BLUE LANCE

Sarbanes-Oxley Control Transformation Through Automation

An Executive White Paper

By

BLUE LANCE, Inc.

Where have we been? Where are we going?

Contents

About Blue Lance, Inc.

Blue Lance, Inc. is a leader in development of real-time monitoring, auditing and computer forensics technology for Windows and Novell networks. Its flagship product LT Auditor+ is used to secure the assets of the world's largest corporations, banks, government agencies, education and healthcare institutions.

Founded in 1985, Blue Lance pioneered the development of audit trail technology for Novell and Microsoft Windows networks along with a number of firsts in network audit security, including real-time monitoring, automated filtering of data and secure consolidation of system logs.

Executive Summary

The Sarbanes-Oxley Act of 2002 (SOX), specifically section 302 and 404, has changed the way Information Technology (IT) departments view their organization's business requirements. IT departments need to clearly understand their organization's financial reporting requirements and the people, process and technology required to support and protect the financial data and the financial reporting process.

It's not enough to have documented policies and procedures in place that explain how they protect their financial data and reporting processes. They must monitor and maintain logs to provide evidence that their policies and procedures are being followed and are operating effectively.

To accomplish compliance in year one, most organizations and audit firms cast a wide net to identify all controls that might be considered key to internal controls over financial reporting. For most IT departments, this approach created a tremendous amount of anxiety when considering their IT general control environment. Knowing the integrated nature of their IT environments, determining which IT general controls support and protect their organization's financial data and financial reporting processes was a significant challenge.

Once they identified their key IT general controls, they had to ensure they were designed appropriately, documented, operating effectively and monitored. IT departments quickly realized that if they did not attempt to automate these key IT general controls they would be spending a lot of time and effort every year monitoring them and validating their operational effectiveness. Not to mention, their external auditors would be spending an equal amount of time reviewing the non-automated controls each year.

When key IT general controls are automated and a change control process is in place, the auditor can review the automated control and change control process in year one. If the change control process is effective, the auditor could theoretically review the change control process and audit the control where changes have occurred in subsequent years. Relying on a change control process for automated controls can dramatically reduce the auditor's level of effort.

The automation of key IT general controls can also reduce the resource requirements the IT department needs to allocate to monitor these controls.

This white paper presents SOX IT general control compliance from two perspectives that corporate IT departments must understand:

1. Where have we been? – What has corporate IT gone through, and what do we know.

2. Where are we going? – What does corporate IT have to look forward to and key elements that need to be considered, by corporate IT, to be successful.

[1] PCAOB - Bylaws and Rules – Standards – AS2 [Under Item 126 (Page 176)]

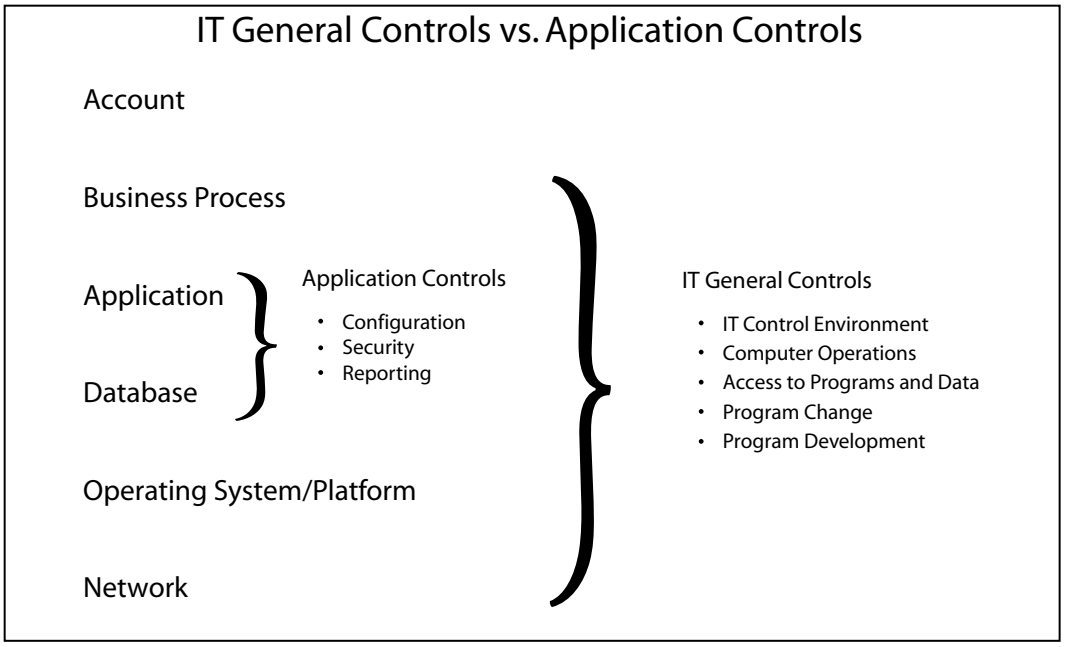
Where have we been?

Sarbanes-Oxley has been broad and far reaching, affecting all publicly-traded companies in the US, and foreign filers in US markets. Section 302 and 404 are the key areas for information technology (IT).

Section 302: Corporate Responsibility for Financial Reports
Section 302 stipulates that the principal executive officers and principal financial officers (usually the CEO and CFO) in a public company are responsible for the internal controls that provide material information used in constructing financial reports.

Section 404: Management Assessment of Internal Controls
Section 404 requires an assessment of the effectiveness of internal controls over financial reporting.

In the rush to meet the regulatory deadlines, companies and auditors cast a wide net when determining what IT internal controls needed to be included to meet the SOX requirements. Many companies and auditors focused on establishing general controls for IT. This is good practice but not necessary for SOX compliance. The final version of SOX narrowed its focus to only those controls that directly affect financial reporting.



On 9 March 2004, the Public Company Accounting Oversight Board (PCAOB) approved Auditing Standard No. 2, titled "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." This standard establishes the requirements for performing an audit of internal control over financial reporting and provides some important directions on the scope and approach required of auditors.

Auditors are using the PCAOB Auditing Standards to evaluate each public company's compliance efforts. Auditing Standard No. 2[1] states the following with regard to IT general controls:

> *"**Information technology general controls.** Information technology general controls are part of the control activities component of internal control…Therefore, the auditor could determine that, based on the nature of these controls over systems access, he or she would need to perform more of the tests of those controls himself or herself."*

Understanding IT General Controls

IT general controls (IT controls) are used to manage and control a company's information technology activities.

For most companies, the integrity of the financial statements greatly depends on the completeness, accuracy, and timeliness of the information flowing through the company's computer systems. The degree to which a company can rely on the integrity of information processing and the effectiveness of automated controls and automated accounting procedures (i.e., calculations and automated postings to accounts) depends on the effectiveness of their IT General Controls.

In April 2004, the IT Governance Institute in cooperation with Information Systems Audit and Control Association (ISACA) published, *IT Control Objectives for Sarbanes-Oxley, The Importance of it in the design, Implementation and Sustainability Of Internal Controls Over Disclosure and Financial Reporting*.

1 PCAOB - Bylaws and Rules – Standards – AS2 [Under Item 126 (Page 176)]

IT General Controls are pervasive controls and include the following 5 high-level areas:

1. **IT Control Environment** – The IT control environment includes the IT governance process, monitoring and reporting. Monitoring and reporting are required to ensure that IT is aligned with business requirements.

2. **Program Changes** – Program changes address ongoing change management including the implementation of software updates.

3. **Access to Programs and Data** – Access controls to programs and data includes methods for preventing unauthorized access, such as secure passwords, firewalls and data encryption.

4. **Computer Operations** – Computer operations include controls over the definition, acquisition, installation, configuration, integration and maintenance of the IT infrastructure.

5. **Program Development** – Program development includes the acquisition and implementation of new applications.

As illustrated in the diagram above, Application Controls and IT General Controls play a significant role in financial statement reporting.

IT general controls and application controls have become more integrated. IT general controls increasingly supplement application and business process controls. IT general controls are required to support the functioning of application controls and both are required to enable an accurate and secure financial reporting process.

Focus on IT

Initially, despite all the publicity surrounding SOX, relatively little attention was focused specifically on the role of IT in the financial reporting process. This was unfortunate, given that the accuracy and timeliness of financial reporting is, at most companies, heavily dependent on a well-controlled IT environment.

SOX requires CEOs and CFOs, but not IT executives (i.e., CIO, IT Director, etc…) to sign legal documents attesting to the veracity of their firm's financial reports. However, due to the pervasive nature of general computer controls, the integrity of company data could be impacted by inadequate IT controls. Therefore, the heads of IT organizations have assumed a role in ensuring the accuracy of the data contained in corporate financial systems.

IT Control Weaknesses Identified in 2004 & 2005

- Abnormal activity not identified in a timely manner – Most systems/applications relied on detective controls rather then proactive controls. This provided slow response time in detecting abnormal activity.

- Audit logs not being reviewed (or that review itself not being logged) – Just creating audit logs was not enough, the logs had to be reviewed and logged as being reviewed.

- Improper account provisioning with segregation of duties – Most companies did not have pro-

cesses in place to make sure application access rights were changed when people left the company or changed positions.

- Insufficient controls for change management – The issue here was that companies did not have appropriate quality assurance checks on changes being made to key financial applications.

Where are we going?

Control Transformation – Maintaining Effective Compliance

Going forward, companies need a dual focus:

1. sustaining an ongoing assessment process for compliance; and

2. balancing control risks while identifying and pursuing improvement opportunities to better the business.

Concern about maintaining and evolving compliance efforts is widespread. A survey conducted in September 2004 among 530 public companies by KPMG's 404 Institute indicated that as many as 70 percent of organizations had not begun, or were just beginning, the planning efforts needed to maintain ongoing compliance.[2]

Automation is Key to Control Transformation

In sustaining an ongoing auditable environment, process automation will be necessary.

SOX's has made the timing of error detection and response a critical issue for many organizations. In the past it may have been acceptable to wait for a manual reconciliation to detect an error. Now with the automation and integration of business processes and information technology, errors need to be detected as soon as possible. This makes most manual controls obsolete.

As management has realized the cost of compliance with the Sarbanes-Oxley, there has been an increased focus on automated controls. Why document and test a manual control for 30 to 50 occurrences when an automated control, supported by adequate change controls, may need to be tested only a few times?

SOX compliance needs to be treated as an ongoing process. The challenge is to follow this new process without crippling the IT department. This can be done by automating as many of these key controls as possible.

What IT Leaders Need to Do in Order to Avoid a Year End Crunch:

Make sure controls put in place last year are required and not redundant.
External auditors, following a strict interpretation of the PCAOB Auditing Standard, concluded it would compromise their auditor independence and the legitimacy of the audit if they were to tell their clients they were establishing controls that were not necessary to pass the SOX audit.

In April 2005, PCAOB Chairman William McDonough acknowledged that it was not the intent of the PCAOB to prevent auditors from telling their clients that they were doing too much and in May 2005 the PCAOB issued a formal advisory, instructing the auditors to work with their clients to determine which controls are unnecessary.

The PCAOB standard includes specific requirements for auditors to understand the flow of transactions. The processing procedures relevant for the auditor to understand the flow of transactions generally are those activities required to initiate, authorize, record, process and report transactions.[3] Such transactions' flows commonly involve the use of application systems … The reliability of these application systems is in turn reliant upon vari-

2 KPMG's 404 Institute, Second Web survey, KPMG LLP, 2004.
3 PCAOB Auditing Standard No. 2

ous IT support systems, including networks, databases, operating systems and more. Collectively, they define the IT systems that are involved in the financial reporting process and, as a result, should be considered in the design and evaluation of internal control.

The PCAOB suggests that these IT controls have a pervasive effect on the achievement of many control objectives.

Automate Controls Wherever Possible

Progress being made with regards to optimizing compliance efforts was captured in a survey of 180 top financial executives at a wide range of companies and in a series of in-depth interviews[4].

> *"Automation plays a key role in capturing these improvements, even though most companies only expect to have new systems fully in place by the end of year two of Sarbanes. Over 75 percent of executives in our survey assigned either "top priority" or "moderate priority" to automation of their compliance and control environment over the next 12 months. Fifty-six percent plan to scrutinize their underlying business processes, and 43 percent will turn their attention to improving and automating manual controls such as reconciliation and security.*
>
> *The survey found that automating the compliance and control environment was a priority for 76 percent of companies. Almost half of all companies in the survey stated that security and access controls were areas they currently automate or plan to automate in the future. Thus, security is the one area on which companies showed the most agreement."*

The biggest opportunities for achieving savings and greater efficiency, is not in developing better documentation but in areas such as testing, monitoring and remediation or mitigation. This is where automation comes in.

Most companies agree that automation will be required in order to enable a sustainable, auditable IT Control environment. However, they have different expectations for what will be the most important application for new controls automation. A survey of 180 financial executives by CFO Research Services identified that almost half of all companies in the survey – state that security and access controls are areas they currently automate or plan to automate in the future.

Automated controls solutions help ensure consistency in both process and controls. These solutions enable organization to prove controls on the basis of defined rules, forcing users to follow authorized processes. These solutions capture data automatically and provide comprehensive audit trails and reports. Proving manual controls is more difficult because it can be hard to validate that the appropriate authorized process is always followed.

4 Excerpt from a report prepared by CFO Research Services in collaboration with Virsa Systems and PricewaterhouseCoopers LLP, August 2005

Reporting Requirements

A challenge for meeting the needs of your end users is that Sarbanes-Oxley has created the need for multiple views into the IT control environment:

- **External Auditor view** – External auditors need to evaluate internal IT general controls over financial reporting and need to assess whether these controls are in place and are designed and operating effectively.

- **Corporate view** – Corporate executives (CEO, CFO, CIO, Internal Audit Director, etc…) and committees need to monitor their internal control environment on an ongoing basis.

- **IT Management view** – IT Management (Managers and Administrators) needs to maintain effective operations while managing and maintaining effective internal IT general controls over financial reporting.

Each of these views, depending on the control being audited or monitored, requires similar data. However, the presentation of that data may vary depending on the end user objectives. For example, an external auditor assessing compliance with password management policies may require a different data view than an IT manager monitoring for password management policy violations. Both are assessing compliance. The external auditor is looking for any potential violations. The IT manager needs additional data to log violations and take remedial action. The logs of the violations and remedial action, which are maintained by the IT manager, will allow the auditor to assess the organizations responsiveness to this control violation.

Framework(s) for IT Controls

IT professionals have no standard or baseline from which to guide their compliance activities. Two frameworks, COSO and COBIT, have been discussed as possible guidelines for implementing IT internal controls over financial reporting.

The COSO Framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission in 1992. This framework has been accepted by the SEC, so it is likely to be favored over others. COSO states that internal controls should be comprised of five components, and that all components must be in place in order for an internal control to be considered effective. COSO's five components are:

1. **Control Environment:** The tone of an organization, influencing the control consciousness of its people, provides discipline and structure; elements include ethical values, management competence and operating style.

2. **Risk Assessment:** The identification and analysis of internal and external risks that present threats to management's achievement of its objective for financial reporting; this forms a basis for determining how the risks should be managed.

3. **Control Activities:** Control policies and procedures are established and executed to ensure management directives are executed by addressing the risks to achieve the company's objectives.

4. **Information and Communication:** Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Effec-

tive communication must flow throughout the organization (down, up, across), and must include communication with external parties, such as regulators and shareholders.

5. **Monitoring:** Internal control systems must be monitored in order to assess the quality of the system's performance over time so necessary modifications can be performed.

Unfortunately, COSO does not specify controls for IT. Enter COBIT. COBIT has emerged as a standard from the COSO practice and helps translate COSO into actions that are applicable to the IT organization. Generally, COBIT encompasses the following four areas:

- **Plan and organize:** Define strategic IT plans and architecture, assess risks, manage projects, manage human resources, and ensure compliance with external requirements.

- **Acquire and implement:** Identify automated solutions, acquire and maintain technology infrastructure and application software, manage changes.

- **Deliver and support:** Define and manage service levels, manage performance and capacity, ensure systems security, manage problems and incidents.

- **Monitor and evaluate:** Monitor processes, assess internal control adequacy, and provide for independent audit.

Without guidance from the PCAOB, the auditors turned to pre-existing IT Control Frameworks, such as COBIT. COSO and COBIT are respectively, 20-years old and 10-years old collections of guidelines and management principles, with COBIT being IT specific.

Summary

Achieving Elements of Compliance with the Sarbanes-Oxley

With the above considerations in mind, Blue Lance believes that public companies cannot achieve cost effective compliance with Sarbanes-Oxley without the automation of key IT general controls and the appropriate monitoring of access to programs, data and computer operations.

Blue Lance, with its LT Auditor+ SOX Reporting Plug-in, allows public companies to automate and monitor key IT general controls and produce evidentiary report logs. These reports enable corporate management, IT management and external auditors to conclude that key IT general controls, supporting internal controls over financial reporting continue to be effective.

Public companies should consider various ways in which accounting information can be compromised in determining the most effective level of system monitoring. Opportunities exist to monitor activity from a number of vantage points, including:

- the operating system's perspective (using available system level auditing capabilities);
- the network communication's perspective (using network traffic monitoring tools);
- from the perspective of the financial application processing accounting information (using available application transaction logging capabilities); and
- a database management system's perspective (using available database access logging capabilities).

The importance of a particular level of alert, monitoring and logging will be situational, where varying circumstances could make the information in one log important one day, but less important another day.

LT Auditor+ Enables Compliance with Sarbanes-Oxley

Organizations that are required to comply with the Sarbanes-Oxley will be able to take advantage of features in the LT Auditor+ SOX Reporting Plug-in, which provides the ability to:

Provisioning Controls. Monitor, log and audit:

- that users maintain unique IDs and are not sharing user IDs - Exceptions Only
  - changes in user job function access rights through transfer or termination and validate access is appropriately revoked in a timely manner
  - privileged user access rights to identify and remove inappropriate system access rights
  - active user access rights to identify and remove inappropriate system access
- Segregation of Duties (SoD) Controls. Monitor, log and audit:
  - job function user access for segregation of duty violations.

- whenever access privileges are granted to an individual user to ensure that SoD conflicts do not exist for users having access to multiple systems profiles or transactions

◈ System level ID Controls. Monitor, log and audit:

- assurance that in-scope systems are restricted to a defined set of personnel
- assurance that personnel are not mistakenly or maliciously threatening in-scope systems

◈ Password Management Controls. Monitor, log and audit:

- user compliance with password management policies

◈ User Access Controls. Monitor, log and audit:

- User and program system access activity (logons, logoffs and connections)

◈ File and Folder Management Controls. Monitor, log and audit:

- User and program access activity to in-scope files, folders, production libraries and directories

◈ Production Environment Control. Monitor, log and audit:

- User and program access activity for in-scope production environment
- changes to production environment and ensure changes are limited to change management personnel
- incidents and failures in the production environment to enable remedial action

◈ Financial Reporting Process Controls. Monitor, log and audit:

- changes to programs and data identified as key to the financial reporting process
- privileged account access to programs and data identified as key to the financial reporting process
- user account access to programs and data identified as key to the financial reporting process

Information technology alerts and monitoring safeguards mitigate risks by protecting information related to financial reporting. Risks can be reduced by ensuring the integrity of the critical and key financial systems, and costs can be reduced through alerts and monitoring safeguards by avoiding potential losses associated with data unavailability and improving response time to new threats against the IT environment.

Implementing necessary IT alerts and monitoring safeguards for enforcing corporate policies will demonstrate a more reliable control environment and enhance the auditability of IT systems.