



Sarbanes-Oxley Compliance for IT Assets and Applications

August 2006

Executive Summary

Since the introduction of the Sarbanes-Oxley Act of 2002, public companies in the United States have been devoting increasing amounts of money and resources trying to gain compliance. The Act requires that public companies have effective internal controls over financial reporting, and that the management of the company certify that there is no financial misstatement.

Since all financial reports are driven by information systems, effective internal controls over information systems are essential to maintaining effective internal controls across the organization. Today, most internal controls at organizations are manual which makes them error-prone and less conducive to repeatability and consistency. Since IT is an integral part of the internal control system required by the Act, it becomes very important that organizations manage their IT assets effectively. Getting an inventory of the IT assets either manually or by using IT asset management tools has often yielded unreliable results. Both methods are expensive, take a long time to complete and have a low repeatability factor.

BDNA's Inventory Consolidation is changing the way companies manage their IT assets. Using BDNA's Inventory Consolidation, companies get an accurate inventory of all their IT systems quickly and easily. A reliable snapshot of the IT inventory for an organization enables effective IT governance and oversight that are critical to maintaining effective internal controls in the organization.

What is Sarbanes-Oxley Compliance?

Sarbanes-Oxley Act of 2002

Several high-profile corporate scandals (e.g. Enron, WorldCom) have shaken investor confidence in recent years. The Sarbanes-Oxley Act of 2002 (the Act or Sarbanes-Oxley) was created to restore investor confidence through enhanced internal control and enterprise governance. http://www.aicpa.org/info/sarbanes_oxley_summary.htm. Management is responsible for Internal Control over Financial Reporting (ICOFR). Under the Act public companies are required to enhance their systems of internal control over financial reporting and disclosure processes. Documentation is required to demonstrate the effectiveness of internal control. CEOs and CFOs have to personally 'certify' that they have tested their system of internal controls and that it is effective. Section 404 of the Act is aimed at improving disclosure and financial reporting and requires that companies issue an annual report on ICOFR while Section 302 is aimed at improving the "Tone at the Top" by requiring CEOs and CFOs to certify and affirm that there is no misrepresentation of the information provided in their quarterly and annual reports. Auditors are required to validate this assertion and provide an 'opinion' on it.

2004 was the first full year for large public companies to attest that they are in compliance with Sarbanes-Oxley. Corporations spent millions of dollars gearing up for the first year of compliance. Most of this work was been done manually because

companies were learning what they needed to do in order for independent auditors to validate their assertions. This was very expensive due to the large numbers of people involved. Starting in 2005 companies started to automate the manual processes they put in place in previous year(s) because they could not continue to spend millions of dollars every year on this regulatory requirement.

Why is IT important?

No financial process is removed from IT. Organizations require complete and accurate information to make decisions and manage operations. Further, the financial reporting process at most of the companies today relies on their IT systems. Companies manage their data, transactions and key business processes electronically. Without IT, businesses cannot be sure that financial reporting is complete and error-free. Therefore, it is very important that a company effectively manage its IT resources.

According to Public Company Accounting Oversight Board's (PCAOB) Auditing Standard #2, "the nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting."

The Auditing Standard #2 also states the following:

IT provides potential benefits of effectiveness and efficiency for an entity's internal control because it enables an entity to

- ❑ Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data.
- ❑ Enhance the timeliness, availability, and accuracy of information.
- ❑ Facilitate the additional analysis of information.
- ❑ Enhance the ability to monitor the performance of the entity's activities and its policies and procedures.
- ❑ Reduce the risk that controls will be circumvented.
- ❑ Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

Control Frameworks

Sarbanes-Oxley requires organizations to adopt an internal controls framework. Various control frameworks exist and none has been selected as a universal standard. The Act mentions as an example the COSO framework, created by the Committee of Sponsoring Organizations of the Treadway Commission. <http://www.coso.org>. Many organizations have adopted COSO at the corporate level. However, COSO doesn't specifically cover internal controls for IT. Therefore, organizations have adopted an additional control framework for IT. The most common framework for internal controls in IT is COBIT – Control Objectives for Information and related Technology. <http://www.itgi.org>.

SOX Section 404

The section of the Sarbanes-Oxley Act that impacts Information Technology (IT) the most is Section 404. According to this section, a public company is required to issue an

internal control report as part of its annual report. The internal control report will primarily need to address the following three components:

- a) affirmation of the responsibility of the management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- b) an assessment of the effectiveness of the internal controls structure and the procedures for financial reporting
- c) an independent auditor's attestation to and reporting on the above two components.

As part of its evaluation of the operational effectiveness of internal controls over financial reporting, management must:

- Disclose all known control deficiencies and weaknesses, and
- Disclose acts of fraud

An independent auditor must validate management's assertions. The auditor may find either material weaknesses (in which case, the auditor cannot provide an "unqualified" opinion), or significant deficiencies (the controls must be remedied by the next fiscal year.)

Challenges

IT systems that store, provide access to and/or process financial information are required to provide auditing capabilities. This requires significant changes to the IT systems at the very least. In some cases companies may be required to completely replace their existing systems (that impact financial reporting) for compliance since they were not purchased/designed with auditing capabilities. For most companies, the cost of updating their IT systems to comply with the controls and reporting requirements of the Act is daunting. A \$1 billion company can easily spend over \$1 million per year in its effort to comply with SOX Section 404. Getting an accurate snapshot of the company's IT infrastructure may be extremely challenging with the manual controls that exist at most companies.

BDNA and Sarbanes-Oxley

BDNA Inventory Consolidation holds the key in such an environment. This product is a valuable tool with capabilities to help companies manage their IT assets in a way that no life cycle IT asset management tool has been able to. The product can generate a detailed inventory of the company's IT assets quickly and efficiently.

BDNA Inventory Consolidation can address certain requirements of SOX Section 404 that will give companies much greater control over their IT assets. It supports the implementation of major control frameworks such as COSO and COBIT. It enables oversight and governance of IT systems that manage information used for generating financial reports. The solution provided by BDNA addresses objectives across all four

COBIT objectives i.e., Plan and Organize, Acquire and Implement, Deliver and Support as well as Monitor and Evaluate.

BDNA's Inventory Consolidation provides:

- ❑ On-demand inventory of financial systems
- ❑ Organization and reporting

On-demand inventory of financial systems

BDNA Inventory Consolidation provides on-demand inventory of financial systems deemed critical for Sarbanes-Oxley compliance. BDNA provides a detailed inventory of critical servers, along with databases, applications, and other software running on the servers. The inventory can be created on a regular calendar, allowing the organization to track changes over time. This allows an organization to manage its IT assets effectively and enables more effective IT governance and oversight.

Organization and reporting

BDNA Inventory Consolidation can organize financial systems by organization units (such as Divisions, Business Units, or Regions), by business cycles (such as Revenue, Financial Reporting, Fixed Assets, Payroll, Procurement, Treasury, Warranty); and by business processes within each business cycle (such as Order Entry, Shipping, Accounts Receivable, etc.). For example, an organization can quickly identify the financial systems in a division (such as Purchasing) that support a given business process (e.g. Accounts Receivable process) in a region (e.g. North America). The product can provide as granular a view as the properties of databases at the organization. This is a very powerful internal control application that can be used to demonstrate the existence of internal controls over financial systems.

Strategic Services

The BDNA Strategic Services organization is staffed with experienced management consultants who can help to specialty reports that provide:

- ❑ a comparison of all financial systems over time to enable the organization to track changes in IT assets
- ❑ a list of all unauthorized software, older versions of financial applications within the organization that may not currently be supported by the vendor
- ❑ a list of all IT systems at the organization that support financial reporting that have weak security parameters such as missing antivirus protection, software versions and patches known to have security vulnerabilities, open network ports that can compromise security etc .

Summary

BDNA's Inventory Consolidation enables oversight and governance of IT systems that manage information used to generate financial reports. This meets key requirements for automation of IT controls for Sarbanes-Oxley section 404 compliance. For additional information contact: sales@bdnacorp.com.