Keystone
TECHNOLOGY CONSULTANTS
helping companies understand and implement new technology

Keystone White Paper: Regulations affecting IT

Introduction

This document describes specific sections of current U.S. regulations applicable to IT governance and data protection and maps those requirements to the Keystone solution. This document covers three major U.S. regulatory acts:

- **Sarbanes-Oxley Act of 2002** designed for U.S. public companies. All publicly-traded companies are required to submit an annual report of the effectiveness of their internal accounting controls to the Securities and Exchange Commission (SEC).
- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)** is designed to provide health insurance portability, fraud enforcement, and administrative simplification for the healthcare industry.
- **Gramm-Leach-Bliley Act of 1999**, is designed to enhance the privacy and security of Nonpublic Personal Information (NPI) for consumers doing business with financial institutions, such as banks, brokerage firms, etc.

The Keystone solution does not guarantee a full compliance and addresses only specific sections of the regulations.

Sarbanes – Oxley "SOX"

U.S. Public Company Accounting Reform & Investor Protection Act of 2002

Key Provisions Affecting CIOs

Requirement	Description	Keystone Solution
Section 404 (a) (1) Management Assessment of Internal Controls	State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting	– Asset management (discovery) and reporting – Firewall, intrusion detection, antivirus monitoring and reporting – Patch management and reporting – Backup management
Section 409 (1) Real Time Issuer Disclosures	Each issuer reporting under section 13(a) and 15 (d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English…	Managed security services and managed asset management ensure the availability of such information. **Reliability:** – System availability reports – Network and CPU utilization – Overall alerts and notification system **Security:** – Vulnerability assessments – Firewall monitoring and alerting – IDS Monitoring and alerting – Antivirus monitoring and alerting – Patch management – Data backup management

HIPAA Security Rule Standards and Implementation Specifications

Administrative Safeguards (164.308)

Physical Safeguards (164.310)

Technical Safeguards (164.312)

Policies & Procedures and Documentation Requirements (164.316)

General Rules (Section 164.306)	Keystone Solution
164.306(a)(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the entity creates, receives, maintains, or transmits.	**Availability:** – System availability monitoring and reports – Network and CPU utilization monitoring and reports – Overall alerts and notification system – Exchange, Notes, email application monitoring **Integrity:** – Vulnerability assessments – Firewall monitoring and alerting – IDS Monitoring and alerting – Antivirus monitoring and alerting – Patch management **Confidentiality (data encryption):** – None
164.306(a)(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information	**Protection:** – Vulnerability assessments – Firewall monitoring and alerting – IDS Monitoring and alerting – Antivirus monitoring and alerting – Patch management assessment – Asset management
164.306(a)(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required	– Firewall incident notifications – IDS incident notifications – Antivirus incident notifications – Vulnerability assessments
164.306(a)(4) Ensure compliance by its workforce	**Compliance:** – None (internal Security policies)

Administrative SAFEGUARDS (Section 164.308)	Keystone Solution
164.308(a)(1) Security Management Process: – Risk Analysis – Risk Management – Sanction Policy – Information System Activity Review	**Risk Analysis & IS Review:** – Vulnerability assessments – Firewall monitoring and alerting – IDS Monitoring and alerting – Antivirus monitoring and alerting – Patch management assessment – Asset Management
164.308(a)(4) Information Access Management – Isolating Healthcare Clearinghouse Function (“*If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.”)*	– Firewall monitoring and alerting – IDS Monitoring and alerting
164.308(a)(6) Security Incident Procedures – Response and Reporting	**Response and Reporting:** – Firewall monitoring, alerting and incident reporting – IDS monitoring, alerting and incident reporting – Antivirus monitoring, alerting and incident reporting – Backups monitoring and notification
164.308(a)(7) Contingency Plan: – Data Backup Plan – Disaster Recovery Plan – Emergency Mode Operation Plan – Testing and Revision Procedure – Applications and Data Criticality Analysis	– Monitor whether the backups successful

Gramm-Leach-Bliley Compliance Matrix

Requirement	Description	Keystone Solution
Section 314.3(a) Information security program	You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in Section 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.	**Administrative, Technical Safeguards:** See section 314.4 (b)
Section 314.3(b) Define objectives	1. Insure the security and confidentiality of customer information; 2. Protect against any anticipated threats or hazards to the security or integrity of such information; and 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.	**Keystone MSSP program:** Provides MSSPs with guidelines (Customer Needs Assessment document, Firewall best practices, etc.) on best security practices and best-of-breed security technologies support for managed security services See section 314.4 (b)
Section 314.4 (b) Identify reasonably foreseeable internal and external risks	Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: 1. Employee training and management; 2. Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and 3. Detecting, preventing and responding to attacks,	– Vulnerability assessments scans and reports – Firewall monitoring, alerting and report – IDS Monitoring, alerting and reporting – Antivirus monitoring, alerting and reporting – Patch management – Backup services

	intrusions, or other systems failures.	
Section 314.4 (c) Design and implement information safeguards	Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.	**Managed Services:** – Managed firewall service – Managed intrusion detection – services – Managed antivirus services – Managed vulnerability assessment services
Section 314.4 (d) Oversee service providers	Oversee service providers, by: 1. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and 2. Requiring your service providers by contract to implement and maintain such safeguards.	Keystone MSSP program helps MSPs to become self-sufficient MSSPs to help their customers to comply with various regulations and enables them to offer the following **Managed Services:** – Managed firewall service – Managed intrusion detection services – Managed antivirus services – Managed vulnerability assessment services
Section 314.4 (e) Evaluate and adjust information security program	(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.	

Keystone Technology Consultants, founded in 1993, provides information technology support, network management, hosted solutions, and high level technology strategy to small and medium sized businesses throughout the north-eastern Ohio area. As a Microsoft Gold Certified Partner, Keystone possesses numerous certifications and skills, and specializes in reducing the cost of information technology while creating an environment that helps its clients define and reach their goals. You may visit them on the web at www.keystonecorp.com.