

»» Sarbanes-Oxley Compliance

How LANDesk Management Solutions Support IT Asset Management and Overall IT Control Requirements

Abstract:

The Sarbanes-Oxley Act of 2002 implements strict financial accountability requirements for publicly held corporations. These new standards require that organizations demonstrate control of internal processes and provide documentation for both internal and external audits.

The task of maintaining the services infrastructure that supports these processes falls squarely on IT. Support activities may include installation and maintenance of standardized, software-based process management and financial tracking tools throughout the company; data storage, backup and access control; process verification, reporting and data extraction; and audit support. IT will also be required to implement controls over its own financial and reporting processes.

Automated systems management solutions such as LANDesk® Management Suite and LANDesk® Asset Manager can provide greater control over the IT infrastructure that supports both business processes and IT asset management and reporting, and substantially eases compliance with Sarbanes-Oxley and other regulatory requirements.

Nothing in this document constitutes a guaranty, warranty, or license, express or implied. LANDesk disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of LANDesk; indemnity; and all others. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of LANDesk.

LANDesk retains the right to make changes to this document or related product specifications and descriptions at any time, without notice. LANDesk makes no warranty for the use of this document and assume no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright © 2004 LANDesk Software Ltd., or its affiliated companies. All rights reserved. LANDesk is either a registered trademark or trademark of LANDesk Software, Ltd. or its controlled subsidiaries in the United States and/or other countries.

*Other brands and names may be claimed as the property of others.

LSI-0299 SP/JA

Table of Contents

Abstract:	1
Executive Summary	4
A brief overview of SOX.....	5
Key elements: Sections 302 and 404.....	6
Internal Controls = Business Best Practices	7
ITIL, COBIT and IT Support of Internal Controls	7
Implementing IT Control Objectives:	
People, Processes and Tools	8
Secure Foundations	8
IT asset knowledge and control.....	9
System wide process control	10
Conclusion.....	10

Executive Summary

The Sarbanes-Oxley Act of 2002 (SOX) requires that senior executives personally attest to the accuracy of financial reports and mandates strict financial controls, documentation and audits for publicly held companies. These processes and controls must be verified through audit, and the results of those audits must be reported in SEC filings and other financial disclosures. Substantial civil and criminal penalties are defined for chief executives of companies who fail to comply with the requirements of SOX.

By requiring strict accountability from CEOs and CFOs, SOX essentially forces organizations to build an information services infrastructure that is consistent, reliable and secure, and whose processes are well documented. This infrastructure can then feed accurate information into both financial disclosures and audits, and enable rapid implementation of new or refined business processes.

So while SOX is oriented around executive-level business processes and procedures, effective IT infrastructure will be the key enabler for the establishment of SOX processes and controls, and the key engine for demonstrating compliance. For most companies, IT will build and maintain that core information services infrastructure, as well as automate data extraction and reporting in support of both internal and external audits. Just as importantly, information security and access control are needed to protect the quality and integrity of financial data and process controls.

LANDesk Software solutions enable IT administrators to quickly implement and maintain both the hardware and software tools needed to support SOX compliance—with minimal impact on current systems and processes, and at a minimal cost.

LANDesk® solutions address three areas of specific concern for compliance with SOX:

- Developing and maintaining a secure foundation on which internal process controls and financial data can be maintained. By taking active control of the data infrastructure, IT can enable enterprise-wide processes, and can help ensure the accuracy, availability and security of both data and process controls.
- Supporting enterprise-wide implementation of high-level process task flows through a centrally located, forms-based tracking tool.
- Quickly defining standardized procedures, logging and tracking tools in order to help ensure process consistency throughout the organization.
- Enabling accurate, real-time inventory and reporting on computing hardware and software as part of an overall asset reporting process. It has traditionally been difficult to maintain accurate data on IT assets. Strong computer discovery, inventory and license monitoring tools combine with preferred state management and extended asset tracking tools to enable IT to provide accurate, validated information on IT assets to financial staff.

Flexible and adaptable infrastructure management solutions from LANDesk Software enable rapid response to changing regulatory requirements, and give organizations greater control over information services to create a secure, reliable information infrastructure. This flexibility then enables easy implementation of new policies and procedures as recommended by auditing teams for overall regulatory compliance.

A brief overview of SOX

SOX was implemented in the wake of corporate reporting scandals, with the goal “To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.”

SOX contains 11 titles that describe specific mandates and requirements for financial reporting.

- **Title I—Public Company Accounting Oversight Board (PCAOB)**
Establishes independent oversight of external corporate audits. Creates and defines a central oversight board tasked with registering public accounting firms as compliance auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control of those public accounting firms, and enforcing compliance with the specific mandates of SOX.
- **Title II—Auditor Independence**
Establishes practices to ensure that auditors remain independent and limits conflicts of interests. Describes the requirements and limits for firms that perform SOX-mandated audits. Describes pre-approval requirements, auditor rotation policy, conflict of interest issues and auditor reporting requirements.
- **Title III—Corporate Responsibility**
Mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. Defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. Enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.
- **Title IV—Enhanced Financial Disclosures**
Describes enhanced reporting requirements for financial transactions, including off balance sheet transactions, pro forma figures and stock transactions of corporate officers. Requires internal controls for assuring the accuracy of financial disclosures, and mandates both audits and reports on those controls. Requires timely reporting of material changes of financial conditions, and specifies enhanced reviews by the SEC or its agents of corporate reports.
- **Title V—Analyst Conflicts of Interest**
Establishes requirements to restore investor confidence in securities analysts and to protect analysts from retribution. Defines codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.
- **Title VI—Commission Resources and Authority**
Establishes practices to restore investor confidence in securities advisors. Defines the SEC’s authority to censure or bar securities professionals from practice, establishes authority to deny the sale of penny stocks by those found in breach of SEC standards, and defines conditions under which a person can be barred from practicing as a broker, adviser or dealer.
- **Title VII—Studies and Reports**
Defines a series of studies and reports to be issued by government agencies to analyze the regulatory conditions that led to—and allowed—the corporate scandals that prompted passage of SOX. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing and others to manipulate earnings and obfuscate true financial conditions.
- **Title VIII—Corporate and Criminal Fraud Accountability**
Also referred to as the “Corporate and Criminal Fraud Act of 2002.” Describes specific criminal penalties for fraud by manipulation, destruction or alteration of financial records or other interference with investigations. Provides certain protections for whistle-blowers.

- Title IX—White-Collar Crime Penalty Enhancements
Also referred to as the “White Collar Crime Penalty Enhancement Act of 2002.” Increases the criminal penalties associated with white collar crimes and conspiracies. Recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.
- Title X—Corporate Tax Returns
Specifies that the CEO should sign corporate tax returns.
- Title XI—Corporate Fraud Accountability
Also referred to as the “Corporate Fraud Accountability Act of 2002.” Specifically identifies corporate fraud and records tampering as criminal offenses and ties those offenses to specific penalties. Revises sentencing guidelines and strengthens penalties. Enables the SEC to temporarily freeze large or unusual payments.

Sections 302 and 404 have greatest direct impact on corporate IT departments.

Key elements: Sections 302 and 404

In effect, sections 302 and 404 require that chief executives ensure that accurate financial data is provided to investors, auditors and the SEC in periodic reports, and that both the data and the internal control processes that it provides are validated through external audit.

Section 302 requires that CEOs and CFOs take personal responsibility for the internal controls that feed up into any quarterly or annual financial reports. By signing those reports, executive officers specifically attest that:

- The report is current, accurate, complete and does not mislead or misrepresent financial conditions
- Internal corporate controls have been designed, implemented and maintained to ensure accurate information
- Internal controls are designed to specifically inform corporate officers of current financial conditions
- The internal controls have been evaluated for effectiveness within 90 days prior to the report, and the results of such evaluations are included in the report
- Deficiencies or weaknesses in internal controls that could diminish the accuracy or availability of current financial data have been reported to the auditor and auditing committee in preparation of a report
- Recent changes to internal controls to correct those deficiencies are documented within the report itself

Section 404 requires that an internal control report be prepared as part of the corporation’s annual report. This internal control report is also delivered to auditors who verify the accuracy and effectiveness of those internal controls and make recommendations for correcting deficiencies.

By focusing individual responsibility on both chief executives and their auditors for the accuracy of financial information, SOX essentially forces organizations to take direct and active control of both their internal business processes and their information infrastructure, or risk substantial civil and criminal penalties.

What does it mean for IT? Reports are only as good as the data on which they are based. IT will feel the pressure as senior executives demand stricter accountability from every department that rolls data up into corporate reports. Since IT systems underpin the activities of nearly every department, IT will receive increased focus and scrutiny.

Internal Controls = Business Best Practices

SOX essentially forces organizations to build an information services infrastructure that is consistent, reliable and secure, and whose processes are well documented. This infrastructure can then feed accurate information into both financial disclosures and audits, and enable rapid implementation of new or refined business processes.

While SOX itself doesn't mandate any particular standard for establishing or evaluating internal financial controls, it does require that companies implement a generally accepted standard easily available to the general public. The guidelines established by the Committee of Sponsoring Organizations (COSO*) of the Treadway Commission are an example of an overall control framework that meets the requirements for internal controls specified in SOX. Responsibility to report on those controls still rests with each individual company.

For more detail on COSO as it relates to SOX, see "Discussion of Amendments Implementing Section 404 on the Sarbanes-Oxley Web site at:

http://www.sarbanes-oxley.com/displaypcaob.php?level=2&pub_id=SEC-Rules&chap_id=SEC14&message_id=269

What does it mean for IT? In the modern company, control frameworks are supported by technological solutions, and IT is responsible to implement and maintain the infrastructure that forms the foundations for those solutions. The drive toward generally accepted IT service management frameworks and standards such as ITIL or COBIT should be a proactive effort that starts with IT and works up into the broader business. SOX forces senior executives to understand—and hopefully support—the need for standards-based IT management foundations.

ITIL, COBIT and IT Support of Internal Controls

Though SOX is oriented around executive-level business processes and financial procedures, effective IT infrastructure can be a key enabler for the establishment of SOX controls, and a key engine for demonstrating compliance.

In "Auditing Standard No. 2" issued by the PCAOB and approved by the SEC, the importance of IT control structures in determining the effectiveness of overall controls is recognized in paragraph 50 (emphasis added):

Some controls (such as company-level controls, described in paragraph 53) might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively.

The potential impact of IT controls on the extent of certain auditing functions is recognized in paragraph 105:

Nature of the control. The auditor should subject manual controls to more extensive testing than automated controls. In some circumstances, testing a single operation of an automated control may be sufficient to obtain a high level of assurance that the control operated effectively, provided that information technology general controls also are operating effectively.

(View the complete text of the PCAOB auditing standards at: http://www.pcaobus.org/rules_of_the_board.asp)

For many companies, IT will build and maintain the core information services infrastructure that supports financial control structures, as well as automate data extraction and reporting in support of both internal and external audits. Just as importantly, information security and access control are needed to protect the quality and integrity of financial data and process controls.

As a result, many companies are turning to enterprise-wide IT control frameworks to develop an information services infrastructure that is specifically designed to facilitate rapid response to changing business and regulatory conditions. The IT Infrastructure Library (ITIL) is the best known and most generally adopted standard for developing effective internal IT controls in support of overall service availability.

ITIL forms the basis of other IT control frameworks, including the Control Objectives for Information and related Technology (COBIT*) guidelines. COBIT specifically addresses the issue of information dependency and how that dependency impacts business processes. More importantly, COBIT addresses auditing issues and requirements and provides a satisfactory framework for an IT-based foundation for compliance with the internal process controls required by SOX.

Implementing IT Control Objectives: People, Processes and Tools

As with any broad standard, ITIL and COBIT combine people, processes and tools to enable both IT and business best practices. There are no technology magic bullets here—implementing IT control processes that can support overall business objectives not only requires that CEOs, CFOs and CIOs work together to plan, evaluate, refine and optimize core technology systems, but also determine how those systems are used throughout the organization to automate data extraction and ensure data security and integrity.

LANDesk Software solutions enable IT administrators to quickly implement and maintain both the hardware and software tools needed to support SOX compliance—with minimal impact on current systems and processes, and at a minimal cost.

LANDesk solutions address three areas of specific concern for compliance with Sarbanes-Oxley:

- Developing and maintaining a secure foundation on which internal process controls and financial data can be maintained. By taking active control of the data infrastructure, IT can enable enterprise-wide processes, and can help ensure the accuracy, availability and security of both data and process controls.
- Supporting enterprise-wide implementation of high-level process task flows through a centrally located, forms-based tracking tool.
- Quickly defining standardized procedures, logging and tracking tools in order to help ensure process consistency throughout the organization.
- Enabling accurate, real-time inventory and reporting on computing hardware and software as part of an overall asset reporting process. It has traditionally been difficult to maintain accurate data on IT assets. Strong computer discovery, inventory and license monitoring tools combine with preferred state management and extended asset tracking tools to enable IT to provide accurate, validated information on IT assets to financial staff.

Flexible and adaptable infrastructure management solutions from LANDesk Software enable rapid response to changing regulatory requirements, and give organizations greater control over information services to create a secure, reliable information infrastructure. This flexibility then enables easy implementation of new policies and procedures as recommended by auditing teams for overall regulatory compliance.

Secure Foundations

Whether you're using spreadsheets and aggregating financial data manually, using ERP systems or implementing a SOX-optimized financial control and reporting system, technology forms the foundation of modern workflow and data handling.

COBIT identifies a series of specific control objectives for IT systems designed to ensure availability and accuracy of data as required by SOX. LANDesk management solutions directly support implementation of foundation control objectives for Acquisition and Implementation, and Delivery and Support objectives, including:

- AI2—Acquire and maintain application software
AI3—Acquire and maintain technology infrastructure
AI5—Install and accredit systems
LANDesk® Management Suite enables secure, targeted application delivery, automated application healing and remote problem resolution. Automated patch management and policy-based application maintenance combine with advanced application availability technologies to automate software installation and maintenance for stakeholders across the enterprise.
- AI6—Manage changes
LANDesk® Management Suite uses detailed hardware and software inventory in combination with change control alerting to keep IT informed of changes to the operating environments of each managed computer. Policy-based management and automated application healing help maintain a preferred configuration on each computer, and application launch denial keeps unwanted change from impacting systems.

Extended inventory querying and reporting enables smooth planning for retirement, upgrade or replacement. Automated OS deployment with application and personality migration eases replacement while minimizing lost productivity and down-time. Policy-based application management automates software configuration and enables controlled expansion in the IT environment.

- DS3—Manage performance and capacity
 - DS4—Ensure continuous service
 - DS5—Ensure system security
- LANDesk® System Manager enables real-time performance monitoring for predictive failure analysis, and problem alerting enables IT to respond quickly to help ensure continuous service. Historical performance trending helps identify the need to expand capacity as performance declines.

Configuration management and software distribution automate deployment and maintenance of software-based system security measures, and modem and USB port monitoring help protect against unauthorized data transfers. Role-based administration and event logging enable limited IT access to specified systems and audit which management users performed which actions.

- DS9—Manage the configuration
- LANDesk® Management Suite uses detailed inventory in combination with software license monitoring, software distribution, OS deployment, automated patch management and change control alerting give IT tight control over the configuration of each and every managed computer. Application healing and policy-based configuration management help maintain system configurations automatically.
- DS10—Manage problems and incidents
- Extensive remote control, file transfer, chat, remote execute and remote power control enable direct and rapid response to most system problems and incidents. Direct integration with leading helpdesk vendors like Remedy and BMC extend task-focused problem resolution with direct configuration management and control features to enable efficient problem identification, tracking, resolution and reporting.

(See the third edition of “COBIT Control Objectives” from the IT Governance Institute for a complete explanation of COBIT, its objectives and methods.)

LANDesk management solutions enable IT to take direct control over infrastructure planning, inventory, configuration management, problem resolution and capacity management to create and maintain a secure foundation on which financial controls can be built and implemented.

A controlled, secure IT foundation gives companies the power to rapidly implement the recommendations of consultants, and to respond quickly and consistently to regulatory changes.

IT asset knowledge and control

The core of effective configuration management and problem resolution is extensive knowledge about IT assets, including system hardware, software, configuration and performance. This asset information is important not only for performance management, but also as it relates to financial reporting and asset control.

LANDesk® management solutions feature detailed device discovery that enables IT to find computing assets running on the network. Extensive hardware and software inventory enables IT to directly identify and document assets. Detailed software usage monitoring and alerting enables tighter policing of license agreements and more effective planning for future software purchases. Extensible inventory query and reporting enables fast, accurate identification and reporting in support of both internal and external audits.

When used in conjunction with process management tools and a unified IT asset repository, this gives IT departments the ability to directly respond to financial controls and to document both assets and depreciation. Custom data collection, contract and lease tracking, and service history tracking support detailed financial accounting for IT spending and bring a historically difficult task under direct control.

System wide process control

While building IT control is only a part of developing and documenting overall financial controls, many IT tools can transfer to provide added value to overall business processes.

For example, developing system access control and data security protects not only IT configurations, but protects financial controls as well. System event logging also enhances accountability and provides audit trails that demonstrate overall control of the information infrastructure. Similarly, centralized document storage and information gathering used to support IT asset management can be extended to support business-wide processes that reach across departments and geographies to enable consistent, accurate record-keeping and process management.

LANDesk® Asset Manager is an extensible, forms-based tool that can be adapted to support nearly any business process. Create centralized task checklists and maintain logs of key activities. Store process information in a central location supported by IT access controls to enable consistent understanding of key processes and policies, and provide secured, centralized information gathering and process reporting. While the system is optimized for IT asset management, it can provide transitional support for overall process control and documentation as well.

Conclusion

SOX forces companies to take control of business processes or face stiff penalties. Developing and documenting business processes and internal financial controls is a complex task that requires the interaction of CEO, CFO and CIO to develop a consistent system optimized to specific needs.

While there is no single magic bullet for SOX compliance, a strong and secure IT foundation will speed compliance activities, enable higher levels of process control and support both internal and external audits. LANDesk® management products can help companies take control of IT systems to implement general controls that enable the specific financial controls mandated in the regulation. By creating a secure, flexible and consistent IT infrastructure, companies adapt more rapidly to changing business and regulatory conditions.

For more information on LANDesk management solutions please contact your LANDesk Expert Solutions Partner or visit our Web site at www.landesk.com to learn more about our leading systems management solutions.