

Case Study: Financial Services Company Creates Controls to Mitigate IT Security Risk and Comply With Sarbanes-Oxley 404

Gartner RAS Core Research Note G00144969, Kristen Noakes-Fry, Paul E. Proctor, 8 December 2006 R2109 09152007

A \$2 billion financial services company addressed potential deficiencies in its Sarbanes-Oxley 404 audit by creating and implementing technical security controls.

WHAT YOU NEED TO KNOW

A financial services company found that the Sarbanes-Oxley Act of 2002 (SOX) not only shifted focus to the integrity of financial reporting but also had broader ramifications for the business. As the company worked to meet the U.S. Securities and Exchange Commission (SEC) mandates for complying with SOX reporting and auditing results for fiscal years ending on or after 15 June 2004, the project team was frustrated by the lack of experienced auditors to assist them in the SOX 404 audit (see Note 1 for disclaimer). While this situation has been common in the Gartner client base, it was expected to abate by the end of 2006 as the standard of due care is clarified, and auditors gain more experience with appropriate enforcement.

CASE STUDY

Introduction

“While SOX was primarily an internal issue, it also changed the way we do business – some [company] applications had even been identified as SOX-related by our clients,” says a leader on the project. This shift in focus changed project priorities. Suddenly, authentication and security controls on laptops became relevant, Statement on Auditing Standards No. 70 (SAS 70) Type II audits were mandatory, and \$250,000 projects that had been rejected recently were now essential (see Note 2).

Gartner spoke with the director of security at the company. Commenting on the impact of SOX, he points out that after the World Trade Center attack, the organization focused on the redundancy and availability elements of business continuity planning (BCP) but that SOX changed this equation significantly.

Note 1 Disclaimer

Note: This is a paid case study contracted by Meta Group prior to Gartner’s acquisition of Meta. Under policy, Gartner does not write contracted white papers, but is fulfilling on a contractual obligation in producing this report. Gartner attempted to get all the facts correct despite personnel change but ultimately we cannot vouch for the project’s success. Gartner does not endorse, nor recommend against, the products used or named in this case study.

Note 2 SAS 70 Audit

SAS 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit represents that an organization has been through an in-depth audit of its control activities, including controls over information technology and related processes. Section 404 of SOX makes SAS 70 audit reports important, indicating whether the controls were placed in operation, suitably designed and operating effectively.

The Challenge

Like many Gartner clients, the company was using a financial reporting process based on a manual process that involved a number of Excel spreadsheets. Little control was maintained over who touched what or who had permission, and the company had limited ability to track any of this activity. Also, the company faced issues related to weak security controls around the accounting software running in the general domain, poor physical access controls to servers and poor configuration management.

Longer-term goals included “re-architecting” the entire financial reporting process to make it more automated and controlled, but the immediate requirement was to ensure the accuracy and integrity

of the existing scheme. To meet these immediate goals, the security department was brought into the discussions.

Lacking the time to re-architect the entire system with appropriate security, the company elected to secure the existing environment around the Excel files. One of the core issues was that any administrator could access anyone's environment.

Objective

The plan was to create a directory, called the secure directory, on each laptop and desktop that would point to spreadsheets in the financial reporting process. A technical control that not even administrators could circumvent was needed to log all accesses and prevent anyone except the directory owner from looking at the information. In the face of SOX 404 requirements, the company had to develop a set of defensible controls that were effective and low cost and could be implemented quickly (see Note 3).

Approach

The financial services company addressed SOX the way many companies do – by establishing a compliance committee and working through the issues in priority order. At first, the plan was to build an appropriate protection scheme with access control, policy management and auditing, but it became apparent to the committee that the company had neither the time nor the money to implement this type of robust solution. Instead, the committee opted for a combination of policy, process and technology controls.

Obstacles

Although risk management controls are essential to pass a Section 404 audit, no representatives of the information security department had been included on the compliance committee. Then a situation developed that required information security expertise.

To make matters worse, neither the company's internal nor external auditors were able to assist – not so much from conflict of interest as from simple inexperience. Because of the demand on auditors'

Note 3 SOX 404

SOX, administered by the SEC, defines which business records are to be stored and for how long they must be retained. It currently states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." IT departments are challenged to create and maintain an archive of corporate records to satisfy the requirements of SOX. Section 404 of SOX focuses on the critical role of internal control over financial reporting, emphasizing the importance of ethical conduct and reliable information in the preparation of financial information reported to investors.

time during the first round of SOX 404 controls audits, the company suffered from being assigned a group of inexperienced auditors. A representative notes, "We were a \$2 billion company but felt as though we were getting no respect."

Selecting a Data Protection Product

To create the secure directories and address financial reporting control issues, the committee decided to implement technical controls, including:

- Secure directories on each computer that even system administrators were not able to access
- Defensible controls to aid with access and monitoring in their spreadsheet system

For the needed technical controls, the company selected Digital Guardian, a host-based data-protection product from Verdasy's (Waltham, Massachusetts). Digital Guardian permits an operating system shim to trap system calls to control and monitor access with another layer of control beyond the operating system.

Alterations in the Financial Reporting Process

Implementing Digital Guardian, in combination with policy and process controls about the use of the secure directory within the financial reporting process, resulted in the company making decisions to:

- Remove the Great Plains accounting application from the general domain, thus isolating the ERP system from the risks in the general domain.

- Implement Citrix on the accounting server so that users had to go through it to get to Great Plains. Citrix had the necessary password complexity and aging controls that Great Plains lacked. Since employees used the same password on both Citrix and Great Plains, the company could implement complexity and aging on Great Plains without requiring employees to remember another password.
- Add physical access control to the data center by creating an authorized list – all workers, including administrators, had to be on that list to enter the server room. Security personnel also checked IDs and logged who went in to the room as well as who escorted them.
- Implement change control for all the applications related to financial reporting and security devices, such as firewalls.

Results

The Digital Guardian product was initially deployed in 2005 on 200 IT, finance, human resources and executive laptops. The security controls thus implemented helped the company to avoid material deficiencies in these areas.

Critical Success Factors

The financial services company was able to combine people, process and technology effectively to create a defensible position for its controls.

Corporate culture was important to success. At first, employees were concerned that the Digital Guardian software would be like “Big Brother” and violate their privacy, but as they became comfortable with the software and the overall process, they realized the ways in which the new product protected their security and privacy.

Lessons Learned

- Thinking from the past was not enough to meet the SOX 404 challenge. Passing the Section 404 audit requires rethinking the solution to a compliance problem.
- Organizations need to balance strategic and tactical requirements.
- Change and configuration management is one of the necessary elements that Gartner recommends for a basic control environment to address compliance.