Microsoft
Global Foundation Services

Microsoft Compliance Framework for Online Services

Online Services Security and Compliance

Service delivery and operations teams at Microsoft needed to adapt their compliance practices due to the changing landscape of regulations, statutes, and industry best practice standards for online services. Readers of this paper will gain an understanding of the framework Microsoft developed in order to more efficiently utilize existing staff and resources, and to establish and maintain online services compliance. The Microsoft Compliance Framework for Online Services allows the company to better meet complex obligations through reducing risk of operational disruptions and increasing confidence in service stability, and by obtaining third party verifications as proof of continuing adherence to compliance requirements.

This paper is one of a series introducing the Online Services Security and Compliance (OSSC) team, a part of the Global Foundation Services division who manages security for the Microsoft cloud infrastructure. For more information about how OSSC manages security risks to the cloud infrastructure, see Securing Microsoft's Cloud Infrastructure.

Published: October 2009

Table of Contents

Executive Summary

Since the launch of MSN® in 1994, Microsoft has been building and running online services. Global Foundation Services (GFS) provides the cloud infrastructure for these services including ensuring availability for hundreds of millions of customers around the world 24 hours a day, every day. Hosting such familiar consumer-oriented services as Windows Live™ Hotmail® and Bing™, and business-oriented services such as Microsoft Dynamics® CRM Online 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 means the company must adhere to numerous regulatory, statutory, and industry standards for securing personal and financial data. For more information about how Online Services Security and Compliance (OSSC) manages security risks to the cloud infrastructure, see Securing Microsoft's Cloud Infrastructure.

To satisfy the various audits Microsoft product or service delivery groups are subject to, GFS teams were often asked for the same types of information repeatedly over the course of a year. Internal teams and partners would also ask about compliance with various regulations, statutes, and industry standards while responding to inquiries from customers and prospects. Having established expertise in responding to these requests, the OSSC team, part of the GFS division, was often asked about how best to prepare for scrutiny from outside auditors in the future. OSSC, along with Microsoft senior management, identified the need for a more centralized approach to preparing for and undergoing audits with the specific goals 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.

The Microsoft Compliance Framework for Online Services (Compliance Framework) was developed by OSSC to address this need. The 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 regulations or requirements. In addition to ensuring that compliance expectations are continually achieved, applying the Compliance Framework has helped produce Statement of Auditing Standard (SAS) 70 Type I and Type II attestations; to attain International Organization for Standardization / International Electrotechnical Commission 27001:2005 (ISO/IEC 27001:2005) certification; and to more efficiently pass various audits from independent third parties.

This paper introduces the Compliance Framework in more detail, and provides examples of how to develop compliance domains and to apply control objectives to them in the context of specific industry standards or regulatory requirements. The OSSC team within the GFS division builds on the same security principles and processes Microsoft has developed through years of experience managing security risks.

The Changing Landscape for Online Services Compliance

Any company offering online services that involve collecting personal or financial information from users will find its operations must comply with certain regulations or statutes. Which laws apply depend on the unique circumstances of a business, such as the types of data the company processes, where the company's data centers are based, or 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 GFS-managed cloud infrastructure 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. At many companies, these reviews can 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 requirements the company must address in addition to the standards Microsoft elects to pursue, such as ISO 27001:2005 and SAS 70 Type I and II attestations.

Requirement	Description
Payment Card Industry Data Security Standard (PCI-DSS)	Security controls for collection, storage, or processing of credit card information.
Media Ratings Council (MRC)	Defines standards for data integrity, online advertising campaign control objectives, audience measurement, disclosures, and ethics.
Sarbanes-Oxley (SOX)	Dictates specific requirements for financial reporting by public U.S.–based companies. The titles cover such areas as corporate responsibility, auditor independence, analyst conflicts of interest, and other subjects related to financial disclosures.

As online businesses continue to evolve at Microsoft and new online services are introduced into the GFS environment, additional compliance expectations are expected which could include regional and country-specific data security laws, regulations and standards.

How Microsoft Dealt with Online Services Audits

Microsoft teams historically met these 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 each for certain online services, financial accounting, and reporting systems. 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 several employees.

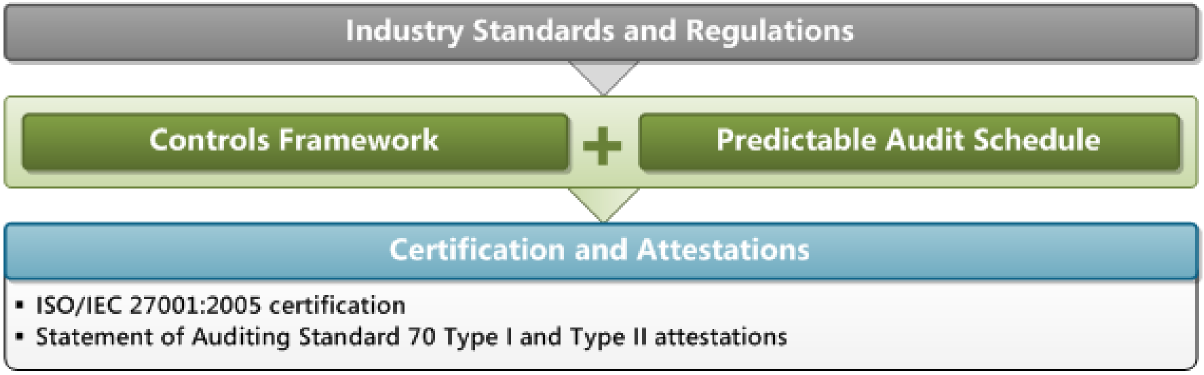
When Microsoft looked at the work involved in successfully completing compliance reviews with a focus on the teams involved, a different story altogether emerged: many of the same staff members were called upon to provide similar information for every audit. These employees participated in numerous consecutive 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.

OSSC recognized that the operational environment for online services at Microsoft 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. Given the changes in the economic landscape and that redundancies of effort had already been identified, Microsoft sought another way to address this gap.

Microsoft Compliance Framework for Online Services

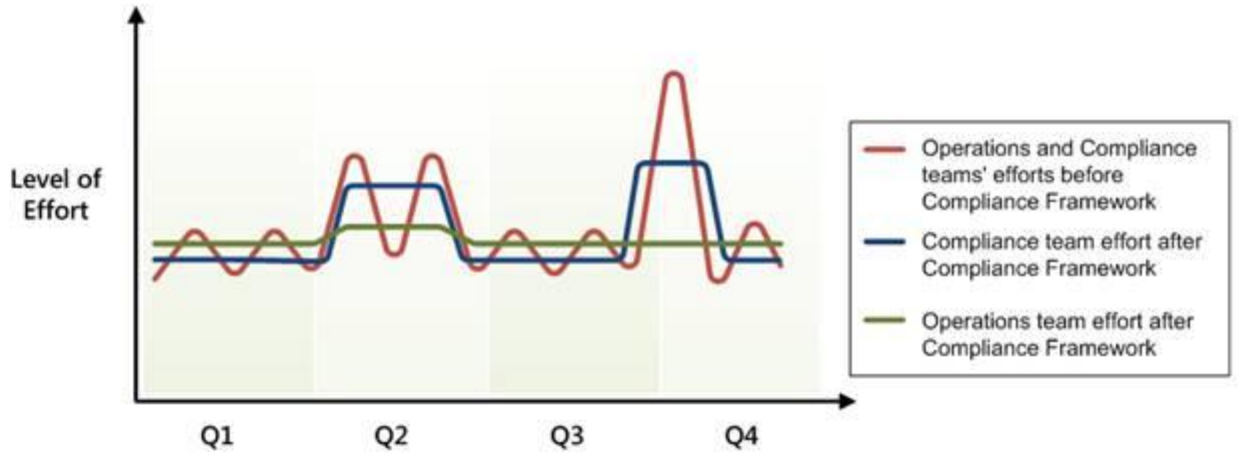
OSSC continued to analyze how reacting to individual audits as discrete efforts undermined the productivity of their staff. By working with the teams most frequently impacted by these efforts, OSSC identified an opportunity to reduce redundancy and proposed a solution to streamline processes and to proactively manage compliance expectations in a more comprehensive manner. This continuing 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 the most efficient and 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.


Industry Standards and Regulations
Controls Framework
+
Predictable Audit Schedule
Certification and Attestations
▪ ISO/IEC 27001:2005 certification
▪ Statement of Auditing Standard 70 Type I and Type II attestations

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 mature process for audit coordination has allowed Microsoft to begin using the Compliance Framework to streamline reviews of GFS teams and infrastructure 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 both SAS 70 Type I and Type II attestations and ISO/IEC 27001:2005 certification.

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

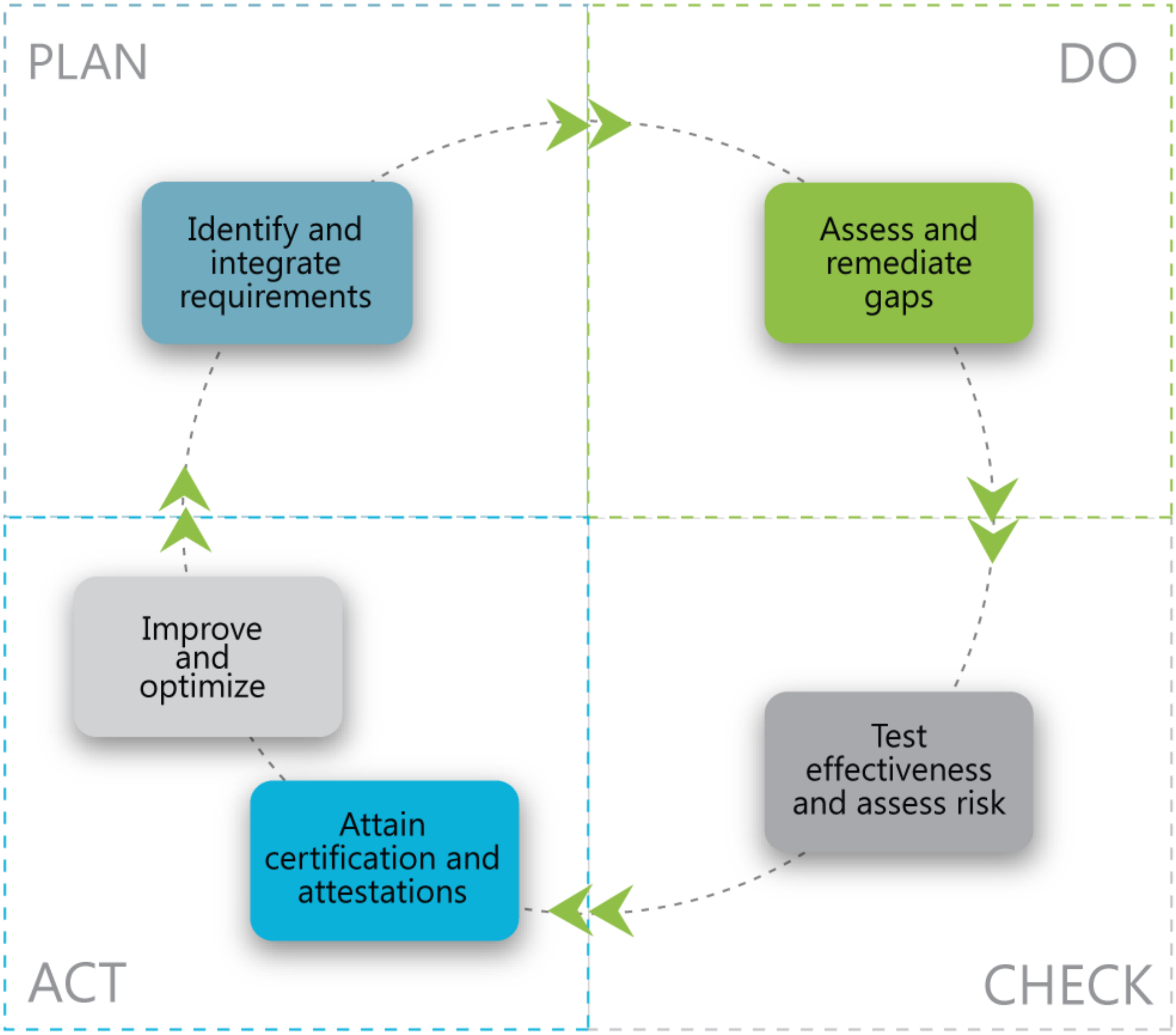
The OSSC team within GFS is responsible for the Microsoft cloud infrastructure Information Security Program, including policies and programs used to manage online security risks. The mission of OSSC is to enable trustworthy online services that create a competitive advantage for Microsoft and its customers. Having this standard approach also enables each of the Microsoft service teams to focus on the unique security needs of their customers.

The OSSC team drives the effort to provide a trustworthy experience in the Microsoft cloud through the Microsoft Information Security Program using a risk-based operating model and a defense-in-depth approach to controls. This includes 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 in the ISO/IEC 27001:2005 standard. With a continuing emphasis on optimization, Microsoft is using this methodology to extend use of the Compliance Framework from the GFS infrastructure into product and service delivery groups who offer online services within the Microsoft hosting environment.

The following illustration shows the Compliance Framework methodology.


PLAN
DO
Identify and integrate requirements
Assess and remediate gaps
Improve and optimize
Test effectiveness and assess risk
Attain certification and attestations
ACT
CHECK

- **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 ISO/IEC 27001:2005 “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 ISO/IEC 27001:2005 “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 ISO/IEC 27001:2005 “Check” phase.
- **Attain certification and attestations** – Engagement with third-party certification authorities and auditors occurs. This aligns with the ISO/IEC 27001:2005 “Act” phase.
- **Improve and optimize** – If issues or non-conformities are found, the root cause is documented and assessed further. Such findings are tracked until fully remediated. This phase also involves continuing to optimize controls across security domains to generate efficiencies in passing future audit and certification reviews. This aligns with the ISO/IEC 27001:2005 “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 what audits were being done repeatedly and sought a unified set of domains through which to identify and categorize compliance controls. OSSC determined that language in the ISO/IEC 27001:2005 *Information technology — Security techniques — Information security management systems — Requirements* was sufficient for use as the starting point for a controls framework. For a copy of this standard, see http://www.iso.org.

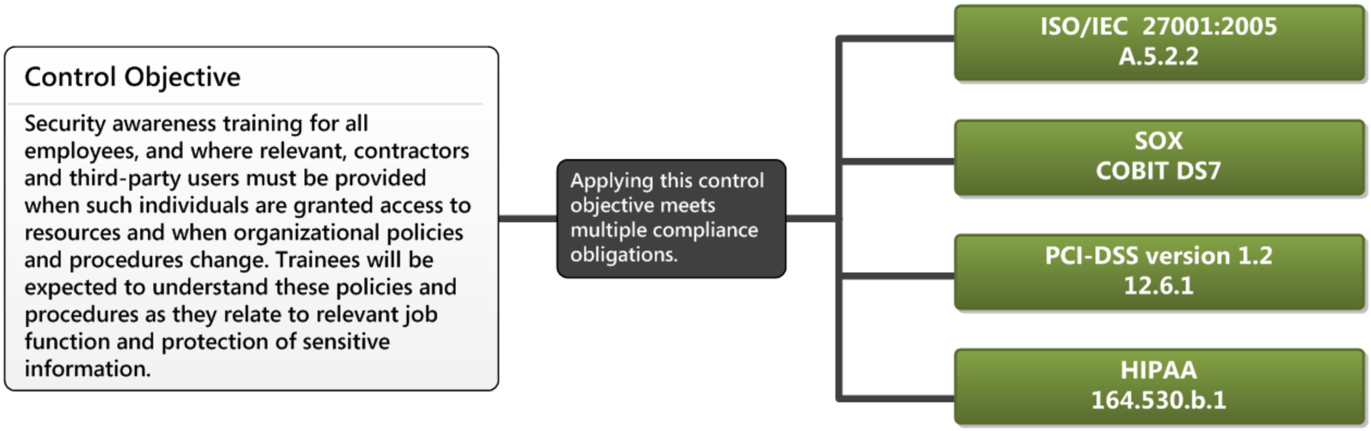
Microsoft has added one domain not included in the ISO/IEC 27001:2005 in order to address certain requirements. The following table lists the domains and provides the general description for how Microsoft interprets them.

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.
Asset Management	Establishes the means for classifying assets and defines other key objectives including acceptable use. Also, specifies what ownership means.
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.
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.
Communications and Operations Management	Contains many sub-domains that specify the control objectives for operational procedures, including monitoring, data backup and retention, and network security. Also defines standards for media handling, electronic commerce services, information exchange, and protection against malicious code. Includes objectives for system planning and acceptance, and management of third party service delivery.

Domain	Description
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.
Information 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.
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.
Risk Management	Provides baseline definitions and timelines for risk assessment and mitigation.
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.
Privacy	Sets expectations about how privacy policy is developed and communicated within the company and to customers.

Control Modules

Microsoft used the control objectives given in ISO/IEC 27001:2005 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 27001:2005; 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 be provided when such individuals are granted access to 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.

Having associated objectives with internal policies and procedures, regulations, industry standards, and other reference systems means the Compliance Framework can also be used to create groupings of controls based on these associations. Microsoft has added information such as examples of control activities and suggestions of how to use existing testing and documentation processes to the Compliance Framework in order to enable the creation of control matrices to help teams more quickly become organized to prepare for compliance reviews.

Control matrices can be organized in numerous ways. Some situations call for organizing modules to align controls to a given set of standards. For example, if a new online health information service will use credit cards for billing, a control matrix can be created based on the control objectives associated with both PCI-DSS and HIPAA. This filtering to a selection of control objectives simplifies the process of preparing the release and operations teams by providing examples of control-to-test activity pairs and how these are associated with a given control objective. This reuse of existing controls, policy and procedure language, and testing processes enables service delivery teams to bring a new service offering operation into compliance more efficiently and with fewer conformance issues than if such teams develop a compliance program in isolation.

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 Data Center 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 27001:2005. 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.

Such matrices are in use at Microsoft and 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 SAS 70 Type I and Type II attestations and to attain ISO/IEC 27001:2005 certification. This work allowed the SAS 70 Type II 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 data center 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

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

International Organization for Standardization and International Electrotechnical Commission. *Information technology — Security techniques — Information security management systems — Requirements*. Geneva, Switzerland: International Organization for Standardization, 2005.

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

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

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

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

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

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

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

Appendix

The reference tables in this section show how the control objectives in the Microsoft Compliance Framework for Online Services align with compliance domains. The control objectives included here have been generalized with the intent of making the language easier for other companies to use them as a starting point for developing a compliance framework of their own. The actual language used by Microsoft for control objectives differs from that included in this appendix.

Also, in many cases, Microsoft determined that language in the ISO/IEC 27001:2005 *Information technology — Security techniques — Information security management systems — Requirements* was sufficient for use as a common control objective in the Compliance Framework. Where this is the case, the reference number of the requirement, the control, or the control objective has been included in the "Control Objective" column. 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 Compliance Framework uses the same definitions as those found in A.2–A.2.17 of the ISO/IEC 27001:2005 requirements.
- The scope definition, which uses the same language as that found in A.1 of the ISO/IEC 27001:2005 requirements.

Information Security

This domain aligns with A.5 Security Policy section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Information security program	Executive management provides clarity on the direction of and support for security initiatives through regular meetings; supervises the creation and implementation of the information security program; ensures that the program is in alignment with business objectives, applicable regulations and statutes, and industry standards; and reviews the effectiveness of the program periodically approving changes when needed. The information security program should dictate how information the company creates, receives, maintains, or transmits is classified in terms of sensitivity and how, based on that classification, confidentiality, integrity, and availability is addressed.
Management oversight and approval	Senior management or a designated authority inside the company must provide supervision for creation and maintenance of the information security program, including periodic reviews of the effectiveness of the program and the provision of approvals for any changes they deem necessary.
Information security program reporting	The status of the information security program should be reported to senior management or a designated authority on an annual basis, including a discussion of compliance with the program, risk assessment results, and change recommendations.
Adjustment of the information security program	The information security program should be adjusted to address changing business objectives, environmental modifications, and applicable regulatory and industry requirements based on ongoing monitoring and evaluation activities.
Information security policy	A clear direction for policy should be set by senior management that aligns with the information security program and that demonstrates support for and commitment to information security through the creation and maintenance of information security policy throughout the company.
Information security policy document	Approved information security policies should be communicated to all employees and relevant third parties through publication of policy documentation.

Description	Control Objective
Review of the information security policy	At a minimum, the information security policy should be reviewed annually. Significant environmental, organizational, or operational changes should also trigger a policy review in order to verify continuing adequacy and effectiveness of the policy.
Retention of information security policy document	Retention of the information security policy is based on its creation date or when it was last in effect. The policy should be retained for six years from the latter of the two possible dates.

Organization of Information Security

This domain takes its name from and aligns with the A.6 Organization of information Security section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Internal organization	See A.6.1 in ISO/IEC 27001:2005.
Management commitment to information security	See A.6.1.1 in ISO/IEC 27001:2005.
Information security co-ordination	See A.6.1.2 in ISO/IEC 27001:2005.
Allocation of information security responsibilities	Information security responsibilities for all employees and contractors are defined through clearly stated policies and procedures.
Information security officer	The responsibility of developing, implementing and distributing security policies and procedures should be assigned to one individual.
Security alerts management	The responsibility of monitoring and analyzing security alerts and information, and distributing them to the appropriate personnel should be assigned to an official or a team.
Security incident management	The responsibility of establishing, documenting and distributing security incident response and escalation procedures should be assigned to an official or a team.

Description	Control Objective
User administration	The responsibility of administering user accounts should be assigned to an official or a team.
Data access management	The responsibility of monitoring and controlling all access to data should be assigned to an official or a team.
Authorization process for information processing facilities	See A.6.1.4 in ISO/IEC 27001:2005.
Confidentiality agreements	See A.6.1.5 in ISO/IEC 27001:2005.
Contact with authorities	An individual or a team should be assigned the responsibility of managing and maintaining appropriate contacts with relevant authorities such as law enforcement agencies and regulatory bodies.
Contact with special interest groups	An individual or a team should be assigned the responsibility to manage and maintain appropriate contacts with external parties such as security groups and industry forums.
Independent review of information security	See A.6.1.8 in ISO/IEC 27001:2005.
External parties	See A.6.2 in ISO/IEC 27001:2005.
Identification of risks related to external parties	See A.6.2.1 in ISO/IEC 27001:2005.
Protection of hosted environment	The hosted environment and data for each hosted entity should be protected.
Management of connected entities	A list of connected third parties should be maintained, and policies and procedures regarding the connection and disconnection of third parties should be in place, including careful review of third parties before connection occurs.
Addressing security when dealing with customers	See A.6.2.2 in ISO/IEC 27001:2005.

Description	Control Objective
Addressing security in third party agreements	See A.6.2.3 in ISO/IEC 27001:2005.
Documentation of third party assurances	A contract or other written agreement should document that satisfactory assurances have been provided that the third party will meet the applicable security requirements.
Information use and disclosure	The permitted and required uses and disclosures of information by a third party should be established in third-party agreements.
Reporting of security incidents	The third party should be required to report any security incidents that may affect the information processing facilities or services, under the scope of the contract, through the agreement with the third party.
Termination of third party agreements	Termination of the contract if a material term of the contract has been violated should be detailed in the third party agreement.
Regulatory compliance	The third party should be required to protect sensitive data and to comply with applicable regulatory requirements through the agreement with the third party.

Asset Management

This domain takes its name from and aligns with the A.7 Asset Management section in the ISO/IEC 27001:2005 requirements.

Description	**Control Objective**
Responsibility for assets	See A.7.1 in ISO/IEC 27001:2005.
Inventory of assets	Information assets should be identified, given a security classification, and tracked by physical location. The inventory must also record ownership and indicate when last verification of all inventory detail occurred.
Ownership of assets	In order to be able to keep an accurate inventory, a designated owner must be identified for each tracked asset.
Acceptable use of assets	Acceptable uses for assets should be documented and applied.
Acceptable use of workstations	The proper use of a given type of workstation, including how it is physically positioned within a work environment, should be detailed in policies and procedures. Limitations for special types of workstations, such as those used to access protected health or financial information, must be described through policies and observed through application of procedures.
Acceptable use of technology	When to introduce and how to use technologies must be described in acceptable use policies and, when appropriate, explicitly approved by senior management. Such policies must provide details about acceptable locations and which products are approved for use.
Maintenance of access list	Personnel with access to network devices, including modems and wireless routing equipment, must be recorded in an access list, in accordance with usage policies.
Acceptable secure usage	Authentication and session time-out requirements should be described in usage policies. Such details must cover how sensitive information may be accessed remotely and include specifics about how modems may be used by vendors.

Description	Control Objective
Information classification	The criteria for information classification should be based on the need for and value of the information, and the expected degree of protection when handling information.
Classification guidelines	See A.7.2.1 in ISO/IEC 27001:2005.
Information labeling and handling	In accordance with information classification guidelines, methods for labeling and handling classified information must be documented.

Human Resources Security

This domain takes its name from and aligns with the A.8 Human Resources Security section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Prior to employment	Individuals must be screened and must understand their roles and responsibilities pertaining to information security based on job, task, or project descriptions. Such understanding should be documented in the form of a contract or employee agreement signed by the individual prior to beginning work.
Roles and responsibilities	See A.8.1.1 in ISO/IEC 27001:2005.
Screening	See A.8.1.2 in ISO/IEC 27001:2005.
Terms and conditions of employment	See A.8.1.3 in ISO/IEC 27001:2005.
During employment	Management responsibilities pertaining to human resources security should be defined to ensure that all relevant security procedures have been explained and are adhered to by vendors, contractors, and employees during each individual’s employment. All employees, contractors, and third-party users must be given an adequate level of education and training in security procedures to ensure awareness of how to minimize possible security risks. Security breaches must be addressed through a formal disciplinary process established by senior management and documented in relevant policy statements.

Description	**Control Objective**
Management responsibilities	See A.8.2.1 in ISO/IEC 27001:2005.
Information security awareness, education, and training	See A.8.2.2 in ISO/IEC 27001:2005.
Information security awareness	Periodic training updates and other reminders of information security awareness should be provided.
Information security education and training	The topics of password management, login monitoring, and how to protect information and assets from malicious software must be addressed in information security training and education.
Disciplinary process	See A.8.2.3 in ISO/IEC 27001:2005.
Termination or change of employment	Human resource policy and procedures should describe how and when to ensure the safe return of equipment and how and when to remove an individual's access to network resources at the time the individual is no longer employed. Such policies will also cover adjustment of information access and asset ownership should the individual remain employed in a different classification, such as becoming a contractor after having been an employee.
Termination responsibilities	See A.8.3.1 in ISO/IEC 27001:2005.
Return of assets	See A.8.3.2 in ISO/IEC 27001:2005.
Removal of access rights	See A.8.3.3 in ISO/IEC 27001:2005.

Physical and Environmental Security

This domain takes its name from and aligns with the A.9 Physical and Environmental Security section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Secure areas	Facilities used to process critical or sensitive information must be protected by defined security perimeters with appropriate security barriers and entry controls to secure the area in accordance with policies and procedures. Security protections must take in to account the identified risks associated with the classification of the information being secured.
Physical security policies and procedures	Safeguards for the facilities and equipment should be implemented through policies and procedures to prevent unauthorized physical access, tampering, and theft.
Physical security maintenance records	How changes to the physical security components of a facility will be addressed and documented, including what process will be used to inform relevant staff and contractors of impending work, should be described in policies and procedures.
Physical security perimeter	Areas that contain information and information processing facilities should be protected by a physical security perimeter.
Physical entry controls	Access to areas used to store and process information should be controlled and monitored according to information security policies and procedures allowing access as appropriate according to an individual's role and responsibility.
Identification badges	Employees, contractors, temporary workers, and visitors must be provided with and display identification badges as a means of identity verification.
Visitor access control	Physical access to secure areas should be limited for visitors. Policies and procedures should ensure that visitors are granted authorization before being granted access to secure areas, are given badges that are easy to distinguish from those of employees, and that visitor activity logs are maintained.

Description	Control Objective
Securing offices, rooms and facilities	Offices, rooms, and facilities used for accessing sensitive information must have physical security measures designed in accordance with existing policies and applied.
Securing workstations	Workstations that are used for accessing sensitive information should have physical security safeguards designed for them and applied. The physical attributes of workstation surroundings must be specified in policies and procedures.
Securing network jacks	Access to network jacks should be limited to authorized personnel.
Securing wireless access points	Physical access to wireless access points and gateways, and the use of handheld devices in data centers should be restricted.
Protecting against external and environmental threats	See A.9.1.4 in ISO/IEC 27001:2005.
Working in secure areas	See A.9.1.5 in ISO/IEC 27001:2005.
Surveillance	In order to monitor sensitive areas, surveillance systems should be in place and should include cameras where appropriate.
Retention of surveillance data	To allow for review when needed, retention of surveillance data should be for a minimum of 3 months except in the case that laws or agreements do not permit a 3-month retention period. Data center access logs should be reviewed with regular frequency.
Security of field offices	Similar levels of physical protection to those used in the headquarter offices should be applied to field offices.
Public access, delivery and loading areas	See A.9.1.6 in ISO/IEC 27001:2005.
Equipment security	See A.9.2 in ISO/IEC 27001:2005.
Equipment siting and protection	See A.9.2.1 in ISO/IEC 27001:2005.
Supporting utilities	See A.9.2.2 in ISO/IEC 27001:2005.
Cabling security	See A.9.2.3 in ISO/IEC 27001:2005.

Description	Control Objective
Equipment maintenance	See A.9.2.4 in ISO/IEC 27001:2005.
Security of equipment off-premises	See A.9.2.5 in ISO/IEC 27001:2005.
Secure disposal or re-use of equipment	See A.9.2.6 in ISO/IEC 27001:2005.
Removal of property	See A.9.2.7 in ISO/IEC 27001:2005.

Communications and Operations Management

This domain takes its name from and aligns with the A.10 Communications and Operations Management section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Operational procedures and responsibilities	The correct and secure operation of information processing facilities should be established. The associated responsibilities and appropriate operating procedures should be documented.
Documented operating procedures	See A.10.1.1 in ISO/IEC 27001:2005.
Change management	Change management should be controlled including having in place policies and procedures to address how information system, software, and facilities modifications are proposed and how such changes are approved by management. Potential impacts of changes should be analyzed and documented as part of the review and approval process. Change management procedures must also take into account the ability to roll systems back to a previously operational state and plans to test modifications to verify system stability and security.
System update and patch process	The latest vendor-supplied security patches must be tested and applied within one month of release to system components and software.
Segregation of duties	To minimize the potential for fraud or misuse, areas of responsibility and duties for critical functions should be segregated.

Description	Control Objective
Separation of development, test and operational facilities	In order to reduce the risks of unauthorized access or changes to the operational system, development and test facilities should be separate from each other and from operational facilities.
Monitoring	Monitoring of networks and information systems should be in place to detect unauthorized activities and information security events.
Audit logging	Documentation of user activities, exceptions, and information security events must be produced and kept for an agreed period to assist in the case an investigation is needed in the future. Logs and other automated records of access control monitoring may be used as documentation.
Automated audit trails	Critical systems should have automated audit trails implemented.
Audit events	Auditable events should be identified and data that can be used to review these events should be recorded in the audit trails.
Retention of audit trails	Audit logs should be kept for a minimum of one year. Logs up to 3 months old should be available online.
Monitoring system use	Use of information processing facilities should be monitored and the results of the monitoring activities reviewed daily.
Monitoring system access	Access to system components should be monitored on a per-user basis.
Protection of log information	Information captured in logs and the means by which logs are created should be protected against tampering and unauthorized access.
Limit of access to audit trails	Individuals should be granted access to view audit trails on a need-to-know and least privilege principles.
Back-up of audit trails	Back-ups of audit trails should be stored on a centralized server.
Wireless network logs	Wireless network logs should be stored on a log server on an internal LAN.
Protecting integrity of audit trail	Alerts should be generated whenever audit logs are changed.

Description	Control Objective
Administrator and operator logs	See A.10.10.4 in ISO/IEC 27001:2005.
Fault logging	See A.10.10.5 in ISO/IEC 27001:2005.
Clock synchronization	See A.10.10.6 in ISO/IEC 27001:2005.
Data Retention	Applicable business, legal, and regulatory requirements should be addressed through the definition of a data retention policy.
Third-party service delivery management	The implementation of agreements should be verified, compliance with the agreements monitored and changes to agreements managed to ensure that the services delivered meet all requirements agreed with the third party.
Service delivery	See A.10.2 in ISO/IEC 27001:2005.
Monitoring and review of third party services	See A.10.2.2 in ISO/IEC 27001:2005.
Managing changes to third-party services	See A.10.2.3 in ISO/IEC 27001:2005.
System planning and acceptance	Operating requirements for current and new systems should be included in a specified system planning and preparation process that also incorporates a review of projected trends as well as new business requirements. Requirements for the operation of new systems should be established, documented, and tested prior to their acceptance and use with the goal of minimizing the risk of system failure.
Capacity management	Current system usage is monitored and tuned according to a capacity planning and management process that also anticipates future capacity requirements with the goal of ensuring system availability and performance based on specified requirements.
Baseline security configuration	Uniform implementation of security controls is ensured through use of configuration standards and guidelines regarding how to provision hardware and software.
Segregation of servers	Having one primary function per server should be required in baseline configuration standards.

Description	Control Objective
Disabling of unnecessary protocols, services, and functionality	All unnecessary functionality and insecure protocols or services should be disabled by default in baseline server configuration standards.
System acceptance	See A.10.3.2 in ISO/IEC 27001:2005.
Protection against malicious and mobile code	The capability to detect and protect against malicious software (such as computer viruses, network worms, Trojan horses, logic bombs, etc) and unauthorized software are included as safeguards.
Controls against malicious code	See A.10.4.1 in ISO/IEC 27001:2005.
Anti-virus safeguards	Anti-virus capabilities should be in place, up-to-date, and running. In addition, these safeguards should be capable of generating audit logs.
Safeguards against spyware and adware	The capability to detect, protect against, and remove spyware and adware should be in place.
Controls against mobile code	See A.10.4.2 in ISO/IEC 27001:2005.
Back-up	Back-up policies and procedures should be in place that includes testing the restoration process regularly.
Information back-up	See A.10.5.1 in ISO/IEC 27001:2005.
Network security management	Taking into account dataflow and legal implications, the data in networks and the underlying network infrastructure should be protected.
Network controls	See A.10.6.1 in ISO/IEC 27001:2005.
Direct access to information	Direct public access between external networks and system components that store sensitive data (such as databases, logs, and trace files) should be denied.
Restrict outbound traffic	Restrictions should be in place to limit outbound traffic from applications that process sensitive data to IP addresses within the DMZ.

Description	Control Objective
IP masquerading	To prevent internal IP addresses from being translated and revealed on the Internet, measures should be taken to hide them.
Channel encryption	Sensitive information transmitted over the internet or other public networks should be encrypted or protected by other equivalent security techniques.
Encryption of administrative access	Administrative access, whether by remote or non-console means, should be encrypted using appropriate technologies.
Encryption of data on wireless networks	Strong techniques for encrypting data or authenticating to devices should be used to protect sensitive information while in transit on wireless networks.
Intrusion detection	The ability to detect anomalous activities or deviations from a baseline configuration that may be indicative of a suspected compromise and to alert incident response teams should be in place. Where applicable, the capability to prevent such activities or deviations should also be put in place.
Updates to intrusion detection and prevention systems	Maintenance procedures for intrusion detection and prevention systems should be in place to ensure these tools are current.
Proactive vulnerability scanning	Procedures used for internal and external network scans should specify a regular cycle, for example quarterly, for conducting these scans. Internal and external networks scans should also be triggered based on major updates to the network, for example: adding system components, changing the network topology, modifying firewall rules, or making product upgrades.
Wireless network scanning	At least quarterly, a wireless network analyzer should be used to identify and scan all wireless devices in use on the network.
Penetration tests	At a minimum of once a year, penetration tests should be conducted. Penetration tests should also be conducted after any significant change.
Security of network services	See A.10.6.2 in ISO/IEC 27001:2005.
Changes to default configuration	Passwords, service identifiers, community strings, and so on supplied by vendors should be changed before deploying a network service or device.

Description	Control Objective
Media handling	Operating procedures should be established to protect documents, computer media (for example, tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction as appropriate based on the asset's classification.
Management of removable media	See A.10.7.1 in ISO/IEC 27001:2005.
Removable media maintenance records	The movements of electronic media and the person responsible for moving a given asset should be recorded and those tracking records should be maintained.
Management approval for movement of media	Management must approve movement of removable media from a secure area.
Reuse of media	Sensitive information should be removed from electronic media before it is reused as described in applicable procedures.
Disposal of media	The final disposition of information, including the hardware or electronic media on which it is stored, or both should be addressed in policies and procedures.
Destruction of hardcopy materials	Mechanisms such as cross-cutting, shredding, incinerating, pulping and so on should be used to destroy hardcopy materials securely.
Destruction of electronic media	Mechanisms such as purging, degaussing, shredding and so on should be used to destroy electronic media.
Information handling procedures	The handling, storage and distribution of information should be protected from unauthorized disclosure or misuse based on standard procedures.
Inventory of removable media	All removable media should be accounted for in an inventory.
Protection of sensitive authentication data	Proper authorization is required for the storage of sensitive authentication data.
Security of system documentation	Protections against unauthorized access should be in place for system documentation.

Description	Control Objective
Exchange of information	See A.10.8 in ISO/IEC 27001:2005.
Information exchange policies and procedures	The exchange of information through the use of all types of communication facilities should be protected through the use of formal exchange policies, procedures, and controls.
Exchange agreements	The exchange of information and software between the organization and external parties should be managed through the establishment of agreements.
Physical media in transit	While physical media is in transit beyond the company's physical boundaries, it should be protected against unauthorized access, misuse, or corruption.
Transportation of media	See A.10.8.3 in ISO/IEC 27001:2005.
Electronic messaging	Electronic messaging, including the data being transmitted, should be appropriately protected.
Business information systems	Information associated with the interconnection of business information systems should be protected by appropriate policies and procedures.
Electronic commerce services	The secure use of electronic commerce services should be governed by policies and procedures.
Electronic commerce	Electronic commerce information passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification through application of appropriate safeguards.
On-Line transactions	See A.10.9.1 in ISO/IEC 27001:2005.
Publicly available information	See A.10.9.2 in ISO/IEC 27001:2005.

Access Control

This domain takes its name from and aligns with the A.11 Access Control section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Business requirement for access control	Based on business and security requirements, access to information, information processing facilities, and business processes should be controlled.
Access control policy	Based on business and security requirements for access, an access control policy should be established, documented, and reviewed.
User access management	See A.11.1.1 in ISO/IEC 27001:2005.
User registration	Access to all information systems and services should be granted and revoked through a formal user registration, modification, and de-registration procedure.
Inactive user accounts	A tracking mechanism should be in place to identify inactive user accounts. Those accounts should be reviewed at least once every 90 days and, if determined to no longer be needed, access should be removed.
Vendor accounts	Accounts for remote maintenance should be enabled for vendors for only as long as needed.
Privilege management	User access privileges should be allocated and controlled based on need-to-know and least-privilege principles.
Access management for terminated users	Access for terminated users should be revoked immediately as documented in termination procedures.
Password management	Access control for information systems should include appropriate password management processes.
Review of user access rights	See A.11.2.4 in ISO/IEC 27001:2005.
User responsibilities	Responsibilities for maintaining effective access controls must be communicated to users.
Communication of password policies and procedures	Password policies and procedures should be communicated to users.

Description	Control Objective
Password use	See A.11.3.1 in ISO/IEC 27001:2005.
Unattended user equipment	See A.11.3.2 in ISO/IEC 27001:2005.
Clear desk and clear screen policy	See A.11.3.3 in ISO/IEC 27001:2005.
Network access control	Appropriate authentication and access control mechanisms should be used to control access to networks.
Policy on use of network services	Use of networks and network services should be described in appropriate policies.
User authentication for external connections	See A.11.4.2 in ISO/IEC 27001:2005.
Two-factor authentication	Two-factor authentication should be implemented for remote network access by appropriate personnel. Technologies used during authentications should include use of a combination of access control technologies, authentication services, and user identification tokens in accordance with applicable standards and requirements.
Equipment identification in networks	See A.11.4.3 in ISO/IEC 27001:2005.
Remote port protection	See A.11.4.4 in ISO/IEC 27001:2005.
Segregation in networks	Information services, users, and information systems should be segregated on networks to enable a graduated set of controls to be applied to networks based on logical groupings of these elements.
Network connection control	See A.11.4.6 in ISO/IEC 27001:2005.
Firewalls	Based on the company’s established security standards, firewall configurations that restrict connections between publicly accessible servers and the systems that store protected information should be implemented and documented.
Session timeout for modems	After a predefined period of inactivity, modem sessions should timeout.
Network routing control	Based on the access control policy, routing controls should be applied for the networks.

Description	Control Objective
DMZ	In order to prohibit direct routes for inbound and outbound internet traffic and to facilitate filtering and screening of network traffic, a DMZ should be in place.
Operating system access control	Appropriate authentication and authorization mechanisms should be used to control user access to operating systems.
Secure log-on procedures	See A.11.5.1 in ISO/IEC 27001:2005.
User identification and authentication	See A.11.5.2 in ISO/IEC 27001:2005.
Password management system	To manage passwords and enforce password policies, a password management system should be used.
Use of system utilities	See A.11.5.4 in ISO/IEC 27001:2005.
Session time-out	See A.11.5.5 in ISO/IEC 27001:2005.
Limitation of connection time	See A.11.5.6 in ISO/IEC 27001:2005.
Application and information access control	Appropriate authentication and authorization mechanisms should control access to information and application functions in an application.
Information access restriction	The least privilege and need-to-know principles should be the basis of the access control policy and for granting user access to information and application functions.
Sensitive system isolation	See A.11.6.2 in ISO/IEC 27001:2005.
Isolation of databases	High business impact data should be isolated by placing such databases in an internal network zone.
Mobile computing and teleworking	See A.11.7 in ISO/IEC 27001:2005.
Mobile computing and communications	See A.11.7.1 in ISO/IEC 27001:2005.
Teleworking	See A.11.7.2 in ISO/IEC 27001:2005.

Information Systems Acquisition, Development and Maintenance

This domain takes its name from and aligns with the A.12 Information Systems Acquisition, Development and Maintenance section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Security requirements of information systems	Information security requirements should be incorporated during all phases of the software development lifecycle, including the design, development, and implementation phases. They should also be applied to all types of information systems including operating and infrastructure systems, business applications, off-the-shelf products, online services, and user-developed applications.
Security requirements analysis and specification	Projects involving development of new information systems or enhancements to existing information systems should include specification, analysis, and documentation of security requirements as appropriate.
Correct processing in applications	Applications should incorporate appropriate internal controls in order to mitigate the risk of errors, data loss, unauthorized modifications, and disclosure of information.
Input data validation	See A.12.2.1 in ISO/IEC 27001:2005.
Control of internal processing	See A.12.2.2 in ISO/IEC 27001:2005.
Message integrity	See A.12.2.3 in ISO/IEC 27001:2005.
Output data validation	See A.12.2.4 in ISO/IEC 27001:2005.
Cryptographic controls	See A.12.3 in ISO/IEC 27001:2005.
Policy on the use of cryptographic controls	See A.12.3.1 in ISO/IEC 27001:2005.
Encryption	Sensitive information in storage and while in transit should be protected, where appropriate, by encryption to ensure confidentiality.
Key management	See A.12.3.2 in ISO/IEC 27001:2005.
Protection of encryption keys	The keys used for encrypting sensitive data should be protected against unauthorized disclosure and misuse according to appropriate policies and procedures.

Description	Control Objective
Key management processes	The lifecycle of keys used to protect sensitive data should be managed according to appropriate policies and procedures.
Protection of disk encryption keys	Management of logical access to disk encryption and decryption keys should be segregated from management of operating system access.
Digital signatures	The authenticity and integrity of sensitive data should be protected through use of digital signatures where appropriate.
Non-repudiation services	Disputes about occurrence or non-occurrence of an event or action should be resolved through use of non-repudiation services where appropriate.
Security of system files	See A.12.4 in ISO/IEC 27001:2005.
Control of operational software	See A.12.4.1 in ISO/IEC 27001:2005.
Changes to default configuration	During installation of software on operational systems, passwords and other vendor-supplied defaults should be changed.
Testing of operational changes	A separate development or test environment should be used for development and testing of changes to system infrastructure and software before implementation into production.
Control of operational code	Development code and compilers should not be kept on operational systems; only operational code should be.
Protection of system test data	Test data should be carefully selected, protected, and controlled. Production data should only be used for production systems, not for development or testing.
Removal of test data from production systems	Production systems should be free from test data before they become operational.
Access control to program source code	See A.12.4.3 in ISO/IEC 27001:2005.
Integrity protection of system files	File integrity monitoring software should be deployed to alert personnel on unauthorized modification of critical system and content files.

Description	Control Objective
Security in development and support processes	See A.12.5 in ISO/IEC 27001:2005.
Software development methodology and guidelines	The development, implementation, and maintenance of software should be governed by a formal, adopted, and documented software development life cycle (SDLC) methodology. The SDLC should be the basis of published policies and procedures practice to ensure delivery of secure software and systems.
Secure design education	Development personnel should be trained to understand and use security controls as part of designing new software.
Threat assessment	Threat assessments and the security controls intended to be part of a software design should be reviewed and approved through a documented management process.
Secure coding guidelines	Common coding vulnerabilities should be communicated and addressed through secure coding guidelines and standards in order to mitigate the risk of exposure or exploitation of information systems.
Security code review	A review process, established in policy and procedure, should be practiced to ensure security design requirements and common vulnerabilities have been addressed in new or modified source code.
Security quality assurance	Testing of the implemented security controls should be performed in accordance with published policies and guidelines.
Change control procedures	See A.12.5.1 in ISO/IEC 27001:2005.
Risk assessment for major changes	When a significant change occurs, a risk assessment should be prepared and reviewed in accordance with formal procedures established to effectively manage risks.
Technical review of system changes	Major system changes should trigger a technical review to be performed to assess the overall security risk.
Restrictions on changes to software packages	See A.12.5.3 in ISO/IEC 27001:2005.

Description	Control Objective
Information leakage	The risk of information leakage through the use and exploitation of covert channels should be controlled and mitigated.
Outsourced software development	See A.12.5.5 in ISO/IEC 27001:2005.
Technical vulnerability management	An effective, systematic, and repeatable management process should be used to reduce the risk of exposure to and exploitation of known technical vulnerabilities.
Control of technical vulnerabilities	See A.12.6.1 in ISO/IEC 27001:2005.
Vulnerability review of information systems	An organization that specializes in application security should review information systems for common technical vulnerabilities.

Information Security Incident Management

This domain takes its name from and aligns with the A.13 Information Security Incident Management section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Reporting information security events and weaknesses	See A.13.1 in ISO/IEC 27001:2005.
Reporting information security events	Timely reporting and escalation of security events through a formal process to appropriate management channels should be established and implemented.
Reporting security weaknesses	Timely reporting and escalation of security weaknesses through a formal process to appropriate management channels should be established and implemented.
Management of information security incidents and improvements	See A.13.2 in ISO/IEC 27001:2005.
Incident management responsibilities and procedures	See A.13.2.1 in ISO/IEC 27001:2005.
Testing of incident response plan	Annual testing of the incident response plan should occur.
Alerts from monitoring systems	The incident management plan should address reviewing and handling alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
Allocation of responsibilities	Alerts should be handled by specific personnel assigned to this role.
Learning from information security incidents	The types, volumes, and costs of information security incidents should be quantified and monitored. Recurring or high-impact incidents or malfunctions should be further analyzed in order to identify needed modifications to the incident response plan.
Training for security breach responsibilities	Staff with security breach responsibilities should receive appropriate training.
Collection of evidence	See A.13.2.3 in ISO/IEC 27001:2005.

Business Continuity Management

This domain takes its name from and aligns with the A.14 Business Continuity Management section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Information security aspects of business continuity management	A business continuity management process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements. The process should minimize the impact on the organization and aid recovery from loss of information assets to an acceptable level through a combination of preventive and recovery controls.
Including information security in the business continuity management process	See A.14.1.1 in ISO/IEC 27001:2005.
Business continuity and risk assessment	See A.14.1.2 in ISO/IEC 27001:2005.
Developing and implementing continuity plans including information security	See A.14.1.3 in ISO/IEC 27001:2005.
Disaster recovery plan	Loss of sensitive data should be recoverable through a documented and tested plan.
Emergency mode operation plan	Continuation of critical business processes designed to protect the security of sensitive information while operating in emergency mode should be documented and tested to prepare for emergency situations.
Business continuity planning framework	See A.14.1.4 in ISO/IEC 27001:2005.
Testing, maintaining, and reassessing business continuity plans	See A.14.1.5 in ISO/IEC 27001:2005.

Risk Management

This domain aligns with the requirements described in section 4, Information Security Management System, in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Risk assessment	On at least an annual basis, a formal risk assessment should be completed to identify vulnerabilities and threats. Mitigation of risks and vulnerabilities identified in accordance with the risk analysis should be taken into account in security measures designed to limit or prevent the impact of security incidents.
Risk treatment	A risk treatment decision should be made for each identified risk to either mitigate or accept the risk. If the risk is accepted, this decision should be made in accordance with risk acceptance criteria.

Compliance

This domain takes its name from and aligns with the A.15 Compliance section in the ISO/IEC 27001:2005 requirements.

Description	Control Objective
Compliance with legal requirements	See A.15.1 in ISO/IEC 27001:2005.
Identification of applicable legislation	See A.15.1.1 in ISO/IEC 27001:2005.
Intellectual property rights (IPR)	See A.15.1.2 in ISO/IEC 27001:2005.
Protection of organizational records	See A.15.1.3 in ISO/IEC 27001:2005.
Data protection and privacy of personal information	See A.15.1.4 in ISO/IEC 27001:2005.
Masking of sensitive data	Before displaying it, sensitive data should be masked.
Prevention of misuse of information processing facilities	See A.15.1.5 in ISO/IEC 27001:2005.
Regulation of cryptographic controls	See A.15.1.6 in ISO/IEC 27001:2005.

Description	Control Objective
Compliance with security policies and standards, and technical compliance	Regular reviews of information system security should be conducted to ensure compliance with the appropriate policies and procedures. Audits of technical platforms and information systems should show compliance with applicable security implementation standards and documented security controls.
Compliance with security policies and standards	See A.15.2.1 in ISO/IEC 27001:2005.
Technical compliance checking	See A.15.2.2 in ISO/IEC 27001:2005.
Information systems audit considerations	Operational systems and audit tools should be safeguarded by controls during information systems audits to protect the integrity and prevent misuse of the audit tools.
Information systems audit controls	See A.15.3.1 in ISO/IEC 27001:2005.
Protection of information systems audit tools	To prevent any possible misuse or compromise, access to information systems audit tools should be limited. Audit trails should be protected from alteration through use of controls such as limiting access, protecting against unauthorized modifications, backing-up files, and use of file integrity monitoring.
Response to compliance findings	Issues arising from non-compliance with legislation, standards, or policies should be tracked and mitigated.
Mechanisms for reporting compliance with legislation, standards and policies	A point of contact should be identified and available to accept reports of compliance concerns or issues by individuals. For when necessary, a formal process should be in place for the escalation, investigation, and resolution of such occurrences.

Privacy

This domain aligns with Microsoft corporate policy regarding privacy of information for customers.

Description	Control Objective
Privacy policy and procedures	A clear policy direction in line with business objectives and relevant laws, regulations, and applicable industry requirements should be set by management to demonstrate support for and commitment to privacy. This direction should result in the issue and maintenance of a privacy policy across the organization, which addresses administrative, physical, and technical safeguards to protect the privacy of information. The privacy policy should be updated as necessary to comply with changes to laws, regulations, and standards.
Privacy policy document	The privacy policies and procedures approved by management should be published and communicated to employees and all relevant third parties.
Retention of privacy policy document	In accordance with applicable laws, regulations, standards, and policies, the privacy policy document should be retained for a period of a minimum of six years from the date of its creation or the date when it last was in effect, whichever is later.
Privacy roles and responsibilities	The responsibility of developing and implementing privacy policies and procedures should belong to a privacy official. An individual should be tasked with receiving and responding to privacy complaints.
Notice	Appropriate notices should: • Be designed and managed to comply with applicable laws, regulations and standards that may specify content, delivery, frequency, documentation, retention, and change requirements. • Inform individuals of the types of information collected, the intended uses of the information, and how that information is shared with third parties. • Include the options available to the individual including how to contact the organization with a privacy complaint or inquiry and the options available for limiting the use and disclosure of their personal information. • Be provided in clear and conspicuous language and presented prior to the collection of personal information.

Description	Control Objective
Choice / consent	Consent will be obtained from an individual through an appropriate mechanism and in a clear and conspicuous manner before their personal information is collected, used, or shared. This consent gathering process will comply with applicable laws, regulations, and standards that may specify content, explicitness, documentation, and retention. The individuals will have the opportunity to choose whether or not to disclose personal information to a third party or to opt out of having it used for a purpose that is incompatible with the purpose for which it was originally collected or subsequently authorized. In the case of sensitive information, use and disclosure should be explicit.
Use and sharing of information	To limit the use and disclosure of personal information and to ensure compliance with applicable laws, regulations, and standards, policies and procedures must be created and maintained to govern its use. Notice and consent requirements will be used in accordance with established policies and procedures. Protected information should be disclosed to third parties only when appropriate safeguards have been put in place to protect the information and should be limited in scope according to all relevant notices and gathered consents.
Integrity	The accuracy and completeness of protected information should be safeguarded, as relevant for its intended use.
Access	An individual should be able to access their personal information, where appropriate, and should also be allowed to correct, amend, or delete their personal information.
Confidential communications	An individual should have an opportunity to request and receive confidential communications of protected information by alternative means or at alternative locations, where appropriate.

Terms & Conditions

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

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

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