



CASE STUDY:

ACCUDATA SYSTEMS HELPS COMPANIES MEET SOX DEADLINES

BACKGROUND

In response to the financial troubles at Enron, WorldCom and other major corporations, the U.S. Congress passed the Sarbanes-Oxley Act (SOX) in 2002. Beginning November of 2004, SOX requires the principal officers of most publicly traded companies to certify the accuracy and completeness of their annual and quarterly financial statements. It also requires them to testify to the effectiveness of the company's underlying financial and business controls.

Though regulators have issued some guidelines, SOX does not definitively assign a scope to IT compliance requirements. SOX regulations, in fact, do not specify which IT controls need to be documented and tested or how the auditing should be conducted. Corporations have few clearly defined standards or rules to follow to achieve compliance. As a result, many companies are scrambling to understand and meet initial and ongoing compliance requirements of this legislation.

PROBLEM

One of the world's largest offshore/onshore drilling contractors recently engaged Accudata Systems to assist in the preparations for its upcoming SOX audit. The Company needed a set of control standards to measure against when assessing its current level of compliance. Additionally, the Company needed help testing, remediating, and documenting IT-related resources to meet the year-end reporting deadlines for SOX compliance.

Though the Company presently conducts both quarterly and annual audits, with the ratification of SOX, the results of these audits must be certified as to their accuracy and tied to earnings statements. Non-compliance could impact the Company dramatically - negatively affecting stock prices and exposing management to potential legal prosecution.

The Company engaged Accudata Systems to provide it with a 'checklist' of IT standards and best practices - tailored specifically to the Company's IT environment - against which it could be audited. Accudata Systems was tasked with four primary objectives for this engagement:

- Identify all technologies currently in use throughout the Company
- Develop a checklist of recognized, standards-based best practices for these technologies
- Perform an independent, third party audit of the systems in preparation for the compliance audit
- Document the Company's compliance with and deviation from these standard best practices

Financial data, which traverses the network both internally and externally, flows effortlessly throughout the corporate environment. SOX regulations require the Company to know which employees are able to 'touch' that financial data, where it travels, and where it is backed up and stored. The 'chain of custody' for financial information must be certain - who can see it, access it, and change it.



SOLUTION

First, Accudata Systems worked with the Company's IT organization to develop a checklist of the technologies currently in use for which they needed standard best practices. Once those technologies were documented, Accudata Systems gathered all the information the Company had on existing internal processes, standards, and configurations.

After all the information on the current network was collected, Accudata Systems consultants researched existing standards and best practices for these technologies. The standards chosen were very strict, most of them originating from the National Security Agency (NSA) or from the National Institute of Standards and Technology (NIST). For certain technologies - for example RSA ACE Server - there were no independent standards on how to secure them. For these technologies, Accudata Systems researched the vendors' documentation to extract vendor recommended best practices to add to the checklist.

After establishing standard best practices appropriate for the Company's environment, consultants developed a security checklist for each technology in use. In particular, the Company wished to focus on the configuration of its devices, ensuring it was compliant in that area. Because some of these standards were very strict, they would not align with what the Company needed. Accudata Systems aligned the standards that were reasonable for a corporate environment and documented what part of each standard was being used as well as what part was not being used.

For example, one standard outlined an 8-character password and another stated a 12-character password. Accudata Systems documented any deviations they decided not to comply with and supplied a justification of why. This documentation helped the auditors understand why the Company deviated from the standard. Generally, with proper documentation and justification, a deviation from the standard is not considered an audit issue.

Additionally, the Company requested Accudata Systems to perform an independent, third party assessment of its systems in preparation for its compliance audit. After the standards were agreed upon across all environments, Accudata Systems audited the Company's IT infrastructure against those standards. The audit results included various data evidence and screen shots, and provided the Company with a forecast of what it could expect from the audit firm. The Company then had an opportunity to remediate any found issues.

RESULTS

As a result of this rather complex effort, the Company now has a baseline of security checklists as well as a baseline audit that it will use to begin building its SOX compliance program. In the executive summary report produced for the project, the Company learned how close to compliance its environment was across all the thousands of security checks in the checklist.

But they also needed long-term information - what were the trends, the issues, the weaknesses in their network. For this, Accudata Systems designated nine categories of data - Key Performance Indicators (KPIs) - and extracted data into those KPIs. Each environment could be examined differently, depending on what the Company wanted to look at. Categories of information can be extracted and measured for compliance, and the Company can determine the categories it needs to focus on. For example, checks 2-1 thru 2-10 cover auditing router configurations. If the Company is compliant with 8 of these 10 checks, then they are 80% compliant for auditing on that device. The Company can now see clearly which KPIs need attention and which are secure.

Accudata Systems helped the Company determine its pain points and measure compliance against an established baseline of standards. This will help the Company set priorities, establish more focused budgets, and measure real improvements made over the coming year, helping it meet ongoing SOX legislation requirements.