Information Security Management System for Microsoft's Cloud Infrastructure

Online Services Security and Compliance

Contents

Executive summary 1
Information Security Management System (ISMS) 3
Continuing challenges for cloud service providers 4
Alignment with accepted standards as a solution 7
Information Security Management Forum (ISMF) 9
Risk Management Program 11
Information Security Policy Program (ISPP) 14
Conclusion 16
Additional resources 17

Executive summary

This paper describes the Microsoft Cloud Infrastructure and Operations (MCIO) Information Security Management System (ISMS) program and some of the processes and benefits realized from operating this model. It includes an overview of the key certifications and attestations Microsoft maintains to demonstrate to cloud customers that information security is central to Microsoft's cloud operations.

Microsoft's Cloud Infrastructure and Operations organization delivers the infrastructure and network for over 200 consumer and enterprise cloud services. The Online Services Security and Compliance (OSSC) team within MCIO manages the ISMS and was created to ensure that our cloud services are secure, meet the privacy requirements of our customers, and comply with complex global regulatory requirements and industry standards.

While many of the ISMS capabilities must be provided at the service application layer, all services have some level of dependency on the cloud infrastructure (datacenters and networks).

The ISMS is based on the *ISO/IEC 27001 Information Technology Security Techniques Information Security Management Systems Requirements*, which provides a well-established framework for integrating risk evaluation into the daily operations of running a cloud infrastructure.

It was developed through more than two decades of experience in delivering online and traditional information systems and is used to drive continual improvement and risk-informed decision making. Microsoft uses third party auditors to validate that the ISMS program is both relevant and effective.

Organizations who are considering using a cloud service provider face making a decision similar to the choice of outsourcing key services, such as payroll or retirement programs. Choosing to place information in the cloud

requires an informed decision to transfer operational risk to the cloud provider.

Weighing the benefits and costs of transferring operational risk involves closely reviewing the trustworthiness of cloud service providers. Risks to information security and concerns about privacy remain high on the list of issues cloud customers are evaluating. Microsoft has designed its cloud infrastructure ISMS to both effectively manage its cloud infrastructure security program and to be relied upon by customers as part of establishing confidence in transferring operational risk.

For more information on our cloud infrastructure's security, privacy, and compliance strategies, please visit our web site at http://www.microsoft.com/datacenters. There you will find a number of videos, white papers, and strategy briefs covering these topics.

Information Security Management System (ISMS)

A number of teams across Microsoft contribute to identifying information security risks, developing policies to protect the infrastructure on which data is hosted and accessed, and revising policies and controls to address such risks. This results in an informed set of risks, policies, and decisions that form the core competency of the Microsoft ISMS.

The OSSC team is responsible for coordinating these processes for Microsoft's cloud infrastructure, and operates three key programs as part of the ISMS:

- *Information Security Management Forum* – A structured series of management meetings in specific categories which conduct 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 maintaining information security policy and for making changes when deemed necessary.

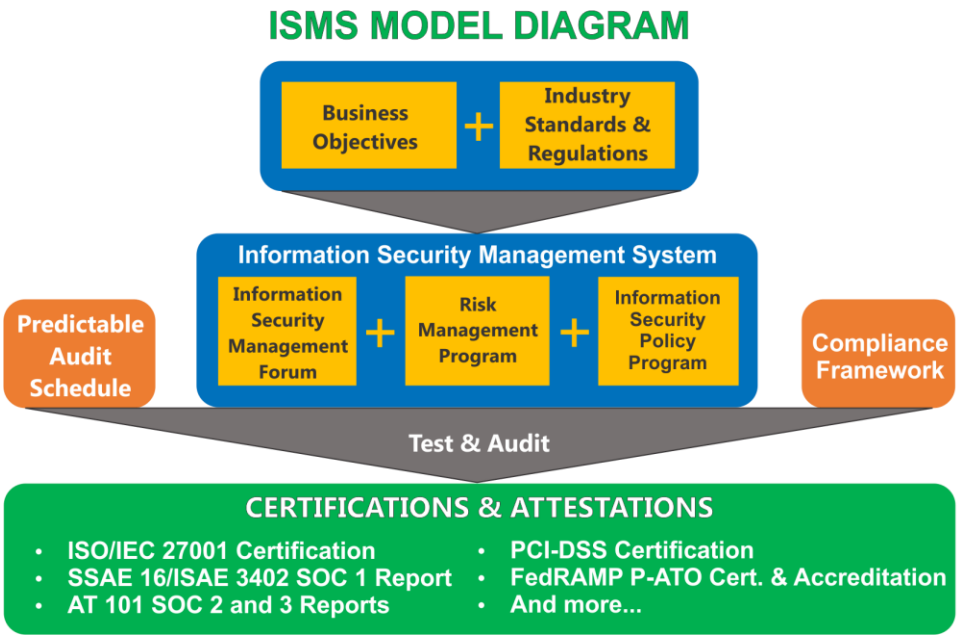
These ISMS programs work in conjunction with each other as well as broader security and compliance initiatives. For a description of Microsoft's comprehensive approach to cloud infrastructure information security, the framework for testing and monitoring the controls used to mitigate threats, and the teams and processes involved, please refer to two other published papers, *Securing Microsoft's Cloud Infrastructure* and *Microsoft's Compliance Framework for Online Services*[1].

The ISMS allows these information security processes to be more readily synchronized with each other. And, as shown in the following illustration, this approach allows Microsoft to more efficiently and effectively operate in alignment with a variety of certification and attestation obligations, including:

- *International Standards Organization 27001 (ISO/IEC 27001)*
- *Service Organization Controls (SOC) Reports (1-3)*
- *Sarbanes-Oxley (SOX)*

[1] These 2 papers can be found at www.microsoft.com by searching for them by name.

- *Payment Card Industry - Data Security Standard (PCI - DSS)*
- *Federal Risk and Authorization Management Program (FedRAMP)*



By combining the program elements of multiple regulations and compliance obligations into this singular *ISMS* program, the teams involved are able to improve their organizational processes 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 Microsoft meet certification and attestation obligations for its cloud infrastructure. Being able to earn and maintain such credentials gives proof to our cloud customers that Microsoft runs an effective information security program.

Continuing challenges for cloud service providers

Many leaders in government and enterprises consider the greatest barrier to adoption of cloud services to be concerns about information security, privacy, and reliability. While these risks exist across the entire cloud ecosystem, end-to-end risk of adopting cloud services must be evaluated. A critical aspect of this is the fact that every cloud customer retains responsibility for assessing and understanding the value and sensitivity of the data they may choose to move to the cloud. This allows evaluations of

cloud service providers to be based on the specific needs of the data and processes being considered for cloud adoption. Organizations considering moving services to the cloud should keep the following information security challenges in mind as they determine cloud adoption strategies:

- **Growing interdependence amongst cloud providers and customers.** The business operations of cloud customers have become more dependent on cloud service providers and a disruption of a cloud service can prevent a business from operating. With these new dependencies come mutual expectations that services and hosted applications are secure and available.
    - Microsoft's infrastructure and services are built to be resilient and capabilities are regularly tested. In addition, Microsoft provides guidance on how to use services in a way to meet resiliency goals
- **Complex global regulatory requirements and industry standards influence the ability of enterprises and public sector organizations to meet their compliance needs while using cloud services,** as well as the ability of cloud service providers to meet these requirements. Additionally, countries and regions pass laws that govern the provision and use of online environments which can be inconsistent with each other.
    - Microsoft must be able to comply with many regulatory and industry obligations because Microsoft's cloud services are adopted by many industries around the world. Microsoft's compliance programs as well as its ability to share third party reviews of its capabilities are key to meeting this challenge.
- **Evolving technologies, massive scale, changing business models, and dynamic hosting environments all represent challenges to security and compliance.** The scale and continuing growth of the online cloud service environment requires Microsoft to rely heavily on automation. New technologies requires creating new types of security controls.
    - Microsoft's Information Security Program maintains strong internal partnerships among security, product, and service delivery teams. This allows them to meet current needs while continually building capabilities for future needs.
- **Continuous and increasing sophistication of attacks are a challenge for everyone using and offering online and cloud services.** Traditional

attacks continue while new attacks challenge traditional security practices.

- Microsoft brings together research, development, operations and response teams to protect its customers from criminal and unlawful attacks and intrusions. They work with industry partners, peers and research organizations to understand and respond to the evolving threat landscape. They also share recommended practices with consumers of cloud services so they too can take action to protect themselves.

To summarize, cloud consumers need to rely on and trust the capabilities of cloud service providers and cloud service providers need to manage information security risks in a way that creates trust with customers.

Cloud customers, having decided to transfer some risk to a cloud provider by consuming a cloud service, should understand what the cloud provider has done and is doing to protect customer 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 has been chosen because they represent a broad set of requirements, many of which are internationally recognized, and emphasize the need to continuously track and evaluate effectiveness of an overall information security program.

Industry Standards and Regulations	Description
ISO/IEC 27001	Internationally recognized specification of standards for an ISMS that includes processes for examining, controlling, and managing threats to information security.
SSAE 16/ ISAE 3402 SOC 1 Report **AT 101 SOC 2, and 3 Reports**	The SOC attestation reports provide user entities and their auditors a third party opinion on the design and operational effectiveness of a service organization's control environment. The SOC 1 report focuses on controls relevant to financial reporting while the SOC 2 and SOC 3 reports are specific to Trust Services Principles (security, availability, integrity, confidentiality, and privacy). Given MCIO's role as an infrastructure provider that does not handle data, the two principles applicable to MCIO are security and availability.
SOX	U.S. securities law 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.
PCI-DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
FedRAMP	The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The FedRAMP program at Microsoft is based on the National Institute of Standards and Technology Special Publication 800-53, '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 transfer decisions.

Alignment with accepted standards as a solution

Addressing compliance is 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 technology 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 relies on its ISMS to increase efficiency and improve the ability to consistently repeat processes with greater clarity about responsibilities, and improved internal coordination. The OSSC ISMS is aligned with the current version of the *ISO 27001 Security Control Domains* shown in the diagram below.

Aligning the ISMS program elements to the ISO 27001 security control domains allows OSSC to clearly 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. Each ISMS area described in this paper also provides management context that allows Microsoft's cloud infrastructure teams to adapt to changes in information security regulations and standards.

Information Security Management Forum (ISMF)

The Information Security Management Forum (ISMF) acts as the governance program within the ISMS and is the mechanism by which the ISMS operates. As with the other programs in the ISMS, the ISMF is organized to align with the ISO/IEC 27001 standard. Applying the practices defined in ISO/IEC 27001 enables Microsoft's cloud infrastructure teams to consolidate and improve information security governance efforts.

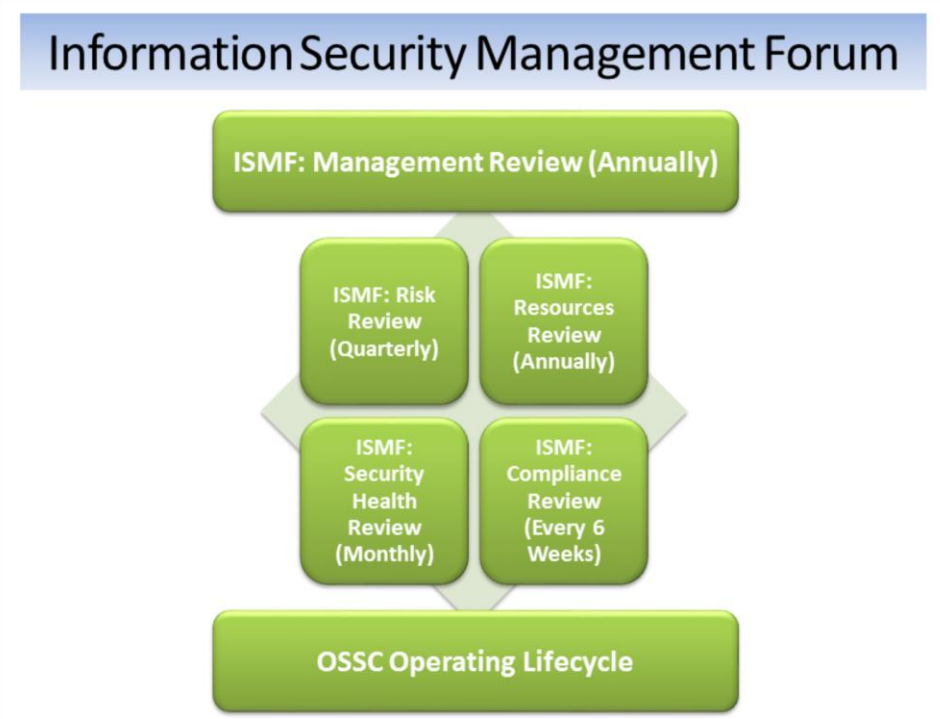
The ISMF consists of a series of regular management meetings scheduled throughout the year that are designed to review key aspects of program governance.

Certain meetings enable senior management to focus on long-term strategies while other meetings address the short-term tactics being used to manage information security risks.

Elements of these meeting series have been formalized to ensure attendance by the appropriate managers and service owners, particularly when they are responsible for providing a report or hold decision-making authority. For example, Senior Information Security managers participate in each of these meetings with appropriate subject matter experts attending as required.

Additional structure and tools have been established so decisions and issues are recorded and tracked to better facilitate follow-up discussions and to verify specified actions were taken.

The ISMF: Management Review meeting includes internal customers as well as senior managers from specific teams in MCIO and Microsoft who review the efficiency and effectiveness of the ISMS as a whole to ensure that the ISMS is meeting its intended purpose.



While relatively simple in concept, having a structured governance program in place provides many benefits to Microsoft's cloud infrastructure teams. For example, the ISMF framework makes aligning information security activities with new compliance obligations a more efficient process. Additionally, the ISMF meetings schedule is designed to synchronize with the other business and compliance cycles to which the teams adhere.

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 other elements of the ISMS that this paper describes, such as the *information security policy and standards*.
The following table provides additional details about the types of review meetings in the ISMF:

ISMF Review Meetings	Frequency	Details
ISMF: Management	Annually	The Management Review evaluates results and inputs from internal and external sources, including review of major

		developments in other areas of Microsoft that may affect information security decision making, to ensure continual improvement of the ISMS, operating effectiveness, and progress toward meeting business and security objectives.
ISMF: Resources	Annually	The Resources Review examines the current financial position of the ISMS to ensure the balance and application of resources is appropriate to meet operational requirements and implement risk treatment plans.
ISMF: Security Health	Monthly	The Security Health Review includes MCIO security leadership oversight and evaluates results of security monitoring processes to ensure prompt detection of events or errors and determine appropriate responsive actions.
ISMF: Risk	Quarterly	The Risk Review appraises the risk posture and security issues across the ISMS environment that may be discovered in a number of ways, including annual risk assessment, facility or datacenter risk assessments, new security incidents or vulnerabilities, and business impact assessments.
ISMF: Compliance	Bi-Monthly	A number of topics fall into this category: Policy Refresh (annual), Issue Review (monthly), Control Activity Refresh (quarterly), and Audits.

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 MCIO 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 27005: Information Security Risk Management standard and National Institute of Standards and Technology (NIST) Special Publication 800-53 in support of government requirements such as the Federal Risk and Authorization Management Program (FedRAMP).

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

1) **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.
2) **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:
    a. ***Primary assets*** – Business processes, activities, and information.
    b. ***Supporting assets*** – Hardware, software, network devices, personnel, and facilities.
3) **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.
4) **Assess risks** – The potential business impact and the likelihood of 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.
5) **Report and review risks** – Provide management with the data to make effective business decisions. This phase includes risk determination,

including whether to take measures to avoid, reduce, transfer, or accept risks.

6) **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 authorizing special projects 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: Security Health 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

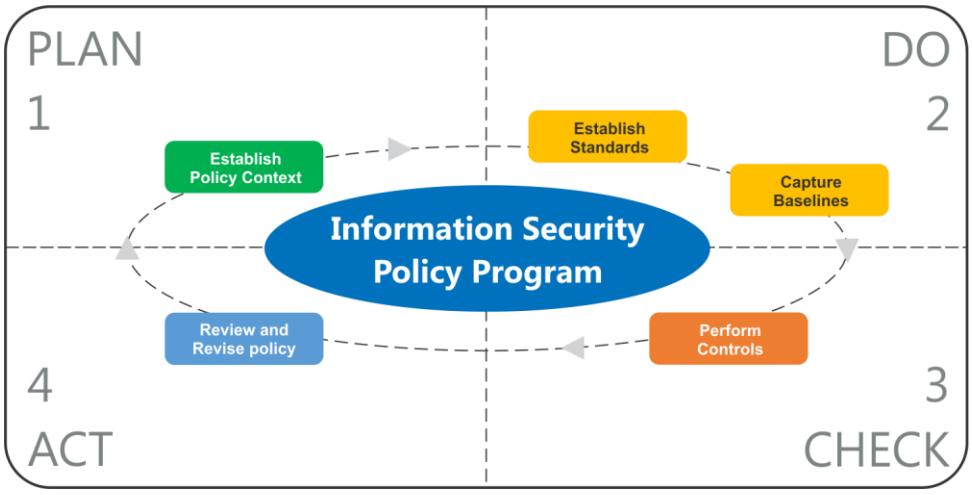
policy requirements. The overall effectiveness of the *Risk Management Program* is evaluated as needed in the ISMF: Management Review. Elements of this formalized risk program are included in all aspects of the OSSC ISMS decision-making process.

Information Security Policy Program (ISPP)

The Information Security Policy Program uses the ISO/IEC 27001 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 the cloud infrastructure teams providing them. The inclusion of stakeholders from these member organizations in this process has prompted more effective adoption of the Information Security Policy.

Policy exceptions may be granted based on review of requests. Exception requests 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.



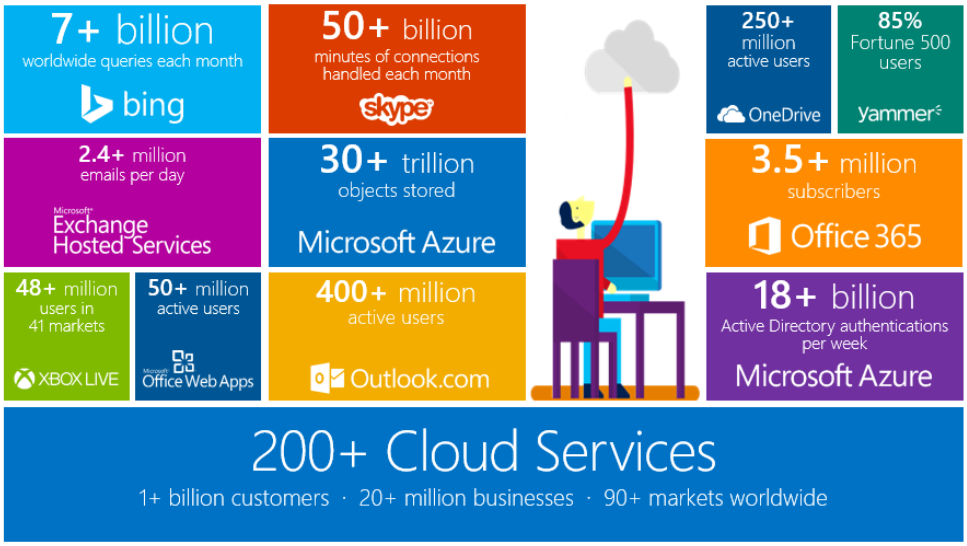
The recommendations that result from this review process are in turn reviewed in the ISMF: Management Review. If circumstances warrant, incidental changes would be reviewed in an ad-hoc meeting with policy approvers, in accordance with the approved SOP for policy management. Updates to the Information Security Policy, and decisions to modify the policy would happen as part of one of the ISMF: Management meetings.

Conclusion

One of the challenges posed by the cloud is the need of cloud consumers to rely on the capabilities of cloud providers. The 200+ cloud and online services that Microsoft offers to its 1 billion+ customers are delivered in over 90+ markets worldwide. Those services are required to meet many government and industry-mandated security requirements as well as the customer expectations.

Microsoft operates a comprehensive compliance program to demonstrate that these expectations are met. Microsoft also maintains a set of certifications, attestations and compliance capabilities that are validated by third-party auditors. The results of these third-party audits are shared with customers and are an important element in establishing trust, reliance and transparency of Microsoft's cloud services.

Microsoft will continue to address current and evolving risks and provide the information customers need to manage those risks and to have confidence in Microsoft as a cloud service provider wherever Microsoft stores its customer's data.



Additional resources

Microsoft Cloud Infrastructure and Operations homepage: http://www.microsoft.com/datacenters

Microsoft FedRAMP ATO: http://cloud.cio.gov/fedramp/microsoft

Microsoft Cloud Infrastructure and Operations ISO 27001 certificate on the BSI registry (certificate # 533913): http://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=licence%3d533913%26company%3dMicrosoft&licencenumber=IS 533913

Microsoft Cloud Infrastructure and Operations ISO 27001 certificate on the BSI registry for Leased Datacenter Sites (certificate # 587621): http://www.bsigroup.com/en-US/Our-services/Certification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=company%3dMicrosoft&licencenumber=IS 587621

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

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

Microsoft Security Development Lifecycle (SDL) – version 5.2, process guidance: http://msdn.microsoft.com/en-us/library/84aed186-1d75-4366-8e61-8d258746bopq.aspx

Microsoft SDL Threat Modeling Tool: http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx

Cloud Security Alliance: https://cloudsecurityalliance.org/