other programs in the ISMS, the Information Security Management Forum is organized to align with the ISO/IEC 27001:2005 standard. Applying the practices defined in ISO/IEC 27001:2005 enabled OSSC to consolidate and improve some information security governance efforts. The team also formalized certain aspects of this management meeting series in order to ensure the appropriate managers attend meetings for which they are responsible for providing a report or for which they hold decision-making authority. This formalization effort also entailed ensuring that the timing of meetings was in alignment with other business and compliance initiatives. Additional structure and tools were put in place so that decisions and issues are recorded and tracked to better facilitate follow-up discussion or to verify that specified actions were taken.

While relatively simple in concept, OSSC is reaping the benefits of having this more structured governance program in place. For example, the Information Security Management Forum framework makes aligning information security activities with new compliance obligations a more efficient process than before this program was formalized. Information Security Management Forum (ISMF) consists of a series of regular meetings designed to review key aspects of governance of the program.



Information Security Management Forum meetings follow a regular schedule designed to synchronize with the other business and compliance cycles to which GFS adheres. Certain meetings enable senior management to focus on long-term strategies while other meetings are intended to track and manage the shorter-term tactics being used to manage information security risks. The ISMF: Annual Review meeting includes internal customers as well as senior managers from specific teams in GFS and Microsoft who review the efficiency and effectiveness of the ISMS as a whole to ensure that the ISMS is meeting its intended purpose.

The following table provides additional details about the seven other types of review meetings in the Information Security Management Forum. Senior Information Security managers participate in each of these meetings with appropriate subject matter experts attending as appropriate or required.

ISMF Review Meetings	Frequency	Details
ISMF: Executive	Weekly	This meeting occurs weekly and involves reviewing major developments in other areas of Microsoft that may affect information security decision making.
ISMF: Budget	Monthly	This budgetary review meeting occurs monthly.
ISMF: Metrics	Monthly	This monthly review covers metrics to ensure controls are effective and to determine where processes within GFS should be improved.
ISMF: Project	Monthly	This meeting focuses on key projects that are underway to improve the overall security program, the tools that the program uses, or new projects intended to expand the program. For example, many of the tools that are used to support the program are implemented via defined projects.
ISMF: Program	Monthly	This set of meetings reviews the status of on-going operational programs that support the ISMS, for example, business continuity management, Online Services Security Training and Communications, and physical security.
ISMF: Risk	Quarterly	This meeting discusses key risk areas that may be discovered in a number of ways, including annual risk assessment, facility or data center risk assessments, new security incidents or vulnerabilities, and business impact assessments (as needed).
ISMF: Compliance	Monthly	A number of topics fall into this category: Policy Refresh (annual), Issue Review (monthly), Control Activity Refresh (quarterly), and Audits.

The inputs, discussions, and outputs from these meetings are used in a variety of other programs, such as the Risk Management Program, the Compliance Framework, and in the information security processes OSSC uses to track issues and policy exceptions. Many of the inputs to these reviews include details from the annual risk assessments and updates to the information security policy and standards, the other elements of the OSSC ISMS this paper describes.

Risk Management Program

Protecting the customer and maintaining the public trust while competing in business and addressing regulatory requirements drives the need to be agile with risk data. The Risk Management Program in GFS provides a structured approach to identifying, prioritizing, and directing risk management activities for the Microsoft Cloud Infrastructure. The methodology is based on the ISO/IEC 27001:2005 standard and National Institute of Standards and Technology (NIST) Special Publication 800-30 in support of Federal Information Security Management Act of 2002 (FISMA) standards.

The following critical information security risk management functions provided through the Risk Management Program are managed by OSSC for the Microsoft Cloud Infrastructure:

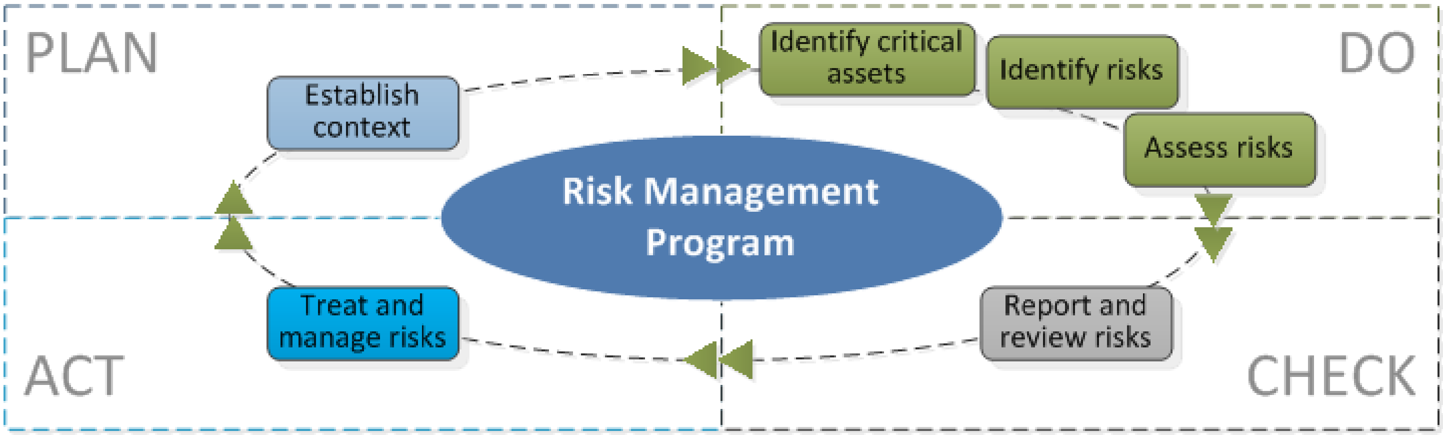
- Conduct risk assessment activities, including facilitation of business decision making with risk owners and business managers.
- Support the ISMS in order to help protect the confidentiality, integrity, and availability of sensitive information.
- Help protect the Microsoft Cloud Infrastructure and Microsoft from expensive and disruptive incidents by identifying and managing risks to the environment.
- Provide risk-ranking criteria that can be used by a variety of processes, such as policy exceptions and problem and issue management.

The Risk Management Program consists of six processes:

- **Establish context** – Setting the context or scope of the risk assessment includes establishing many characteristics before beginning the assessment in order to ensure appropriate data is collected and evaluated. The type of details captured while determining the assessment context include: the geographical locations of the information assets and equipment; how information is exchanged internally and with external parties; and what legal, regulatory, policy, and contractual requirements apply given the locations involved.
- **Identify critical assets** – Once the risk assessment context has been established, asset owners evaluate which assets are critical and which are not in a process that often reuses analyses conducted for asset management or business continuity planning efforts. The assets considered include:
    - **Primary assets** – Business processes, activities, and information.
    - **Supporting assets** – Hardware, software, network devices, personnel, and facilities.
- **Identify risks** – Workshops or interviews are used to solicit input from asset owners and business managers in teams that support the given scope of the assessment. Also, operational data is evaluated to identify risks.
- **Assess risks** – The potential business impact and the likelihood of their occurrence are investigated in this phase, which also includes looking for and estimating the effectiveness of potential controls that are used to reduce or eliminate the impact of risks.
- **Report and review risks** – Provide management with the data they need to make effective business decisions. This phase includes risk determination, including whether to take measures to avoid, reduce, transfer, or accept risks.

- **Treat and manage risks** – This phase involves identifying accountable risk owners and applying risk treatment plans to the risks that management decided to reduce, transfer, or avoid in the previous phase. Possible treatments include implementing special projects or other predefined controls intended to address those risks.

These processes support the information security policy statements and standards that are reviewed and modified through another ISMS program, the Information Security Policy Program. Those Information Security Policy Program documents define much of the context from which these Risk Management Program processes operate.



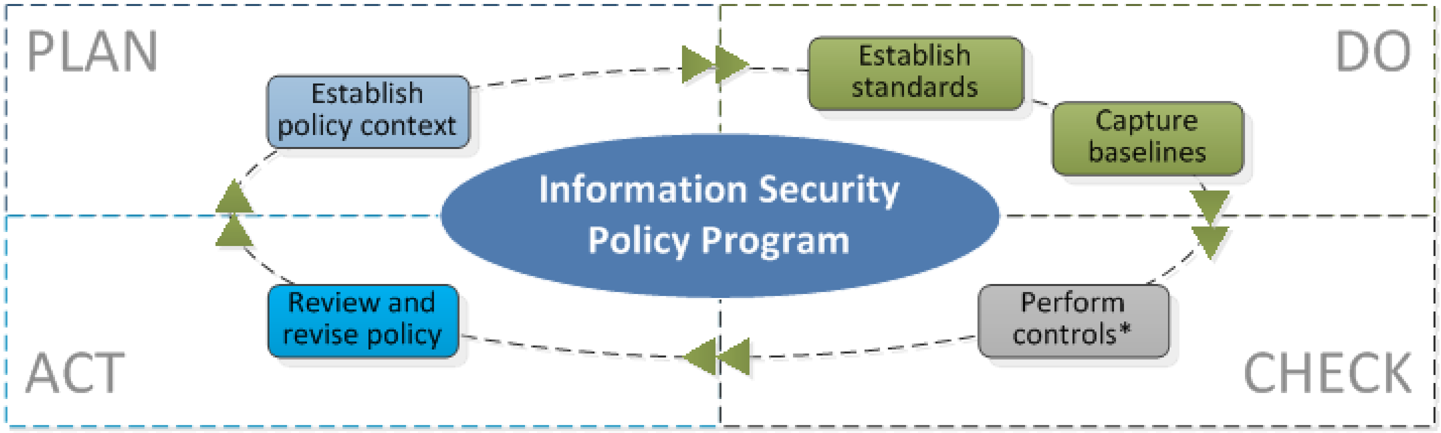
Of these processes, those involving risk review and treatment most directly provide inputs to the other ISMS programs. Risk remediation recommendations are reviewed by senior management in the ISMF: Risk meetings. Risk treatments may result in the addition of new control activities or updates to existing control activities while residual risks are again reviewed through the risk assessment process. The ongoing risk assessment work and the results of putting risk treatments into effect all feed into appropriate Information Security Management Forum program activity. For example, the ISMF: Metrics meeting may include reviewing the measured effects of treatments through an information security risk scorecard. The ISMF: Compliance meeting may entail validating that the control activities remain sufficient to address the identified regulatory or policy requirements. The overall effectiveness of the Risk Management Program is evaluated as needed in ISMF: Executive meetings and in the ISMF: Annual Review. Elements of this formalized risk program are included in all aspects of the OSSC ISMS decision-making process.

Information Security Policy Program

The Information Security Policy Program uses the ISO/IEC 27001:2005 domains as an organizing concept for developing the information security standards, baselines, and policies. The policy review process includes stakeholders from teams within Microsoft that consume Microsoft Cloud Infrastructure services, as well as managers from teams internal to the GFS division. The inclusion of stakeholders from these member organizations in this process has engendered more effective adoption of information security policy for online services.

Policy exceptions may be granted based on review of requests submitted by the member organizations. Such exceptions, if made, are reviewed by the security team to evaluate the risks that they may present. These already identified risks undergo the assessment and review process specified in the Risk Management Program. Appropriate risk treatments identified in those reviews are suggested to management, who then decide whether to grant the requested exception. Once granted, the approval and authorization is documented and recorded. Policy exceptions are then tracked and reviewed in the relevant Information Security Management Forum meetings.

Policies, standards, and baselines are reviewed on an annual basis. Changes to business or regulatory requirements, emerging technologies, or responses to security incidents or newly identified threats may also result in ad hoc reviews and updates of the Information Security Policy Program components.



*Through Compliance Program activities

The recommendations that result from this review process are in turn reviewed in the ISMF: Annual Review. If circumstances warrant ad hoc updates to information security policy, decisions to modify policy would happen as part of one of the ISMF: Executive review meetings.

Conclusion

The fundamental problem for cloud customers is to decide whether transferring risk outside of the organization to a cloud service provider is the right choice. The outsourcing of specific tasks or projects to vendors is one example of where the process of determining whether to transfer risk has become a standard business practice. Standard contractual terms and conditions exist, and mechanisms to verify security claims of an outsource provider are part of routine business practices. Cloud computing lacks established practices for efficient supplier and customer understanding and for risk transference. The same types of capabilities need to be developed for the cloud ecosystem. While the cloud industry develops and matures, having an information security program such as the OSSC ISMS as described in this paper along with third-party validation provides cloud customers the independently verified findings they need to make informed decisions.

Microsoft, with its continuing focus on trustworthy computing and information security, has built its OSSC ISMS on what many consider to be the broadest, most comprehensive, and best recognized definition of an information security program—that found in ISO/IEC 27001:2005. Microsoft uses a core set of certifications and attestations to demonstrate that the OSSC ISMS programs, including those defined in this and previous GFS white papers, continue to be effective and that they remain relevant in the still-changing realm of cloud computing. Customers and partners who seek to establish a baseline for establishing trust would do well to consider how to infuse information security into their daily operations, and may want to use a similar strategy by developing an ISMS of their own.

Additional Resources

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

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

The Microsoft Security Development Lifecycle (SDL): http://www.microsoft.com/security/sdl/

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

International Organization for Standardization: http://www.iso.org

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

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

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

Disclaimer

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.