Microsoft's Compliance Framework for Online Services

Online Services Security and Compliance

Executive summary

This paper introduces the Microsoft Compliance Framework which is used to manage its online services cloud infrastructure. It provides examples of how to define compliance domains and apply control objectives to meet the needs of industry standards, regulatory requirements and business decisions. This paper also provides readers with an understanding of how the framework more efficiently utilizes staff and resources, and establishes and maintains online services compliance.

Contents

Microsoft relies on its service delivery and operations teams to adapt their compliance programs to satisfy a variety of audits and attestations. The teams must ensure coverage of complex requirement sets and manage frequent changes which result from the changing landscape of regulations, statutes, standards, and industry best practices for online services.

In particular, Microsoft's Cloud Infrastructure and Operations (MCIO) organization is subject to a large number of compliance obligations as they provide the base online infrastructure for all Microsoft online and cloud services which includes datacenters, networking, operations and tooling. Many of the more than 200 Microsoft online and cloud services must meet compliance needs that include healthcare regulations, regional privacy laws, credit card industry processing mandates, and government standards. These compliance requirements typically specify capabilities at this base infrastructure layer.

Before a compliance framework was established, requests for the same types of information were made repeatedly over the course of a year from multiple teams to satisfy audits from various external auditors. Internal teams and partners would also ask about compliance with various regulations, statutes, and industry standards while responding to inquiries from customers and prospects.

Microsoft's Online Services Security and Compliance (OSSC) team, part of the MCIO division, responded to the need to reduce the impact on the operations teams by developing a centralized approach to preparing for and undergoing audits. Specific goals consisted of increasing efficiencies in preparing for such reviews by consolidating requests made to operations staff, automating workflow between operations staff and compliance teams, and streamlining the process of providing the required operational details to auditors and other stakeholders. Microsoft's Compliance Framework for Online Services was developed to address this need.

The Microsoft Compliance Framework includes a standard methodology for defining compliance domains, determining which objectives apply to a given team or asset, and capturing how domain control objectives are addressed in sufficient detail as they apply to a given set of industry standards, regulations or business requirements.

In addition to ensuring that compliance expectations are continually achieved, applying the Compliance Framework has helped SOC 1 (SSAE16/ISAE3402) and SOC 2 (AT101) Type 2 attestations; to attain International Organization for Standardization / International Electro-technical Commission 27001 (ISO/IEC 27001) certification; to attain an Authorization to Operate (ATO) from the Federal Risk Authorization and Management Program (FedRAMP); to produce a Report on Compliance (ROC) for the Payment Card Industry Data Security Standard (PCI-DSS) and to more efficiently pass various audits from independent third parties.

The Compliance Framework for Online Services allows Microsoft to have a clear understanding of the control activities that cloud infrastructure teams must operate, the reason behind each control activity (i.e., the specific clause from a requirements document such as SOC 2 or the specific element of security policy that drives the need to perform the control activity) as well as a number of other metadata mappings that allow Microsoft to effectively and efficiently manage its program. The compliance program also includes both self-reviews performed by Microsoft teams and third-party reviews of the overall Information Security Management System and performance against the control framework. The third parties that conduct the regular audits of the cloud infrastructure environment provide a scalable mechanism for Microsoft to communicate the capabilities of its online and cloud infrastructure to their customers and partners.

This Compliance Framework model is extended to Microsoft's consumer and enterprise services, allowing for trusted third parties to examine relevant service elements and provide in-depth reviews of targeted services such as Office 365 and Microsoft Azure. The independent assessments are logically stacked upon one another to reflect dependencies and are shared with customers and partners. This allows capabilities to be examined for each Microsoft service that cover the entire capability stack from the datacenter all the way to the application layer.

The approach Microsoft takes to managing its compliance program and control framework is necessary to meet the complex and changing requirements associated with operating online and cloud services. It also provides visibility into the overlapping and sometimes conflicting requirements that must be met to operate and use a cloud service.

The Compliance Framework allows Microsoft to effectively and efficiently manage the multitude of compliance programs. With the appropriate governance oversight, it allows Microsoft teams to demonstrate that they meet the compliance requirements associated with specific business functions in a scalable way.

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.

The changing landscape for online services compliance

Any company offering online services will find its operations must comply with certain regulations or statutes. The laws and requirements which apply depend on the unique circumstances of a business, such as the types of data the company processes, where the company's datacenters are located, and rules pertaining to the privacy of personally identifiable information for the countries in which its customers are located. In addition, numerous industry standards exist that were developed to ensure the integrity of data and data collection methods, the privacy of customer data, and the validity of details analyzed for the various reports businesses produce, especially financial reports from publicly held companies.

The cloud infrastructure for online services at Microsoft must meet a significant number of these government-mandated, internally derived and industry best practice security requirements. Administrative and technical controls that ensure these requirements are met require a periodic review to validate that compliance is being maintained. These reviews often occur more than once per year because the standards apply to multiple services or business units.

The following table provides an overview of some of the compliance regulations Microsoft must address.

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'.

How Microsoft dealt with online services audits before the compliance framework

Initially, Microsoft teams met compliance expectations on a service-by-service basis. For example, although a SOX audit only needs to happen once per year, Microsoft experienced multiple SOX audits in a given year, one for each online service, financial accounting, and reporting system that needed to demonstrate SOX compliance. Each audit conducted as its own effort was mostly in isolation from any others that may have been happening at nearly the same time. These disconnected projects resulted in numerous solutions and redundant work performed by many employees.

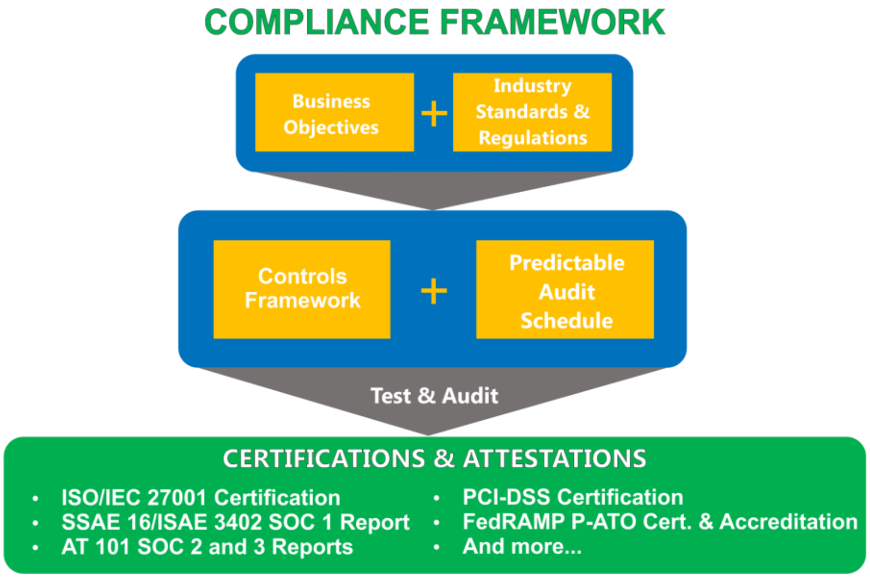
When Microsoft looked at the work involved in successfully completing compliance reviews with a focus on the teams involved, a different story emerged: many of the same staff members were called upon to provide similar information for every audit. These employees participated in numerous consecutive audits or, worse yet, multiple concurrent audits, each managed as a discrete effort. For example, in one year the same team would be approached multiple times for information pertaining to a given audit with requests for slightly different operational details often happening nearly simultaneously. Unanticipated and unnecessary costs, overutilization of certain teams, and disruption to operational and development plans were some examples of the problems with continuing to treat each audit separately.

Furthermore, it was recognized that the operational environment for online services would continue to grow in size and complexity as many of the company's plans to launch new products and services into the Microsoft cloud came to fruition. Essentially, the compliance and operations teams were being asked to adhere to more requirements with the same number of staff resources. A significant gap was developing between the capacities of existing staff to fulfill meeting these changing demands and an increasingly complex compliance workload was growing larger. Microsoft sought another way to address this gap.

Microsoft's Compliance Framework for Online Services

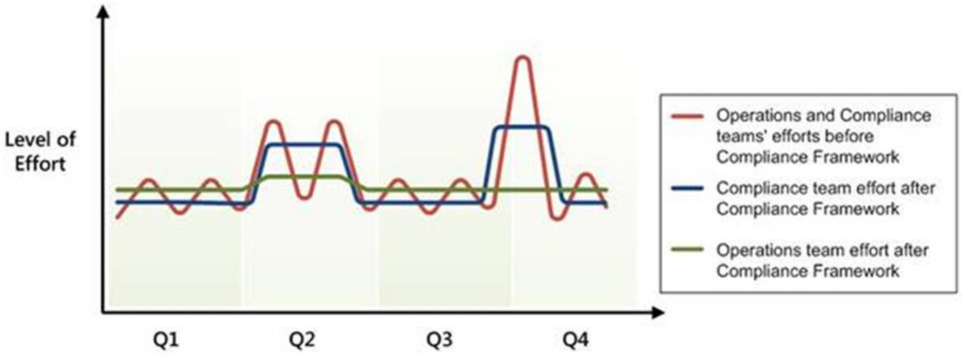
By analyzing how reacting to individual audits as discrete efforts undermined the productivity of operations and audits team, and by working with the teams most frequently impacted by these efforts, OSSC identified an opportunity to reduce redundancy and proposed a solution to streamline processes and to manage compliance expectations in a more comprehensive manner. This evaluation of how Microsoft responded to audits also uncovered the prospect of providing a higher level of confidence to customers that Microsoft meets compliance obligations in a highly effective manner. Using the Compliance Framework enables Microsoft to achieve and maintain compliance within the context of the company's many business commitments.

The Compliance Framework resulted from those efforts. As shown in the following illustration, it provides the controls framework and the process methodology now in use to create new efficiencies in responding to and successfully completing compliance reviews or audits.


COMPLIANCE FRAMEWORK
Business Objectives
+
Industry Standards & Regulations
Controls Framework
+
Predictable Audit Schedule
Test & Audit
CERTIFICATIONS & ATTESTATIONS
• ISO/IEC 27001 Certification
• SSAE 16/ISAE 3402 SOC 1 Report
• AT 101 SOC 2 and 3 Reports
• PCI-DSS Certification
• FedRAMP P-ATO Cert. & Accreditation
• And more...

The Compliance Framework is a continuous, scalable program that ensures Microsoft is meeting security requirements and that the Online Services Information Security Program, policy, standards, and associated controls and processes remain current as compliance requirements change. Combining control objectives with a comprehensive process for audit coordination has allowed Microsoft to use the Compliance Framework to streamline reviews of cloud infrastructure and operations teams as well as service delivery teams and hosted applications. One of the successes of having implemented the Compliance Framework is that Microsoft's cloud infrastructure has efficiently achieved and maintained a number of attestations and certifications.

The following illustration shows an approximation of when the compliance workload would spike in a typical year before the implementation of the Compliance Framework at Microsoft in comparison with how the workload has become more predictable and balanced for operations and compliance teams since.



Online Services Security and Compliance team (OSSC)

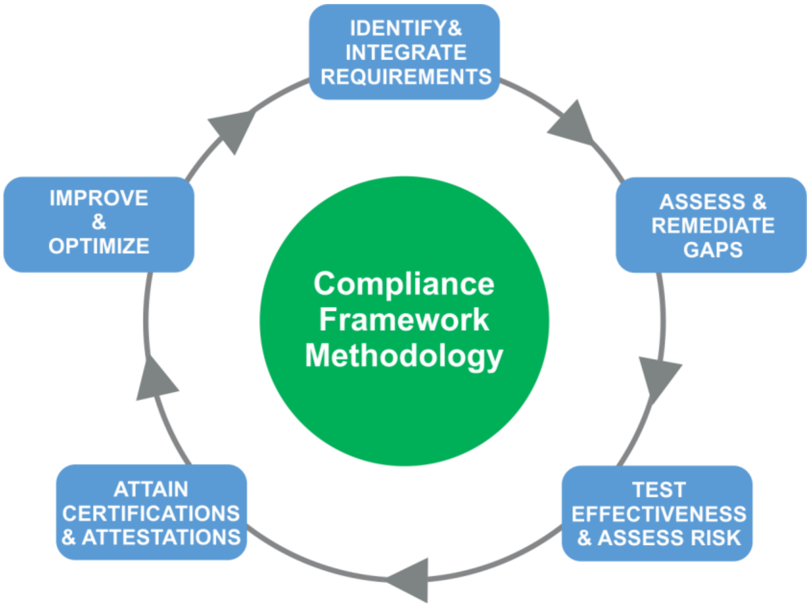
The OSSC team within MCIO is responsible for the Microsoft cloud infrastructure Information Security Program, including policies and programs used to manage online security risks. Microsoft's use of a common infrastructure for all online and cloud services allows each of the Microsoft service teams to focus on the unique security needs of their service and customers while relying on MCIO and OSSC to manage infrastructure requirements.

The OSSC team drives the effort to provide a trustworthy experience in the Microsoft cloud through the Microsoft Information Security Program using a risk-based operating model and a defense-in-depth approach to controls. This includes the development and maintenance of the Compliance Framework through which the team applies best practice processes, including a variety of internal and external reviews throughout the lifecycle of online services and to each element in the infrastructure. Auditable requirements come from government and industry mandates, internal policies, and industry best practices. The Compliance Framework ensures that these compliance expectations are continuously evaluated and incorporated.

Online services compliance process

The Compliance Framework methodology is based on the "Plan, Do, Check, Act" process outlined in the ISO/IEC 27001 standard. Although the standard no longer prescribes this process it is still a suitable approach to pursue. With a continuing emphasis on optimization, Microsoft is using this methodology to extend use of the Compliance Framework from the MCIO infrastructure into product and service delivery groups who offer online services within the Microsoft hosting environment.

The following illustration shows the Compliance Framework methodology.


Compliance Framework Methodology
IDENTIFY& INTEGRATE REQUIREMENTS
ASSESS & REMEDIATE GAPS
TEST EFFECTIVENESS & ASSESS RISK
ATTAIN CERTIFICATIONS & ATTESTATIONS
IMPROVE & OPTIMIZE

- **Identify and integrate requirements** – Scope and applicable controls are defined. Standard Operating Procedures (SOP) and process documents are gathered and reviewed. This aligns with the "**Plan**" phase.
- **Assess and remediate gaps** – Gaps in process or technology controls are identified and remediated. This includes implementing new administrative and technical controls and aligns with the "**Do**" phase.
- **Test effectiveness and assess risk** – Effectiveness of controls is measured and reported. On a consistent and regular basis, independent internal audit groups and external assessors review internal controls. Compliance with internal security standards and requirements, such as verification that product groups are adhering to the Microsoft Security Development Lifecycle (SDL), occurs in this phase. This aligns with the "**Check**" phase.
- **Attain certification and attestations** – Engagement with third-party certification authorities and auditors occurs. This aligns with the "**Act**" phase.
- **Improve and optimize** – If issues or non-conformities are found, the reason is documented and assessed further. Such findings are tracked

until fully remediated. This phase also involves continuing to optimize controls across security domains to generate efficiencies in passing future audit and certification reviews. This aligns with the "**Act**" phase.

When this process is used by a product or service delivery group, that team begins with a self-assessment using one of the control modules that were developed as part of creating the Compliance Framework. These modules are described in more detail later in this paper. The business unit then follows the standard methodology described earlier while taking advantage of existing documentation and, where possible, centralized mechanisms for documenting evidence of the application of the selected controls. After completing this process once, the team enters a maintenance phase during which these phases are repeated on a routine and predictable schedule, thus increasing efficiencies and reducing the impact on the team's other initiatives.

Compliance domains

Microsoft analyzed the audits which were repeatedly being performed and sought a unified set of domains through which to identify and categorize compliance controls. OSSC determined that language in the ISO/IEC 27001 standard was sufficient for use as the starting point for a control framework. For a copy of this standard, see http://www.iso.org.

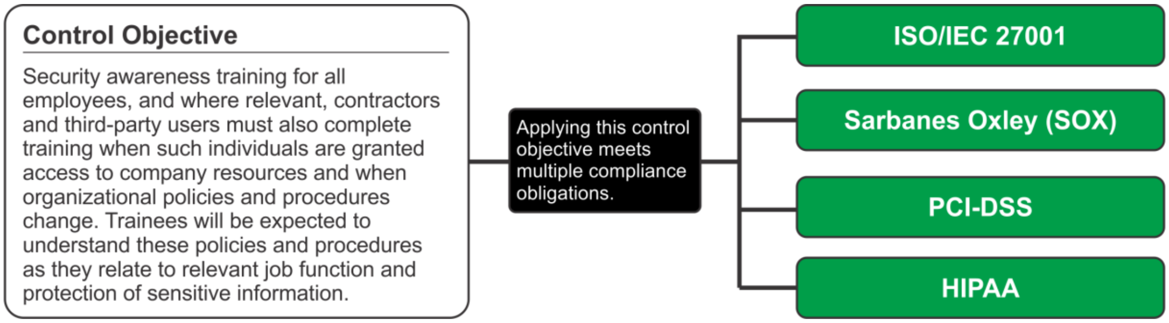
The following table lists the domains and provides the general description for how Microsoft interprets them.

Domain	Description
General Information	Contains the terms used to create a control objective and establishes a baseline definition for each term.
Information Security	Outlines baseline Information Security Policy and Information Security Program expectations.
Organization of Information Security	Defines roles and responsibilities for meeting information security control objectives. Also, defines how information security will be managed with third parties, including vendors and partners.
Human Resources Security	Specifies the objectives for ensuring security awareness, training, and acceptance before and during employment, and at termination or change of employment status.

Domain	Description
Asset Management	Establishes the means for classifying assets and defines other key objectives including acceptable use. Also, specifies what ownership means.
Access Control	Details user responsibilities for maintaining security of credentials. Defines how user credentials are managed, including those provided for third party access. Provides control objectives for various types of user access, specifically: network, operating system, application and information, and mobile computing and remote network access.
Cryptography	Ensures proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information.
Physical and Environmental Security	Defines the physical security of objects and locations, including data centers and network equipment. Also, describes the means through which physical security will be achieved.
Operational Security	Details how to correct and secure operations of information processing facilities.
Communications Security	Outlines protection of information in networks and its supporting information processing facilities.
Systems Acquisition, Development, and Maintenance	Specifies the security requirements for information systems, including cryptographic standards and how security is implemented through all phases of information system acquisition, development, and maintenance.
Supplier Relations	Details how to protect the organizations assets that are accessible by suppliers.
Information Security Incident Management	Describes plan for managing security vulnerabilities and incidents. Defines how such events are reported and documented.
Business Continuity Management	Details how information security is to be addressed in business continuity planning, including such topics as business impact analyses, emergency mode operation and disaster recovery.
Compliance	Outlines general compliance with legal requirements and how control objectives are to be applied in relation to them. Addresses adherence to security policies and standards, audit considerations, and how findings are responded to.

Control modules

Microsoft used the control objectives given in ISO/IEC 27001 as a starting point in an analysis of many other compliance requirements in order to create a superset of compliance objectives. Wherever possible, associations with other applicable requirements have been made to a single common control objective in order to reduce redundancy. The following illustration shows how one control objective from the Human Resources Security domain addresses multiple compliance requirements, including the following industry standards and regulations: ISO/IEC 27001; SOX, for which IT compliance is often demonstrated by applying the Control Objectives for Information and related Technology (COBIT); PCI-DSS; and HIPAA.



Control Objective

Security awareness training for all employees, and where relevant, contractors and third-party users must also complete training when such individuals are granted access to company resources and when organizational policies and procedures change. Trainees will be expected to understand these policies and procedures as they relate to relevant job function and protection of sensitive information.

Applying this control objective meets multiple compliance obligations.

Another approach is to apply control objectives based on the function of a given team. Often, when multiple teams support the information system operations of an entity, aligning compliance requirements with the ongoing activities a team is responsible for establishes a good basis for then finding compliance efficiencies in the rest of the organization. In this scenario, a Datacenter module and a Network Operations module might be warranted.

The following table introduces a sampling of the types of data Microsoft uses to organize the control matrices in the Compliance Framework.

Field	Description
Domain	Name of the domain. For Microsoft, these align with the domains found in ISO/IEC 27001. See the preceding Compliance Domains section for the complete list that Microsoft is using.

Sub Domain	Name of the sub domain. Most of the domains have a sufficient number of control objectives within them that this additional layer of organization adds clarity.
Control Objective	A statement of what is expected and, when appropriate, how that expectation is to be met. An objective defines the goals that controls must meet.
Associated Standard (External Compliance Requirement)	A record of how this objective aligns with regulations, industry standards, or other reference systems. At Microsoft, this data is captured through one or more possible values with each representing a specific set of compliance requirements.
Applicable Security, Standard Operating Procedure (SOP), or System Reference	A record of how this objective aligns with the internal expression of compliance requirements through various forms of governance documents with each value representing a corresponding SOP or policy statement.
Sample Control Activity	A recommendation about how to implement a unified process. For example, many companies use a centralized change management process for updating information technology operations. A sample control activity might suggest using such processes or tools.
Sample Testing Activity	A recommended testing activity or reference to additional documentation for how this control is or should be tested.

Matrices such as this have decreased the amount of time it takes to identify the appropriate control objectives and to define the controls that need to be applied in order to prepare for and pass an audit based on a given set of standards. By using this approach, Microsoft has also seen efficiency gains by utilizing unified processes shared amongst disparate teams and increased confidence in meeting compliance obligations by providing better visibility to ongoing monitoring and risk mitigation efforts.

Conclusion

Striving to control the costs of compliance, to reduce disruption of operational and development plans, and to garner continuing validation that the Compliance Framework meets or exceeds industry standards benefits Microsoft customers and partners in a number of specific ways:

- Microsoft has used the Compliance Framework to produce SOC attestations, to receive FedRAMP ATOs, and to attain ISO/IEC 27001 certification. This work allowed the SOC Type 2 testing to be applied as the foundation for PCI-DSS audit work and the internal management testing requirements for SOX were simplified.
- Applying the online services compliance process allowed Microsoft to create new controls where gaps existed, to document information security processes and controls in a more accessible manner for auditors, to find better ways to manage risk centrally, and to bring more online applications into compliance with less disruption to operational teams.
- Defining who is accountable for meeting requirements and increasing visibility of expectations along with improved internal and external monitoring resulted in increased assurance of continuously meeting compliance requirements.
- Providing a more predictable schedule for the datacenter walkthroughs required to pass external audits eliminated unnecessary disruption to operations teams.
- Standardizing processes and communications make it easier for Microsoft to apply controls across multiple teams and data centers. This ongoing application of the Compliance Framework also means improvements in automation, where appropriate, are continuing.

Putting in place a Compliance Framework, including a common set of compliance domains and control objectives as well as a clear and iterative process for improving compliance over time, can help organizations control costs and retain focus on what matters most: serving the needs of their customers.

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://msdn.microsoft.com/en-us/security/dd206731.aspx

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

Appendix

The reference tables in this section show how the control objectives in the Microsoft Compliance Framework for Online Services align with compliance domains in the current ISO 27001:2013 version of the standard.

For a copy of this standard, see http://www.iso.org.

General Information

The initial domain, General Information, does not contain enough information to warrant displaying it in a table. Two basic areas are covered:

- The terms used to create a control objective and how a baseline definition for each term may be defined.
- The scope definition, which uses the same language as that found in Table A.1 of the ISO/IEC 27001:2013 requirements.

Information Security

This domain aligns with A.5 Security Policy section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
1	A.5 Information security policies	Security Policy	Define, approve, communicate, and review at defined intervals a formal information security policy.
1	A.5 Information security policies	Policy Exceptions	Document and track approval of exceptions to security requirements.

Organization of Information Security

This domain aligns with the A.6 Organization of information Security section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective

2	A.6 Organization of information security	Security Ownership	Formally assign ownership of information security to a member of senior management.
2	A.6 Organization of information security	Security Roles and Responsibilities	Define and assign information security roles and responsibilities.
2	A.6 Organization of information security	Risk Management Program	Develop, implement, and maintain a risk management program that includes assessment methodology, mitigation strategy and monitoring process.
2	A.6 Organization of information security	Facilities Authorization	Authorize the operation of information processing systems and facilities.
2	A.6 Organization of information security	Authorities and Associations	Maintain contact with appropriate authorities and associations.
2	A.6 Organization of information security	Security Performance Assessment	Periodically assess the performance of policies and procedures governing information security.
2	A.6 Organization of information security	Mobile Security	Define, approve, communicate, and review at defined intervals a formal mobile device and teleworking policy.

Human Resources Security

This domain aligns with the A.7 Human Resources Security section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
3	A.7 Human resources security	Human Resources Process	Ensure appropriate response for security violations, up to and including disciplinary action, in accordance with Human Resources policies and practices.
3	A.7 Human resources security	Personnel Screening	Perform personnel screening and background verification checks when appropriate.

3	A.7 Human resources security	Termination or Change of Employment Responsibilities	Communicate information security responsibilities that remain valid after termination or change of employment responsibilities.
3	A.7 Human resources security	Access Removal	Remove/modify logical and physical access as part of all personnel terminations/transfers.
3	A.7 Human resources security	Security Training	Train and inform personnel of their security roles and responsibilities within the terms of their employment contract.

Asset Management

This domain aligns with the A.8 Asset Management section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
4	A.8 Asset management	Authorized Use	Identify, document, and implement rules for the acceptable and authorized use of information.
4	A.8 Asset management	Asset Inventory	Inventory, classify, and assign ownership to assets.
4	A.8 Asset management	Asset Handling	Develop and implement procedures for the protection and handling of assets.
4	A.8 Asset management	Media Disposal	Securely dispose of media when no longer required.
4	A.8 Asset management	Asset Recovery Upon Termination	Recover all company assets from users upon termination of their employment.

Access Control

This domain aligns with the A.9 Access Control section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
5	A.9 Access control	Access Policy	Define, document, implement and periodically review and update formal logical access control policies and procedures.

5	A.9 Access control	Access Authorization	Authorize and periodically review access to information systems / components.
5	A.9 Access control	Least Privilege	Provision logical permissions and access to system functionality based on least privileges required to satisfy job function.
5	A.9 Access control	External Connections	Authorize, authenticate, and secure external connections to the network.
5	A.9 Access control	Authentication	Configure information systems to authenticate users / components, incorporating the use of a unique identifier, prior to allowing access.
5	A.9 Access control	Default User Accounts	Disable default, test/development, and vendor supplied user accounts from use within the production environment.
5	A.9 Access control	Maintenance, Utilities and Tools	Restrict and monitor maintenance access, system utilities, and diagnostic tools.
5	A.9 Access control	Access Removal	Remove access to information systems / components upon termination or adjust access upon role change.

Cryptography

This domain aligns with the A.10 Cryptography section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
6	A.10 Cryptography	Cryptography	Implement cryptographic policy and procedures for authorization, storage, communication, and generation of cryptographic information.

Physical and Environmental Security

This domain aligns with the A.11 Physical and environmental security section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
7	A.11 Physical and environmental security	Physical Security Policy	Define guidelines and policies for physical security.
7	A.11 Physical and environmental security	Physical Access to Facilities	Prevent and monitor unauthorized physical access to production information systems facilities.
7	A.11 Physical and environmental security	Physical Access to Components	Prevent and monitor unauthorized physical access to sensitive information system equipment or components.
7	A.11 Physical and environmental security	Environmental Threats	Protect information systems from environmental threats.
7	A.11 Physical and environmental security	Protection from Disruptions	Protect information systems from power outages, equipment failures, and disruptions.
7	A.11 Physical and environmental security	Component Disposal	Reuse, retire or dispose of components that contain sensitive data in a secure manner.

Operational Security

This domain aligns with the A.12 Operational security section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
8	A.12 Operational security	Operational Policy	Document, maintain, review, approve and communicate operational policies and procedures.
8	A.12 Operational security	Segregation of Duties	Segregate responsibilities to prevent unauthorized or unintentional modification of information systems or data.
8	A.12 Operational security	Back-up Procedures	Define and implement procedures to back up, store, and recover data.

8	A.12 Operational security	Malicious Software	Employ and maintain preventive, detective, or corrective measures, as appropriate, against malicious and/or unauthorized software, as well as mobile code.
8	A.12 Operational security	Baseline Configurations	Establish and maintain approved baseline configurations for security systems and security functionality within systems.
8	A.12 Operational security	Change Management	Control changes to the organization, business processes, information processing facilities and systems that affect information security.
8	A.12 Operational security	Event Logging	Identify events for logging and verify, retain, secure, and take corrective action in response to logged events.
8	A.12 Operational security	Systems Capacity & Performance	Optimize system performance and capacity utilization to provide sufficient availability through planning, monitoring, and forecasting activities.
8	A.12 Operational security	System Documentation	Restrict access to system documentation.
8	A.12 Operational security	Software installation	Establish procedures to control the installation of software on operational systems.
8	A.12 Operational security	Security Vulnerabilities	Collect information on technical security vulnerabilities and evaluate and take appropriate measures to address associated risk in a timely manner.
8	A.12 Operational security	Minimize Disruptions	Minimize disruptions to business processes.

Communications Security

This domain aligns with the A.13 Communications security section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective

9	A.13 Communications security	Communications Across Networks	Manage, monitor, protect, secure, and control communications across networks.
9	A.13 Communications security	Communication Channels	Secure the exchange of information through authorized communication channels and transactions.
9	A.13 Communications security	Confidentiality and Non-Disclosure Agreements	Identify, review, and document requirements for confidentiality and non-disclosure agreements.
9	A.13 Communications security	Segregation of Environments	Segregate environments to prevent unauthorized or unintentional modification of information systems or data.
9	A.13 Communications security	Network Design	Protect and restrict access to systems and data through network design, segmentation, and configuration.
9	A.13 Communications security	Integrity and Confidentiality	Secure the integrity and confidentiality of user sessions that connect to information systems and equipment.

System Acquisition, Development and Maintenance

This domain aligns with the A.14 System acquisition, development and maintenance section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
10	A.14 System acquisition, development and maintenance	Security Requirements	Prepare, document, and track security requirements when developing or acquiring application software and systems.
10	A.14 System acquisition, development and maintenance	Defense-in-Depth	Employ a defense-in-depth strategy using multiple layers of security boundaries and technologies.

10	A.14 System acquisition, development and maintenance	Development and Delivery	Implement formal information systems development and delivery processes with defined standards, methodology, roles, and responsibilities.
10	A.14 System acquisition, development and maintenance	Secure Software and Systems	Securely build software and systems by restricting access to source code, ensuring the integrity and authenticity of software, managing security issues, and acquiring software from reputable sources.
10	A.14 System acquisition, development and maintenance	Validate Data Integrity	Validate data integrity through checks on inputs, outputs, processing, and storage.
10	A.14 System acquisition, development and maintenance	Verify Security Functions	Verify security functions and operations in a controlled test environment.
10	A.14 System acquisition, development and maintenance	Secure Development Policy	Establish and apply rules for the development of software and systems.
10	A.14 System acquisition, development and maintenance	System Engineering Principles	Establish , document, and maintain principles for engineering secure systems.
10	A.14 System acquisition, development and maintenance	Secure Development Environment	Protect secure development environments for system development and integration efforts.
10	A.14 System acquisition, development and maintenance	System Testing	Establish test procedures and acceptance criteria for validating changes to prevent unauthorized or unintentional modifications to production environments.

Supplier Relationships

This domain aligns with the A.15 Supplier relationships section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
11	A.15 Supplier relationships	External Parties	Identify, assess, and respond to risks when interacting with external parties.

11	A.15 Supplier relationships	Monitor Supplier Services	Monitor, review, and audit provisions of services by suppliers and supplier service delivery.
11	A.15 Supplier relationships	Service Agreements	Document and monitor service agreements for in-house and outsourced services.

Information Security Incident Management

This domain aligns with the A.16 Information security incident management section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
12	A.16 Information security incident management	Incident Response Process	Establish a security incident response process to track, analyze, and resolve security problems.
12	A.16 Information security incident management	Incident Response Procedures and Training	Define incident response plans and procedures, assign roles, and train personnel in their responsibilities.
12	A.16 Information security incident management	Security Incidents	Collect, retain, and present evidence of security incidents conforming to the legal rules of evidence.
12	A.16 Information security incident management	Service Monitoring	Identify and manage security incidents and vulnerabilities in a timely manner.
12	A.16 Information security incident management	Incident Response Capabilities	Periodically test security incident response capabilities.

Information Security

This domain aligns with the A.17 Information security section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
13	A.17 Information security aspects of business continuity management	Business Continuity Process	Develop, implement, test and maintain business continuity processes to protect critical business processes from the risks and effects of catastrophic events.

13	A.17 Information security aspects of business continuity management	Alternate Systems Facilities	Establish alternate information systems facilities for use in responding to catastrophic events.

Compliance

This domain aligns with the A.18 Compliance section in the ISO/IEC 27001:2013 requirements.

Domain	ISO 27001:2013 Section	Objective Name	Microsoft Control Objective
14	A.18 Compliance	Compliance	Comply with relevant regulatory, industry, contractual, legal, and privacy requirements as well as policies, standards, procedures, and business objectives.
14	A.18 Compliance	Data Retention	Retain, protect, and dispose of information records in accordance with data retention policies.
14	A.18 Compliance	Compliance Monitoring	Independently review, evaluate, assess, and monitor compliance with organizational and business objectives and policies as well as legal and regulatory requirements.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site 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.