iSecurity & Sarbanes-Oxley and COBIT Compliance

About Sarbanes-Oxley (SOX)

- United States federal law enacted in 2002.
- Relates to the review of dated legislative audit requirements
- Protects investors by
  - Improving the accuracy and reliability of corporate disclosures
  - Establishing public company accounting oversight board
  - Ensuring corporate responsibility
  - Providing for auditor independence
  - Allowing for enhanced financial disclosure.

SOX Mandates & Requirements

- Sarbanes-Oxley contains 11 titles that describe specific mandates and requirements for financial reporting:
  - Public Company Accounting Oversight Board (PCAOB)
  - Auditor Independence
  - Corporate Responsibility
  - Enhanced Financial Disclosures
  - Analyst Conflicts of Interest
  - Commission Resources and Authority
  - Studies and Reports
  - Corporate and Criminal Fraud Accountability
  - White Collar Crime Penalty Enhancement
  - Corporate Tax Returns
  - Corporate Fraud Accountability

- Click here for a resource explaining each title

About COBIT

> "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."
>
> *(ITGI)*

- COBIT - Control Objectives for Information and Related Technology
- Established by the IT Governance Institute (ITGI) (www.itgi.org) in 1996
- Consists of guidelines & best practices for SOX compliance which have almost become the de facto standard
- There are approximately 300 generic COBIT objectives, grouped under six COBIT Components.
- COBIT guidelines are generally tailored to particular environments.
- Alternative Standards for SOX compliance are ITIL (IT Infrastructure Library) and Six Sigma. An IT organization is free to select any predefined standards, or even one they develop themselves, but the mostly widely accepted standard is COBIT.

COBIT Components

- Executive Summary - Explains the key concepts and principles.
- Framework Foundation for approach and COBIT elements - Organizes the process model into four domains:
  - Plan and organize
  - Acquire and implement
  - Deliver and support
  - Monitor and evaluate
- Control Objective Foundation for approach and COBIT elements - Organizes the process model into the four domains
- Control Practices - Identifies best practices and describes requirements for specific controls.
- Management Guidelines - Links business and IT objectives and provides tools to improve IT performance.
- Audit Guidelines - Provides guidance on how to evaluate controls, assess compliance and document risk

iSecurity Products Supporting SOX (1)

- Firewall – prevents criminals from accessing and stealing sensitive data. Covers all 53 System communications protocols. Logs all access attempts and reports breaches.
- Audit – monitors and reports on all activity in the System I, performs as real-time auditing and detailed server audit trails.
- Compliance Evaluator – provides at-a-glance compliance checks assessing security status, strengths and weaknesses, based on industry and corporate policies.
- Authority on Demand – Control of user authorities, and dynamic granting of additional authorities on an as-needed basis, accompanied by more scrutinized monitoring.
- AP-Journal (including READ logs) – Monitoring of all changes in business-critical data & alerting of relevant personnel upon significant changes.
- Visualizer - Business Intelligence System for display and analysis of data from the System i

iSecurity Products Supporting SOX (2)

- Password - Full password management capabilities, including enforcement of site-defined password policies. Provides detailed daily reports of unsecured passwords.
- Anti Virus - Protection from Windows-compatible viruses and programs used or stored on System i server. Performs automatic pre-scheduled periodic scans.
- Central Admin - Manages multiple systems from a single control point
- Action - includes real-time alarms and protective response mechanisms for the System i
- Capture – performs silent capturing, saving and playback of user sessions
- View - protects and controls the display of classified data in iSeries user workstations.
- Screen - Automatic protection for unattended workstations
- Encryption (future) - Prevents intruders from using stolen information even when they succeed in obtaining it.

iSecurity Compliance with SOX

COBIT Requirement DS5: Ensure Systems Security	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Admin	Anti-Virus	AP-Journal	Action	Capture	View	Screen	AOD	Password	Assessment	Nubridges
DS 5.1 - Manage Security Measures	IT security should be managed such that security measures are in line with business requirements.	√	√	√	√	√	√	√	√	√	√	√	√	√	√	
DS 5.2 - 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.	√	√	√	√	√	√	√	√	√	√	√	√	√	√	
DS 5.3 - Security of Online Access to Data	In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.	√	√	√	√	√		√	√	√	√	√	√	√	√	
DS 5.4 - User Account Management	Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts.	√	√	√	√	√		√	√	√	√	√	√	√	√	
DS 5.7 - 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.	√	√	√	√	√		√	√	√	√	√	√	√	√	

iSecurity Compliance with SOX

COBIT Requirement DS5: Ensure Systems Security	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Admin	Anti-Virus	AP-Journal	Action	Capture	View	Screen	AOD	Password	Assessment	Nubridges
DS 5.8 - Data Classification	"Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing “no protection” should require a formal decision to be so designated."	√	√	√	√	√		√	√	√		√	√	√	√	
DS 5.9 - Central Identification and Access Rights Management	Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	√	√	√	√	√		√	√	√		√	√	√	√	
DS 5.10 - 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.	√	√	√	√	√		√	√	√			√		√	

iSecurity Compliance with SOX

COBIT Requirement DS5: Ensure Systems Security	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Admin	Anti-Virus	AP-Journal	Action	Capture	View	Screen	AOD	Password	Assessment	Nubridges
DS 5.16 - Trusted Path	Organizational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems.	√	√	√	√	√			√	√					√	√
DS 5.17 - 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.	√	√	√	√	√		√	√	√	√		√	√	√	√
DS 5.18 - Cryptographic Key Management	Management should define and implement procedures and protocols to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.	√	√	√	√	√		√	√	√			√		√	√

iSecurity Compliance with SOX

COBIT Requirement DS5: Ensure Systems Security	Description	Firewall	Audit	Visualizer	Compliance Evaluator	Central Admin	Anti-Virus	AP-Journal	Action	Capture	View	Screen	AOD	Password	Assessment	Nubridges
DS 5.19 - 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."	√	√	√	√	√	√		√	√					√	
DS 5.20 – Firewall Architectures and Connections with Public Networks	If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.	√	√	√	√	√		√	√	√	√		√	√	√	

SOX & COBIT Links

- SOX legislation
- SOX Overview
- ISACA Website
- TechTarget Introduction to COBIT
- COBIT forums & information
- Making Sense of SOX Requirements

Raz-Lee Security – Mission & Product Lines

"Raz-Lee Security is committed to providing the best and most comprehensive IBM i compliance, auditing and security solutions"

- Founded in 1983
- 100% focused on IBM i (AS/400)
- Corporate offices in: US, Italy, Germany
- Installed in more than 40 countries, over 12,000 licenses
- IBM Business Partner
- Integration Partner with Tivoli and Qradar
- Partnerships with other major global SIEM & DAM solution providers:
  - Official partnerships with McAfee, RSA enVision, HP OpenView, GFI, NNT
  - OEM by Imperva SecureSphere
  - Proven integration with ArcSight, CA UniCenter, Splunk, Juniper
- Worldwide distribution network

Business Partners

Raz-Lee's Global Distribution Network

iSecurity: Selected Customers

- CHS (Community Health Systems, US)
  - ¬200+ systems and growing
  - Replaced Powertech
- Royal Bank of Scotland
  - Purchased iSecurity after POCs of nearly ALL competitors!
- Venetian Casinos (multi-national)
  - Purchased iSecurity following extensive compliance POC.
- Euronet Worldwide
  - Banking clearinghouse in Europe & Asia
  - Replaced competitor with iSecurity.
- Svenska Handelsbanken
  - One of the largest banks in Scandinavia
  - Used competitor for several years; replaced it with iSecurity.

Internationally renowned IBM i solutions provider

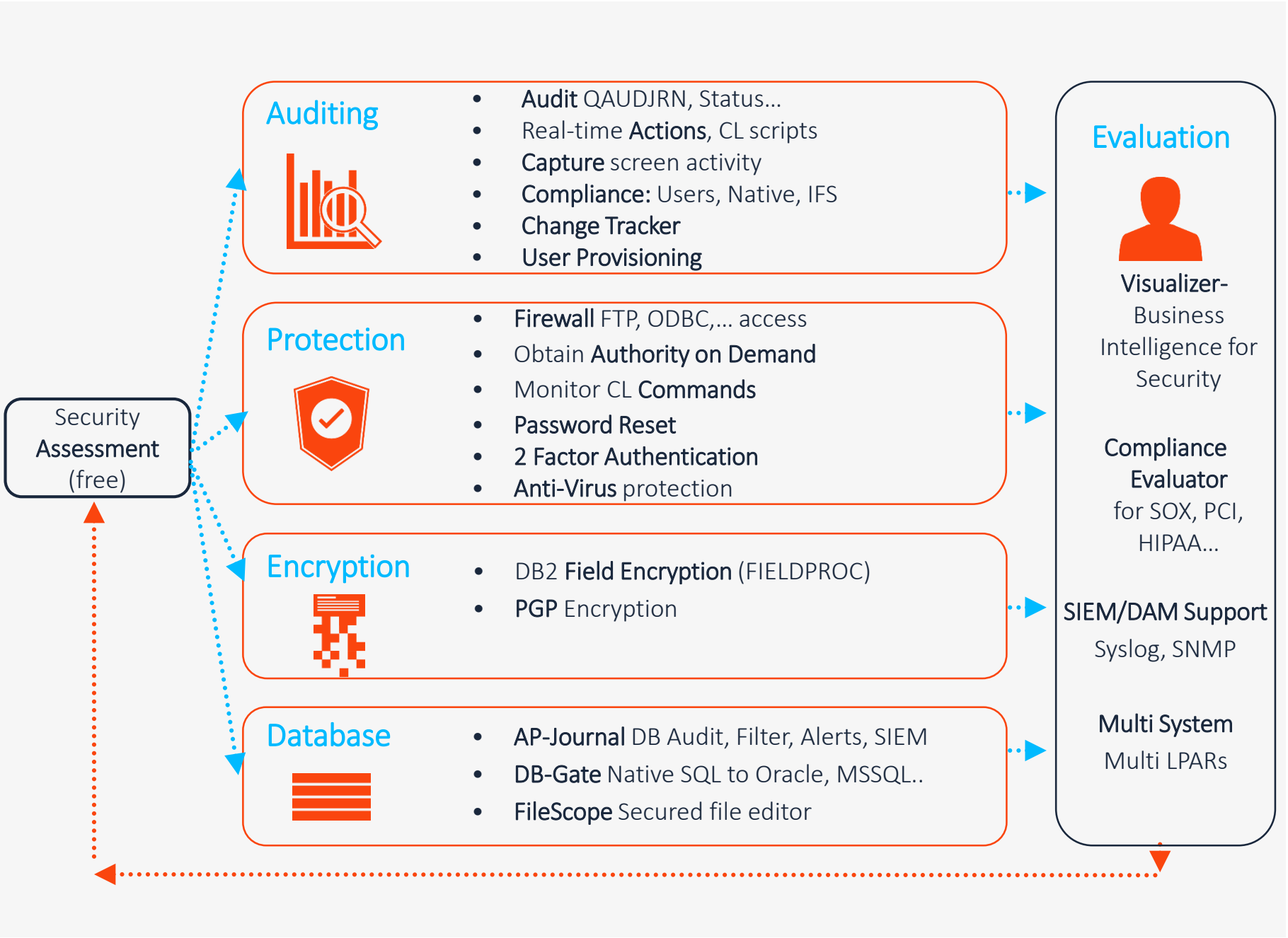
iSecurity Characteristics

The leader in IBM i security with on-going product development

- Full GUI and green screen - short learning curve, ease of use
- Visualizer Business Intelligence analysis
- Hundreds of built-in, customizable reports. Report/Query Generator and Scheduler produces print, screen, HTML, PDF, CSV e-mailed reports.
- Wizards, Real Time/Periodical, Alerts. All done on IBM i
- Supports SIEM with CEF, LEEF formats; Sends SYSLOG, SNMP, Twitter, e-mail, SMS, etc.
- Cross-enterprise reporting, definitions, logs
- Exceptional performance on all sizes of systems
- Unique products: Capture, Change Tracker, DB-Gate, Anti-Virus

iSecurity Suite of Products

- GDPR, PCI, HIPAA, SOX, JSOX, FDA
- Local Regulations
- Auditor's Requests
- Detect Security Breach
- Management Decision



Contact Us

marketing@razlee.com