
Raz-Lee Security White Paper

**Adottare la struttura di COBIT per soddisfare la normativa
Sarbanes Oxley ed altre regole di conformità su IBM System i**

Gennaio 2007

**Questo whitepaper è stato scritto da
AH Technology
Distributore di *iSecurity*
Tradotto in italiano da Avnet Partner Solutions**

Legal notice: This document reflects the understanding of Raz-Lee Security and AH Technology of System i SECURITY and AUDIT compliance with the Sarbanes Oxley Act (SOX) requirements via the use of COBIT. While both companies believe that adopting the measures recommended in this white paper will considerably increase System i compliance with SOX, they are 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 undertake their own research and advice to satisfy their required level of compliance with the Act.

SARBANES-OXLEY

Sarbanes Oxley (SOX), COBIT (obiettivi di controllo per informazione e riguardanti Tecnologia) La normativa Sarbanes Oxley (SOX) è stata promulgata nel 2002 per evitare la ripetizione dei casi come Enron, Tyco, Worldcom ed altre aziende simili negli U.S.A.

L'obiettivo di SOX è proteggere gli investitori migliorando l'esattezza e l'affidabilità delle comunicazioni aziendali. Tale regolamento prevede condanne penali e civili per gli amministratori nel caso in cui i requisiti di legge non vengano rispettati. La parte 404 della normativa stabilisce che le organizzazioni devono certificare e dimostrare che hanno costituito e applicato le procedure di controllo per l'analisi finanziaria.

Mentre lo spirito di SOX è chiaramente di accertare un più alto livello di sicurezza e di integrità delle società, le parole reali di tale normativa non sono abbastanza dettagliate per fornire una guida di riferimento chiara per il raggiungimento degli obiettivi della stessa.

Molti nel campo degli audit e security fanno riferimento alla guida Obiettivi di controllo per informazione e tecnologia (COBIT®) sviluppata dagli U.S.A. e basata sull'Istituto di controllo (ITGI)(www.itgi.org)

Sul relativo Web site, è detto: "COBIT è una struttura IT di controllo e toolset di sostegno che permette che i responsabili colmino la lacuna fra i requisiti di controllo, le edizioni tecniche ed i rischi di affari. COBIT gli permette lo sviluppo politico libero e la buona pratica per controllo nelle organizzazioni societarie.,,

Politiche di sicurezza per il server i di IBM

Questo documento descrive gli obiettivi di COBIT considerati da noi come i più importanti per la sicurezza e verifica di conformità del System i. Dove applicabile, il documento fornisce i riferimenti alle funzioni di iSecurity che possono essere utili nel realizzare il livello richiesto di conformità a COBIT (quindi Sarbanes Oxley). Si consiglia agli utenti del System i che accedono alla documentazione di COBIT di valutare la lista completa dei requisiti.

System i Sites

Il system i viene dotato di un numero significativo di tools di sicurezza incorporati nel proprio sistema operativo. Tali tools permettono la gestione della sicurezza a livello dell'oggetto, utilizzando code messaggi, history log, security e audit journal.

Questo documento rappresenta una guida tecnica. Altri documenti forniscono alle società i riferimenti e le raccomandazioni, le metodologie per realizzare il livello richiesto di conformità. Molti siti stanno usando il software di iSecurity in complemento ai tools nativi del system i.

Di seguito vengono elencate le clausole di COBIT dove gli utenti possono trarre i benefici dall'uso del iSecurity.

Sommario dei requisiti di Sarbanes Oxley

IMPORTANTE

1. Grave esposizione (vedere la sezione DS5.3)

- a. Un system i ha un'applicazione ERP che permette ai relativi utenti di osservare, copiare, modificare e cancellare i relativi oggetti.
- b. Possibilità di accesso tramite i protocolli TCP/IP del system i quali FTP, SQL, ODBC, DDM ed altri tools quali MS Access, MS Excel, IBM System i Access ecc. (la maggior parte dei siti consentono tali accessi) I dati di applicazione sono dunque visionati, copiati, modificati o cancellati tramite il sistema operativo non offrendo nessun meccanismo per proteggere, annotare o segnalare tali transazioni.

2. Mancanza di conformità alla normativa di Sarbanes Oxley (riferimento a DS5.3)

Quando un'applicazione ha le suddette esposizioni, il system i non è CONFORME con Sarbanes Oxley.

Sarbanes Oxley richiede chiaramente che un sistema DEVE potere identificare tutte le modifiche inerenti registrazioni finanziarie.

Tabella 1: Descrizione degli obiettivi di COBIT e funzioni principali di iSecurity

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	View, Capture and Journal. Also Firewall, Audit, Action for improved escalation and response. This section should be reviewed immediately in light of its major impact on non-compliance issues.
DS5.4	User Account Management	Password, User Management
DS5.5	Management Review of User Accounts	Audit, Action, Assessment
DS5.7	Security Surveillance	Firewall, Audit, Action, Capture
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	Firewall, Audit, Action, Anti Virus

DS5 :CONSEGNA E SUPPORTO - Assicura la sicurezza del sistema

DS5.1: Gestire la rilevazione del livello di sicurezza

Questo obiettivo risponde all'esigenza di utilizzare un'applicazione di sicurezza che soddisfi gli obiettivi di business e che evidenzii le esposizioni a rischi.

Questo obiettivo richiede non solo l'esecuzione delle politiche di sicurezza ma anche controlli normali per accertare la conformità del sistema gestito con le politiche assunte.

iSecurity Firewall, Audit & Action ,Assessment

1. FIREWALL può essere usato per controllare e proteggere l'accesso ai dati aziendali da tutti i TCP/IP access points (ODBC, ftp, SQL, accesso del system i, MS access, MS Excel ecc.). FIREWALL può registrare tutte le attività autorizzate, quelle rifiutate, produrre rapporti a richiesta e usando AUDIT e ACTION, comunicare l'anomalia via email, SMS ecc. così come intraprendere azioni di risposta in tempo reale alle minacce.

2. iSecurity ASSESSMENT dovrebbe essere utilizzato regolarmente per garantire che il security setup del sistema non venga modificato.

DS5.2: Identificazione, autenticazione ed accesso

L'accesso e l'utilizzo dei dati dovrebbero essere limitati da regole di identificazione, di autenticazione, che collegano gli utenti e le risorse. Tali meccanismi dovrebbero evitare che utenti non autorizzati, collegamenti al sistema non consentiti utilizzino risorse del sistema.

Firewall,Password Manager Audit & Action

1. Utilizzare PASSWORD MANAGER ed i valori di sistema di OS400 per accertare che gli utenti inattivi siano disabilitati; le parole d'accesso vengano cambiate regolarmente e non sia possibile l'utilizzo di parole d'accesso banali.

2. Usare FIREWALL per fare in modo che gli accessi in TCP/IP dalla rete (vedere DS5.1) utilizzino il protocollo Intrusion Protection Solution (IPS) che consenta ai pacchetti AUDIT ed ACTION, tramite il protocollo IDS (Intrusion Detection Solution),di intraprendere le azioni di risposta alla minaccia. La flessibilità di FIREWALL consente di impostare regole specifiche per accertare che i dati sensibili vengano raggiunti soltanto dalla persona autorizzata (link tra azione e ip address .).

DS5.3: Sicurezza di accesso ai dati

“L’Amministrazione IT dovrebbe attuare le procedure in conformità con una politica di sicurezza che fornisca i comandi di sicurezza e di accesso basati sull’ effettivo bisogno dell’utente di visionare, aggiungere ,cancellare e modificare dei dati.,,

Firewall (vedere anche la risposta a DS5.1, al DS 5.2)

1. Questo obiettivo richiede che, in un ambiente di rete, la sicurezza dovrebbe essere effettuata in modo che l’accesso ai dati da parte degli utenti autorizzati sia tale che esso non possa effettuare nient’altro di piu’ di quanto concesso. Esempio: Soltanto dati protetti, ma non aggiornamento o cancellazione.
2. Usare FIREWALL per forzare tutti gli accessi TCP/IP dalla rete ad emettere un Intrusion Protection Solution (IPS) (vedere DS5.1). L’OS400 del System i consente di controllare esclusivamente le azioni come: READ, WRITE, DELETE, RENAME, CREATE OBJ, CREATE LIB.

PERICOLO: Senza protezione del TCP/IP (via software con il Firewall), il vostro system i è **NON COMPLIANT CON LA NORMATIVA di SARBANES OXLEY** se sussistono le seguenti circostanze :

a. Ogni utente dell’applicazione ha tutte le autorità sugli oggetti del sistema (*allobj authority)

b. L’applicazione è un’applicazione finanziaria

Senza protezione degli exit point TCP/IP, gli utenti con l’autorizzazione *allobj possono accedere ed alterare qualsiasi record. La normativa SOX richiede la capacità di identificare tutti i tentativi di modifica dei records. i5/OS nativo non fornisce un meccanismo per controllare e proteggere i dati da transazioni TCP/IP (ftp, ODBC, SQL, DDM tramite MS access, MS Excel, Access del system i di IBM, ftp del DOS, ecc.).

PERICOLO: Se la vostra applicazione finanziaria è una Green Screen Application(5250), **ci sono più di probabilità che il vostro sistema sia NOT COMPLIANT con la normativa SOX!**

3. Usare **VIEW** per nascondere selettivamente interi records, o i dati nei campi selezionati all’interno dei records, dagli utenti selezionati, senza dovere fare i cambiamenti alle applicazioni. L’interfaccia GUI è usata definire i test di verifica per i records/campi da nascondere.

4. **CAPTURE** può essere usato per registrare le immagini 5250 dell’ attività dell’utente . Le sessioni “catturate” possono essere gestite dal modulo ACTION, a fronte di una possibile minaccia di sicurezza, quale accesso a file protetti o ad attività fuori orario consentito. Le immagini catturate possono essere archiviati per gli scopi legali e per successive analisi.

5. **JOURNAL** fornisce la possibilità per generare uno storico dell’attività per ogni applicazione registrando dati quali numero del cliente, numero paziente, numero di ipoteca, ecc., raccolti da tutti i data files che compongono un’applicazione. Il giornale fornisce l’immagine dei records, prima e dopo le modifiche

DS5.4 : Gestione degli USER

“L'amministratore di sistema dovrebbe stabilire le procedure per accertare l'attività degli utenti al fine di delineare il loro margine di operabilità,. Tra queste dovrebbe esserci quella che stabilisce come vengono assegnate le autorizzazioni. La sicurezza di accesso di terze parti dovrebbe essere definita contrattualmente . Inoltre nei contratti di outsourcing dovrebbero essere contemplati i rischi, comandi di sicurezza e procedure per i sistemi e reti.,,

Parola d'accesso ed amministrazione dell'utente

1. La gestione degli utenti dovrebbe essere vista come una delle pietre angolari della conformità a SOX .Senza politiche rigorose ,certamente realizzabili, un'azienda si troverebbe di fronte ad una attività degli utenti fuori controllo che potrebbe generare gravi danni.

2. Le caratteristiche di autenticazione di **USER MANAGEMENT** sono volte ad accertare l'identità dell'utente.Sul System i sono stati adottati metodologie di autenticazione simili a quelle dei PC con richiesta di domande e risposte personali, così come la generazione univoca di una user password sconosciuta all'amministratore e utente che rimane attiva finchè l'utente non decide di cambiarla.

3. **PASSWORD** permette la gestione semplice e centralizzata delle normative per le parole d'ordine. OS/400 nativo fornisce alcuni dei valori di sistema, tuttavia, non in un contesto di gestione avanzata. **PASSWORD** prende in carico la gestione delle password integrando quando già fornito da i5/OS .

DS5.5: Gestione del controllo degli utenti

“L'amministrazione dovrebbe avere un processo di controllo per rivedere e confermare periodicamente i diritti di accesso . Un confronto delle risorse con la responsabilità registrata dovrebbe essere fatto per aiutare ridurre il rischio di errori, di frode, di abuso, o di alterazione non autorizzata.,,

iSecurity Assessment ,Audit e Action

1. Ci sono un certo numero di moduli di iSecurity che rispondono a questo requisito. iSecurity ASSESSMENT è un applicazione in grado di valutare il setup di sicurezza attualmente in uso sul sistema. iSecurity ASSESSMENT esegue una fotografia dello stato attuale del vostro sistema ed ,utilizzato ad intervalli regolari consente di tenere il sistema sottocontrollo.
2. AUDIT e ACTION possono essere usati in modo complementare per gestire e segnalare eventuali violazioni.

DS5.7: Monitor della sicurezza

“ L'Amministrazione della sicurezza dovrebbe accertarsi che l'attività di sicurezza sia registrata e che ogni violazione di sicurezza sia segnalata immediatamente a tutti coloro che possono essere interessati, sia internamente che esternamente „.

Firewall ,Audit ,Action e Capture

1. FIREWALL registra e segnala ogni attività del TCP/IP . Con AUDIT e ACTION è possibile rispondere immediatamente ad ogni tentativo di violare la sicurezza tramite l'azione stabilita in tempo reale

2. AUDIT e ACTION eseguono la stessa attività quando controllano il Security Audit Journal così come gli eventi ed i messaggi di sistema.

3. CAPTURE (vedere 5.3.4 qui sopra).

DS5.10: Rapporti d'attività di sicurezza e di violazione

“L'Amministrazione della sicurezza IT dovrebbe accertarsi che l'attività di sicurezza e di violazione sia annotata, segnalata, rivista e giustamente sia intensificata in maniera regolare per identificare e risolvere gli avvenimenti che coinvolgono l'attività non autorizzata. L'accesso logico alle informazioni di responsabilità delle risorse del calcolatore (sicurezza ed altre registrazioni) dovrebbe essere assegnato basato sul principio di meno privilegio, o avere bisogno di necessità di sapere. „

Firewall ,Audit e Action

1. Fare riferimento alle informazioni nell'obiettivo 5.7. FIREWALL, AUDIT e possono tutta fornire rapporti normali (in qualunque momento intervallo richiesto) oltre che il controllo continuo, rilevazione, escalation e risposta immediate.

DS5.17: Protezione delle funzioni di sicurezza

“Tutte le impostazioni di sicurezza dovrebbero essere protette sempre dall'alterazione per mantenere la loro integrità. In più, le organizzazioni dovrebbero mantenere un profilo basso circa il loro disegno di sicurezza, ma non dovrebbero basare la loro sicurezza sul disegno che è segreto.„

Firewall, Audit, Action e AntiVirus

1. FIREWALL può essere usato per assicurare che accessi non autorizzati via rete possano aggiornare/cancellare dati dell'interno dei files. Il modulo ANTI-VIRUS può effettuare in tempo reale la rilevazione e rimozione immediata dei virus

DS5.19: Prevenzione da Malicious software

Rilevazione e correzione

“Per quanto riguarda malicious software , siano i virus del calcolatore o i Trojan, l'amministratore IT deve stabilire una struttura adeguata di prevenzione , di rilevazione , di correzione e di registrazione. Business ed IT management dovrebbero assicurare che le procedure siano condivise da tutta l'organizzazione per proteggere i sistemi e la tecnologia informatica dai virus .Le procedure dovrebbero prevedere la protezione ,la rilevazione le azioni correttive ed le registrazioni.”

iSecurity Anti Virus, Firewall, Audit & Action

1. L'utilizzo del modulo ANTI-VIRUS assicura che i viruses ed i malicious code siano trovati ed eliminati nel modo più veloce possibile.

2. FIREWALL protegge da accessi indesiderati via rete volti a modificare e/o cancellare dati.