

White Paper

Sarbanes Oxley and iSeries Security, Audit and Compliance

**This White Paper was written by
AH Technology
Distributors of *iSecurity*
a suite of iSeries security products developed by
Raz-Lee Security**

April 2006

The Sarbanes-Oxley Act

Please refer to the legal notice at the end of the document

Background: Sarbanes Oxley (SOX), COBIT (Control Objectives for Information and related Technology)

The Sarbanes Oxley Act (SOX) was enacted in 2002 to avoid a repeat of cases like Enron, Tyco, Worldcom and other similar companies in the USA.

The objective of SOX is to protect investors by improving the accuracy and reliability of corporate disclosures. The Act carries criminal and civil penalties to executive management and board of directors in case the Act requirements are not met. Under Section 404 of the Act, executives are required to certify and demonstrate that they have established and are maintaining an adequate internal control structure and procedures for financial reporting.

Whilst the spirit of the Act is clearly to ensure a much higher level of security and integrity of corporations, the actual words of the Act are not detailed enough to provide a sufficiently clear set of guidelines for the average corporation to go by.

Many in the security and audit field turn to the guidelines development under the name of Control Objectives for Information and related Technology (COBIT®) developed by the USA based IT Governance Institute (ITGI) (www.itgi.org)

On its website, it is said: "COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations.

Compliance & iSeries Security Policies

This document describes the COBIT objectives considered by AH Technology as the most relevant to iSeries Security, Audit and Compliance. Where applicable, the document provides references to iSecurity functions that can be useful in achieving the required level of COBIT (therefore Sarbanes Oxley) compliance. It is recommended that iSeries users gain access to COBIT documentation to appraise the complete list of requirements.

iSeries Sites

The iSeries comes equipped with a significant number of tools built-in to its Operating System. Such tools cover areas like object level security, built in logging (Journals including the Security Audit Journal, message queues, history log etc), and built in monitoring (message queues etc.).

This document only refers to the 'technical' aspects of implementing the guidelines. Many other documents are available to deal with suggestions and recommendations of the available methodologies for a corporation to go about achieving the required level of compliance.

Many sites are using the iSecurity software to complement iSeries native tools. The relevant COBIT clauses where users can draw benefits from the use of iSecurity are listed below:

Sarbanes Oxley Requirements Summary

IMPORTANT

1. High Exposure (See the section describing DS5.3)

In a case where

- a. An iSeries system has an ERP application that gives its users authority to view, copy, change, and delete its objects. (Many Green Screen Applications do..)
And
- b. It also possible to access the iSeries using TCP/IP access such FTP, SQL, ODBC, DDM and other (using tools such as MS Access, MS Excel, IBM Client Access etc) - Most sites allow such access)

Application data can be viewed, copied, changed or deleted with the operating system offering no mechanism to protect, log or report such transactions.

2. Non Compliance with Sarbanes Oxley Act (Refer to DS5.3)

In the case where the application is a financial application the above exposure exists, the iSeries system is **NOT COMPLIANT** with the Sarbanes Oxley Act.

The Sarbanes Oxley clearly requires that a system MUST be able to identify any attempt to modify a financial record

Table 1: COBIT Objectives Description and iSecurity Relevant Functions

COBIT Objective	Description	iSecurity Functions that can increase compliance
DS5.1	Manage Security Measures	Firewall, Password, Audit, Action, User Management, Visualizer
DS5.2	Identification, Authentication, Access	Firewall, Password, Audit, Action, User Management, Visualizer
DS5.3	Security of Online Access to Data	Mainly Firewall, Audit, Action for improved escalation and response. (*) Please review this section for object authority discussion and IMMEDIATE NON COMPLIANCE.
DS5.5	Management Review of User Accounts	Audit, Action, Assessment,
DS5.7	Security Surveillance	Firewall, Audit, Action
DS5.10	Violation and Security Activity Reports	Firewall, Audit, Action
DS5.17	Protection of Security Functions	Firewall, Audit, Action, Anti Virus
DS5.19	Malicious Software Prevention	Anti Virus

DS5: DELIVERY AND SUPPORT - Ensures Systems Security

DS5.1: Manage Security Measures

This objective addresses the need for establishing an IT security implementation which ensures that security policies and their implementations satisfactorily meet the business objectives and risk exposure.

This objective requires not only implementation of the security policies but also regular checks to ensure the on going compliance of the system setup with the policies.

iSecurity Firewall, Audit & Action, Assessment

1. **Firewall** can be used to manage, control and protect access to company data from all TCP/IP access points into the system (ODBC, FTP, SQL, Client Access, Access, Excel etc). **Firewall** can log all approved and rejected activities, produce reports as required, or with the 'cooperation' of **Audit** and **Action**, deliver immediate escalation via email, SMS etc. as well as real time response to threats.
2. The **iSecurity Assessment** module should be involved on a regular basis to ensure system setup has not changed.

DS5.2: Identification, Authentication, and Access

"The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication, and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections, and other system (network) entry ports from accessing computer resources."

Firewall (including Password Manager) Audit and Action

1. Use **Password** manager and OS system values to ensure inactive users are disabled; passwords are changed regularly and trivial password construction is not possible.
2. Use **Firewall** to address all issues of network TCP/IP access (see DS5.1) to deliver Intrusion Protection Solution (IPS) with **Audit** and **Action** delivering an IDS (Intrusion Detection Solution) - immediate escalation and real-time response to threats. **Firewall's** flexibility allows setting up specific rules to ensure sensitive data is accessed only by the authorised person (linking a task to a specific IP (PC) in the office, disallowing access to data from outside the office, etc.).

DS5.3: Security of Online Access to Data

“IT management should implement procedures in line with a security policy that provides access and security controls based on the individual’s demonstrated need to view, add, change, and delete data”

Firewall (Also see response to DS5.1, DS 5.2)

1. This objective requires that, in a networked environment, security should be implemented so that access to data via authorised personnel is such that where ever possible the highest level of granularity should be adopted to ensure the user can perform no more than is required. Example: Only read data, but not update or delete.
2. Use **Firewall** to address all issues of network TCP/IP access (see DS5.1) to deliver Intrusion Protection Solution (IPS). The iSeries OS enables further granularity by allowing software to separately control different actions (Verbs) like: READ, WRITE, DELETE, RENAME. CREATE OBJECT, CREATE LIBRARY

DANGER: Without TCP/IP protection (by software such as Firewall), your AS/400, iSeries system is **NON COMPLIANT WITH THE SARBANES OXLEY ACT** if the following conditions exist:

- a. Each and every legitimate user of an application has object authority to read (view), change, copy or delete data records.
- b. The application is a **financial** application.

Without TCP/IP protection, users with the above authority can gain TCP/IP access to alter existing financial records. The Act requires the ability to identify any attempt to change financial records.

Native OS DOES NOT provide a mechanism to manage, control and protect data against TCP/IP transactions (FTP, ODBC, SQL, DDM using tools such as MS Access, MS Excel, IBM Client Access, FTP From DOS etc)

DANGER: If your financial application is a **green screen application**, there is a **GRAVE CHANCE** your system is **NON COMPLIANT** with the Act!.

DS5.5: Management Review of User Accounts

“Management should have a control process in place to review and confirm access rights periodically. A comparison of resources with recorded accountability should be made to help reduce risk of errors, fraud, misuse, or unauthorized alteration”

iSecurity Assessment Module, Audit and Action.

1. There are a number of **iSecurity** features which address this requirement. Start with **iSecurity Assessment** module to record your current settings. Review and change as required, meeting your business objectives and security policies. Run the **iSecurity Assessment** again and keep as your reference. From then on execute the **iSecurity Assessment** module on a regular basis and compare its reports to your reference.
2. As a complementary measure use **Audit** and **Action** to monitor all settings they can detect (System values). Set the software to escalate alerts when a setting is changed.

DS5.7: Security Surveillance

“IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner”

Firewall, Audit and Action

1. **Firewall** ensures every TCP/IP activity is logged and reported. With **Audit** and **Action**, you can ensure that an attempt to violate security is escalated immediately with action taken in real-time.
2. **Audit** and **Action** deliver the same result when monitoring the Security Audit Journal as well as system events and messages.

DS5.10: Violation and Security Activity Reports

“IT security administration should ensure that violation and security activity is logged, reported, reviewed, and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know.

Firewall, Audit and Action

1. Please refer to information in objective 5.7. **Firewall**, **Audit** and **Action** can all provide regular reports (in any time interval required) in addition to the continuous monitoring, immediate detection, escalation and response.

DS5.17: Protection of Security Functions

“All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, organizations should keep a low profile about their security design, but should not base their security on the design being secret.”

Firewall, Audit, Action and AntiVirus

1. **Firewall** can be used to ensure no unauthorized access via the network can update / delete / insert data into files. The **Anti-Virus** module can perform on going detection protection and immediate removal of viruses.

DS5.19: Malicious Software Prevention

Detection and Correction

“Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective, and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response, and reporting.

iSecurity Anti Virus, Firewall, Audit & Action.

1. Use the **Anti Virus** module to ensure viruses and malicious code are detected and removed as soon as it is possible.
2. **Firewall** will secure files from unauthorised attempt via the network to change or delete data.

Legal notice: The document reflects AH Technology understanding of iSeries SECURITY and AUDIT compliance with the Sarbanes Oxley Act (SOX) requirements via the use of COBIT. Whilst AH Technology believes that adopting the measures recommended in this white paper will considerably increase iSeries compliance with SOX, AH Technology is not in a position to guarantee that the implementation of the above recommendations ensures a complete and full compliance with ALL aspects of the Act. The information provided is of general nature and users must take their own research and advice to satisfy their required level of compliance with the Act.