



## Sarbanes-Oxley Act and SSH Tectia

### Application Note

The SSH Tectia solution can help public companies implement technical security controls as a part of the Sarbanes-Oxley Section 404 compliance plan. By incorporating confidentiality, integrity, and authentication as security services within the corporate network, SSH Tectia enhances the financial reporting reliability by preventing illegitimate modification of financial data, or unauthorized access to accounting information. The centralized monitoring capabilities of SSH Tectia Manager ensure accountability of secure connections including administration access to managed servers which results in improved internal control and auditing.

#### Business Challenge

The Public Company Reform and Investor Protection Act of 2002, also known as the Sarbanes-Oxley Act (SOX), is today a top priority among US public companies. In response to allegations of dubious financial accounting practices culminating in major corporate scandals, SOX was implemented to establish good corporate governance and to restore confidence in the US public markets.

Section 404 of SOX requires top management to establish an adequate internal control structure and include an assessment of its effectiveness in the annual report. Additionally, an external auditor needs to verify the management's assertions. For accelerated filers Section 404 becomes effective for fiscal years ending on or after November 15, 2004 while all other public companies are affected for the fiscal year ending on or after July 15, 2005.

Technical safeguards play an important role in complying with SOX Section 404 due to the extensive role of IT infrastructure and applications in today's financial reporting and accounting processes. Data integrity, strong user authentication, confidentiality, auditing, and access controls are among the technical controls needed to ensure the validity of the accounting information and to prevent fraudulent access to financial data in the process.

SOX itself does not specify how the technical controls related to Section 404 should be implemented. However, there is a more specific framework available to assist companies in implementing best practices for SOX compliance. Control Objectives for Information Technology (COBIT) is a widely accepted guideline document defining IT-related controls including specific objectives for systems security. COBIT is strongly recommended by the Information Systems Audit and Control Association (ISACA) to achieve SOX compliance.

#### Solution Description

SSH Tectia can help public companies implement technical control objectives related to systems security as a part of the SOX Section 404 compliance directive. By incorporating confidentiality, integrity, and authentication as security services within the corporate network, SSH Tectia enhances the financial reporting reliability by preventing illegitimate modification of financial data, or unauthorized access to accounting information. Strong user authentication, optionally based on smart cards or other hardware tokens, ensures that authorization decisions are based on the true identities of users, which eliminates the risk of un-authorized data access.

SSH Tectia protects business-critical applications by providing a transparent security layer for networked >>>

**SSH Tectia can help in implementing most of the COBIT Delivery & Support (DS5) control objectives for ensuring system security.**

Control Objective	SSH Tectia
5.1 Manage Security Measures	Centralized enforcement, maintenance, and monitoring of security policies with SSH Tectia Manager.
5.2 Identification, Authentication and Access	Strong user authentication allows restricting access to accounting and other financial data to legitimate users and user groups only.
5.3 Security of Online Access to Data	Confidentiality, integrity, and authentication provided by the SSH Tectia client/server solution eliminate the possibility to hijack connections or steal passwords to gain illegitimate access to data.
5.7 Security Surveillance	System administrator access and protected user connections to servers can be logged and audited from a central location with SSH Tectia Manager.
5.8 Data Classification	Enforcement of data classification policies for all data in transit with end-to-end data traffic encryption.
5.9 Central Identification and Access Rights Management	SSH Tectia supports third party identity and access management solutions.
5.10 Violation and Security Activity Reports	SSH Tectia Manager logs secured connections and generates reports for IT security administration to ensure appropriate escalation on a regular basis.
5.11 Incident Handling	Secure communications facilities based on Secure Shell for rapid and reliable addressing of security incidents.
5.13 Counterparty Trust	Supports a broad range of authentication methods including passwords, tokens, and smart cards for reliable counterparty authentication.
5.16 Trusted Path	Offers a trusted path with confidentiality, integrity, and authentication for sensitive data travelling in the corporate network, between users and systems, and between systems.
5.18 Cryptographic Key Management	Incorporates broad and sophisticated support for key distribution, maintenance, and revocation based on PKI. SSH Tectia Manager alternatively provides non-PKI-based, light-weight host key management for smaller and more static environments.

applications, encrypting data traffic end-to-end between workstation and server, or between servers. Business application protection offers security against common network attacks by providing a trusted path for critical information, including financial reporting data, while it travels in the corporate network.

SSH Tectia for secure remote administration, based on the Secure Shell protocol, allows system administrators to manage servers in large and heterogeneous network environments. Various system administration operations, such as software installation, often require high system privileges allowing broad access to different type of data. As a centralized management platform, SSH Tectia Manager uses its monitoring capabilities to enable organizations to implement effective control practices that include system administration operations. Server access log data is centrally stored in the management system's database facilitating reliable auditing of access and authentication data on an on-going basis.

**Solution Benefits**

- Improved SOX Section 404 compliance based on COBIT security objectives.
- Enhanced financial reporting reliability with data transmission integrity and authentication.
- Effective internal control for remote connections with centralized monitoring.
- Strong user authentication prevents unauthorized access to financial reporting data.
- Cost-effective protection based on centralized enforcement, maintenance, and monitoring of security policies.



[www.tectia.com](http://www.tectia.com)

