

ISO17799 and the Gramm-Leach Bliley Act

Written by Stuart Levine

Overview

The ISO17799 is widely regarded as a broad and comprehensive standard for information security best practices. Derived from the pre existing British Standard 7799, this standard has arguably established itself as the premier benchmark for information security. However, increasing awareness of the dangers present and the need for tight controls has resulted in regulations governing critical verticals and also general corporate governance practices. The earliest such regulation is the Gramm-Leach Bliley Act (GLOBE). This regulation is targeted at financial institutions and places relatively clear requirements on firms to implement and maintain security controls and to ensure that financial data is not compromised due to failures of security at the institution or at any of their partners and vendors. The specific requirements of this act are focused on the data protection aspects of security. Given the wide acceptance of the ISO17799 standard and the regulatory requirements imposed by GLB, the question of overlap and compatibility between the two naturally arises. This paper attempts to show the areas of overlap and illustrate that a particular application of the ISO17799 standard will result in also ensuring GLB compliance.

GLBA

The GLB regulation is focused on data protection. The key elements of the regulation, as related to information security, can be listed as:

- 1) Authentication and Access controls
- 2) Physical access controls
- 3) Business Continuity and Disaster recovery
- 4) Audit and compliance processes
- 5) Policies and Procedures

ISO 17799 and the GLB regulation

The ISO 17799 standard is made up of ten domains that cover most relevant aspects of security. These domains can be mapped to GLB requirements to show that adherence to ISO recommended best practices also results in GLB compliance.

Security Policy

The security policy domain in the ISO 17799 recommends the presence of documented policies that cover the critical areas of security, and a corporate strategy for security. This domain also gives guidelines on making such policies generally available and ensuring employee acknowledgement of these policies.

GLB places requirements of policy in several areas of security including access to sensitive information, general network access control, remote access control, data protection, encryption, business continuity, audit procedures and incident response. The presence of policies and procedures related to these areas is mandatory if the conditions of GLB are to be met. If ISO guidelines are met, clear policies for each of these areas, with assigned owners will be present and available and a review process to ensure currency and implementation will be followed.

Security Organization

This domain within ISO ensures that clear roles and responsibilities are assigned within the organization for security related function and a proper segregation of duties is present. It also recommends proper training for security personnel and measures to protect against misuse of privileges.

While not explicitly set out in GLB requirements these guidelines are, in most cases, necessary precedents to compliance. Without clear definitions of security functions and responsibilities, consistent and efficient implementation of policies and maintenance of security is not credible. A clear corporate commitment to the data protection and privacy preservation aims of GLB will require a security org structure to be in place

Asset Classification and Control

This ISO domain outlines controls that ensure that make sure that IT assets are catalogued and tracked and determines if security levels are assigned to assets depending on importance. It also verifies that there are criteria for addition or change in assets and that external access to assets is controlled. A data classification system is also recommended that assigns hierarchical levels of importance to data based on sensitivity. For e.g. such classification could be Eyes Only, Highly Sensitive, Sensitive, and General. Handling procedures, such as the use of encryption and the destruction of paper with sensitive information, are also defined.

GLB places great emphasis on data protection and the proper handling of sensitive data. Securing sensitive data and the systems on which it resides is an essential aim of the regulation. Adhering to the ISO requirements of this domain ensure that data is always classified and treated based on its importance and that there are clear procedures in place to refer to.

Personnel Security

This domain recommends that the hiring process of the organization needs to be evaluated to ensure that adequate background checks and legal safeguards are in place. Also, employee awareness of security and usage policies should be determined. Third party contractors or consultants are also required to be checked. This domain also recommends termination procedures, disciplinary action and employee commitment through Non Disclosures and confidentiality agreements.

GLB requires clear procedures to ensure proper background checks during the hiring process, including criminal and credit checks for employees with access to sensitive data. Timely and thorough termination procedures and user privilege management as well as general employee awareness are key to protecting data from internal misuse or theft. A high percentage of security breaches are due to current or prior employee actions.

Physical and Environmental Security

Restriction of access to the physical premises need to be tested, making sure that adequate controls are in place to allow only authorized personnel access. Also, redundant power supplies, fire suppression and monitoring controls are to be in place. Securing data carrying systems physically and ensuring no physical access to network connections or cables result in the loss of data is part of this domain. Disposal and transport protection, as well as protection of data in storage media should be in place. Photo ID badge requirements are also part of this domain.

GLB places strong requirements on physical security, including the protection of data carrying media and systems and on mitigation mechanisms. Meeting ISO requirements would satisfy data protection requirements from a physical breach of security.

Communication and Operations Management

Operational procedures need to be verified to ensure that information processing occurs in a safe and protected manner. These should cover standard operating procedures for routine tasks as well as procedures for change control for software, hardware and communication assets. Procedures also include maintenance tasks such as antivirus, patch management, firewall rule management, and intrusion detection.

GLB data protection and privacy requirements place a high burden on implementation, maintenance and monitoring of security controls such as firewalls, intrusion detection and antivirus. The absence of these and other routine procedures such as patch management, can lead to a compromise of the network or of specific systems resulting in the deletion, destruction or corruption of data.

Access Control

This domain demands that access to systems and data be determined by a set of criteria based on business requirement, job responsibility and time period. Access control needs to be constantly verified to ensure that it is available only on a need to know basis with strong justification

GLB places emphasis on this area with requirements to clearly map access requirements to job function and define access as narrowly as possible. There are also requirements for strong authentication and periodic review of access controls. There is a natural and explicit overlap here between the ISO domain and GLB.

Systems Development and Maintenance

If a company is involved in development activity, the assessment to determine if security considerations are a key part at all stages of the development lifecycle and proper testing of applications prior to implementation. Segregation and isolation of development from production systems and a proper change control procedure with security provisions is also recommended.

Preservation of privacy, which is one of the critical aims in the GLB regulation, requires that any internally developed or custom built application is designed, developed and tested with security in mind, as these applications would be interacting with sensitive data. Improper access controls or vulnerabilities at the code level can lead to a greater likelihood of data exposure or theft. Developer isolation from production also ensures that there is clear version and feature control and no unnecessary access to data.

Business Continuity Management

Determining the existence of a business continuity plan that minimizes or eliminates the impact of business interruption is a part of ISO. This plan should be linked to a disaster recovery plan and proper backup procedures need to be in place

Availability of the data and redundancy of systems carrying the data are key parts of GLB and this domain of the ISO is highly relevant to being compliant

Compliance

The presence of mechanisms and periodic audit procedures to verify that the organization is in compliance with all regulatory, contractual and legal requirements is covered in this domain. Audits should include security control checks and the audit results should be retained securely.

Periodic audits and compliance checks are required to maintain GLB compliance.

Conclusion

As can be seen, the ISO standard is not specifically focused on data protection, however compliance with ISO requirements will result in most and in the majority of cases all, of the GLB requirements being met as far as the security of the organization itself is concerned.