SEA™

SOFTWARE ENGINEERING OF AMERICA®

System i Compliance

and

Sarbanes-Oxley

An Overview of How iSecurity Works with Sarbanes-Oxley Requirements Using COBIT 4.0

Legal Notice: This document reflects the understanding of Software Engineering of America of System i security and audit compliance related to the Sarbanes-Oxley Act of 2002 requirements using COBIT guidelines. SEA is not in a position to guarantee and assumes no responsibility that the implementation of the recommendations in this whitepaper ensures a complete and full compliance with all aspects of the Sarbanes Oxley Act. The information is provided as an informational piece. SEA advises users to undertake their own research and advice to satisfy their required level of compliance with the Act.

Introduction

The Sarbanes-Oxley Act of 2002 (SOX) has significantly impacted the state of business and its surrounding regulatory environment. Corporate scandals have promoted higher governance standards, with new laws being continuously enacted and modified to ultimately enhance the quality of corporate reporting. The Act itself aims to enhance corporate governance through measures that will strengthen internal checks and balances. While SOX does not specifically provide guidelines related to Information Technology Controls, the guidelines developed under the Control Objectives for Information and related Technology (COBIT) developed by the IT Governance Institute (ITGI) (www.itgi.org) serve as the basis for many security and IT audit professionals in regards to Sarbanes-Oxley compliance.

Sarbanes-Oxley and IT

Organizations that have to comply with SOX have realized that IT controls are essential to complying with Section 404 of the Sarbanes-Oxley Act. CIO's now must be responsible for understanding Sarbanes-Oxley and translating the organizations overall SOX needs into a compliance plan to specifically address IT Controls.

> *"Section 404 of the Act directs the Commission to adopt rules requiring each annual report of a company, to contain (1) a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) management's assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the company's internal control structure and procedures for financial reporting. Section 404 also requires the company's auditor to attest to, and report on management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board.*
>
> *(Source: Securities and Exchange Commission)*

Executive managements reliance and dependence on real time financial and corporate data and IT's crucial integration of highly efficient technology systems to accomplish key business processes make IT controls key components of complying with the Act.

System i & Sarbanes-Oxley

While Sarbanes-Oxley compliance refers to an entire organization, and solutions that must be implemented to span the entire enterprise, corporate firewalls and the native IBM security settings do not effectively address highly critical data that resides on a companies System i. More importantly, much of the data that resides on the System i is protected from outside users, but with corporate governance's primary focus relating to internal controls, it is important to consider specific controls for critical System i data when developing an IT security plan.

Cobit Objectives & iSecurity Products

Below is a table that specifically details how specific iSecurity products can help organizations fulfill specific Cobit objectives. The primary explanation of each objective can be found within this document along with greater detail about how iSecurity assists in meeting these objectives.

Cobit Objective	Summary	iSecurity Products
DS 5.1	**Management of IT Security**	Firewall, Password, Audit, Action, User Management, Visualizer
DS 5.3	**Identity Management**	Firewall, Password, Audit, Action, User Management, Visualizer, View, Capture, Journal
DS 5.4	**User Account Management**	Audit, Action, Assessment & Firewall
DS 5.5	**Security Testing, Surveillance and Monitoring**	Firewall, Audit, Action & Capture
DS 5.7	**Protection of Security Technology**	Firewall, Audit, Action, Anti-Virus
DS 5.9	**Malicious Software Prevention, Detection and Correction**	Firewall, Audit, Action & Anti-Virus
DS 5.10	**Network Security**	Firewall, Audit, Action
DS 10.1	**Identification and Classification of Problems**	Firewall, Audit, Action
AI 3.2	**Infrastructure Resource Protection and Availability**	Firewall, Audit, Action

Detailed Control Objectives

DS5 Ensure Systems Security

Deliver and support (DS) under COBIT 4.0 is related to the delivery of required services, including the management of security and data within the enterprise.

DS5.1 Management of IT Security

COBIT Guideline

"Manage IT security at the highest appropriate organizational level, so the management of security actions is in line with business requirements."

---

iSecurity Products: Firewall, Password, Audit, Action, User Management, Visualizer

iSecurity **Firewall** can be used to manage, control and protect access to company data from all TCP/IP access points (including ODBC, FTP, remote command, and more...). Firewall can assist management in developing and managing IT Security by logging all approved and rejected activities as well as printing out all security rules and definitions used in Firewall to assess overall System i security. **Audit** can also assist management personnel with the implementation of security rules and definitions in conjunction with security policies that are created and enforced in the enterprise. Audit is an application that examines events in real time, and triggers alerts and other responsive actions to potential threats using **Action**. Audit expands the ability of the native System i operating system as well as provides an easy to use, intuitive interface which makes working with a large number of system values and parameters much easier for IT Managers. iSecurity's **Assessment** can be run at any given time to give a detailed view of security settings to ensure system setup is in compliance with standards determined by IT management.

DS5.3 Identity Management

COBIT Guideline

"All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository. Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights."

---

iSecurity Products: Firewall, Password, Audit, Action, User Management, Visualizer, View, Capture, Journal

Using **Password** manager and OS/400 system values, IT personnel can ensure that inactive profiles, default passwords (where the username is the same as the password) and password length are managed to protect identities and user access. **Firewall** can be used to address all issues of network TCP/IP access related to the 53 System i exit points to deliver an Intrusion Protection Solution. Firewall gives small to large businesses the ability to set up specific rules to ensure that sensitive data is only accessed by authorized persons under specific conditions and will assist in compliance related to User Access Rights. The ability to adopt a higher level of granularity is required according to DS5.3 and should be implemented such that a user can perform no more than they are required or need to. Using **Audit & Action** IT management can increase their level of compliance by implementing an Intrusion Detection System that can escalate and respond to threats in real time related to user access. **View** can be used to selectively hide records or data in selected fields within records from selected users that should not have the ability to view, modify or edit specific data on your System i.

DS5.4 User Account Management

COBIT Guideline

"Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are

contractually arranged for all types of users. Perform regular management review of all accounts and related privileges."

---

iSecurity Products: Audit, Action, Assessment & Firewall

Assessment is the first step to understanding the current status of your user settings. This module can be used extensively by IT management to understand current settings in place and assess changes in system values compared to your baseline reference.

Once the assessment of your System i user accounts has taken place, **Firewall** can provide you with the necessary information and management tools for all user profiles, active/inactive passwords, password existence, last sign-on and a log of all failed sign-on attempts so that User Account Management can be administrated and monitored according to your IT Security plan. **Audit** and **Action** assist IT Management in monitoring all settings and system values, and proactively respond to user account issues through escalations and pre-defined procedures in an IT plan.

DS5.5 Security Testing, Surveillance and Monitoring

COBIT Guideline

"Ensure that IT security implementation is tested and monitored proactively. IT security should be reaccredited periodically to ensure the approved security level is maintained. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. Access to the logging information is in line with business requirements in terms of access rights and retention requirements."

---

iSecurity Products: Firewall, Audit, Action & Capture

Firewall gives enterprises the ability to log and report on all TCP/IP activity. With Firewall, businesses can adhere to DS5.5 by periodically reviewing all rules and definitions in a convenient interface or by printing the security parameters and values for review. In addition to Firewall**, Audit** provides detailed logging and reporting on all security audit journal files (including User Activity, Object Access, Application Usage, etc..). **Action,** when used with Firewall and Audit can provide the real time monitoring and response necessary when threats are discovered. **Capture** can provide real time monitoring and security surveillance by automatically capturing and saving user activity as displayed on System i workstation screens.

DS5.7 Protection of Security Technology

COBIT Guideline

"Ensure that important security-related technology is made resistant to tampering and security documentation is not disclosed unnecessarily, i.e., it keeps a low profile. However, do not make security of systems reliant on secrecy of security specifications."

---

iSecurity Products: Firewall, Audit, Action, Anti-Virus

Protection of security related technology from tampering becomes easier when using **Firewall,** as it can be used to prohibit unauthorized access via the network to update, delete and insert data into files. When system protection is a very high concern, **Anti-Virus** can provide ongoing detection and prevention of malicious code from entering your System i and being distributed across the enterprise.

DS5.9 Malicious Software Prevention, Detection and Correction

---

COBIT Guideline

"Ensure that preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.)."

---

iSecurity Products: Firewall, Audit, Action & Anti-Virus

Anti-Virus can provide your System i with protection against viruses and malicious code, while **Firewall** can provide IT management with protection against unauthorized access to files.

DS5.10 Network Security

COBIT Guideline

Ensure that security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) are used to authorize access and control information flows from and to networks."

---

iSecurity Products: Firewall, Audit, Action

Using **Firewall** provides security protection for **all** 53 System i Server Exit Points (including ODBC, Telnet, TCP/IP, FTP, remote command, and more...), including protection for both incoming and outgoing IP addresses. Together with our **Audit** and **Action** modules, businesses are able to provide complete network security with pro-active responses to network security breaches and threats.

DS10.1 Identification and Classification of Problems

COBIT Guideline

"Implement processes to report and classify problems that have been identified as part of incident management. The steps involved in problem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Problems should be categorized as appropriate into related groups or domains (e.g., hardware, software, support software). These groups may match the organizational responsibilities or the user and customer base, and are the basis for allocating problems to support staff."

---

iSecurity Products: Firewall, Audit, Action

Firewall and **Audit** provide complete Intrusion Prevention and Detection for the System i, and when used in conjunction with **Action** can provide real time identification and the necessary corrective response to problems. **Action** offers enterprises the ability to implement processes related to incident identification and notification of specific personnel. These include escalation procedures as well as running CL commands in response to threats and breaches.

AI 3 Acquire and Maintain Technology Infrastructure

AI 3.2 Infrastructure Resource Protection and Availability

COBIT Guideline

"Implement internal control, security and audit ability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated."

---

iSecurity Products: Firewall, Audit, Action

Firewall and **Audit** can provide complete history logs, and data trails in regards to network security as well as system resource availability and monitoring. Within iSecurity **Audit**, System Control can identify critical computer resource change events as well as highly questionable behavior (not in accordance with behavior models defined in WRKACTJOB) and provide corrective notifications and actions via **Action** to IT personnel. Complete audit logs and reports can be generated to make sure internal security is maintained.