

Sarbanes-Oxley Compliance

How LANDesk® Process Manager and Other
Management Solutions from LANDesk
Support Overall IT Control Requirements

Contents

Executive Summary	3
Introduction	3
Key SOX Elements: Sections 302 and 404	4
General Control Frameworks	5
LANDesk® Solutions: Automating Support for Broad-Based Control Frameworks....	6
Secure Foundations.....	6
IT Asset Knowledge and Control.....	7
System-wide Process Control.....	7
Automated Support for Manual Controls.....	7
Conclusion	10

Executive Summary

The Sarbanes-Oxley Act of 2002 (SOX) 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 is also required to implement controls over its own financial and reporting processes.

Now that companies have completed their initial rounds of SOX compliance, they're discovering that a large portion of the overall cost goes into the manual labor required to control and monitor business processes. To drive these costs down, many IT departments are being asked to find ways to add automation to manual business processes—for example, automatically enforcing and documenting the chain of approval required to complete various transactions.

Automated management solutions such as LANDesk® Process Manager, LANDesk® Management Suite, and LANDesk® Asset Manager can provide greater control over the IT infrastructure to support both business processes and IT asset management and reporting, and to substantially ease compliance with Sarbanes-Oxley and other regulatory requirements. And while these solutions may be cost-justified by the support they provide for regulatory compliance, they also provide a strong foundation for achieving much broader risk-management objectives—enforcing organizational discipline to strengthen the business as a whole.

Introduction

SOX requires that senior executives personally attest to the accuracy of financial reports, and also 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, with processes that 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 toward executive-level business processes and procedures, effective IT infrastructure is the key enabler for the establishment of SOX processes and controls, and the key engine for demonstrating compliance. For most companies, IT must 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.

Now that the initial phase-in period for SOX has passed, companies of all sizes have completed their first rounds of compliance. Through these initial rounds, many businesses are discovering that core IT controls need to be complemented by up-front organizational discipline in order to manage risk end-to-end and to effectively manage the total cost of SOX compliance. In other words, producing auditable data at the end of a business process is only part of the compliance challenge. Best practices for regulatory compliance and enterprise risk management start at the beginning of the relevant business processes—and that means re-engineering not just IT processes, but human processes as well.

LANDesk® solutions enable IT administrators to quickly implement and maintain the hardware, software and human resources needed to support SOX compliance—with minimal impact on current systems and processes, and at a minimal cost. These solutions address the following areas of specific concern for 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, and implementing logging and tracking tools in order to help ensure process consistency throughout the organization.
- Enabling accurate asset 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, combined with preferred state management and extended asset tracking tools, enable IT to:
 - Ensure asset state
 - Understand hierarchies and dependencies between assets
 - Verify and document corporate ownership
 - Provide accurate, validated information on IT assets to financial staff
- Defining, enforcing and documenting overall business processes—including human, technical and automated processes—from initial request through final approval. Similar to the automation of IT processes to ensure that transactions are secure and documented, automated enforcement of human processes can help create a culture in which all processes are controlled and compliant by design—and can provide strong evidence of that compliance for audit purposes.

Flexible and adaptable process and infrastructure management solutions from LANDesk support consistent and compliant human behavior, 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.

Key SOX Elements: Sections 302 and 404

SOX was implemented in the wake of corporate reporting scandals with the goal, as stated in the preamble, “To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.” The act contains 11 titles describing specific mandates and requirements for financial reporting. The full text of SOX can be found at www.legalarchiver.org/soa.htm.

Each SOX title is divided into sections. The sections that may have the greatest direct impact on corporate IT departments are Title III, Section 302; and Title IV, Section 404. In effect, these sections 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 provide it are validated through external audit.

Section 302 requires that CEOs and CFOs take personal responsibility for the internal controls that feed 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 specifically to 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 the 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.

General Control Frameworks

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

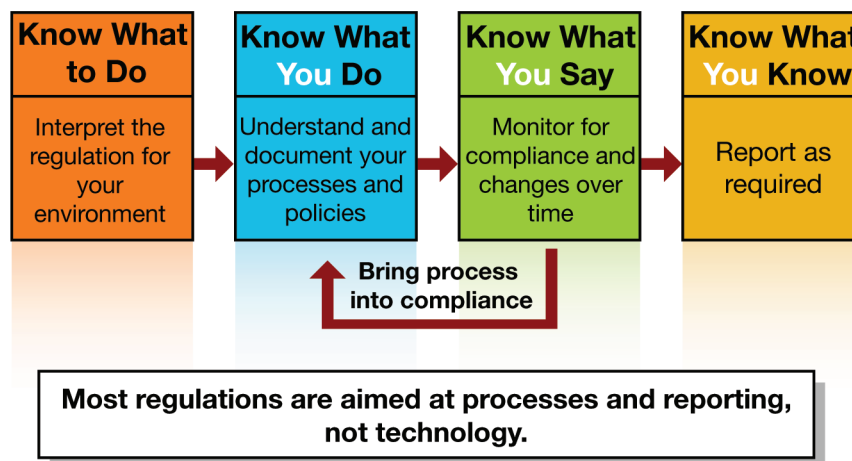
While SOX itself doesn't mandate any particular standard for establishing or evaluating internal financial controls, it does require that companies implement a generally accepted standard easily available to the general public. The guidelines established by the Committee of Sponsoring Organizations (COSO*) 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.

What does it mean for IT? Control frameworks are supported by technological solutions, and IT is responsible for implementing and maintaining the infrastructure of these solutions. The drive toward generally accepted IT service management frameworks should be a proactive effort that extends beyond IT to encompass broad business objectives. Leading standards that support this goal include the IT Infrastructure Library (ITIL*) and Control Objectives for Information and related Technology (COBIT*) guidelines. SOX forces senior executives to understand—and hopefully support—the need for IT management foundations based on comprehensive standards such as these.

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 support overall business objectives requires CEOs, CFOs and CIOs to work together to plan, evaluate, refine and optimize core technology systems—and also to determine how those systems are used throughout the organization to automate data extraction and ensure data security and integrity.

The Compliance Imperative

»» Compliance = Process Management



LANDesk® Solutions: Automating Support for Broad-Based Control Frameworks

LANDesk® 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. These solutions address four areas of specific concern for compliance with Sarbanes-Oxley:

- **Secure foundations:** 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.
- **IT asset knowledge and control:** 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.
- **System-wide process control:** Supporting enterprise-wide implementation of high-level process task flows through a centrally located, forms-based tracking tool, as well as a powerful tool for designing and automating processes from end-to-end. The ability to quickly define standardized procedures, to log events, and to track processes and minimize manual “touches” helps ensure process consistency throughout the organization.
- **Automated support for manual controls:** Creating a compliance-minded culture through automated, front-end management of human processes. The ability to demonstrate and document control over manual processes helps simplify and support regulatory audits, while encouraging efficiency, awareness and accountability throughout the organization.

Flexible and adaptable infrastructure management solutions from LANDesk help enable rapid response to changing regulatory requirements, while giving organizations greater control over information services to create a secure, reliable information infrastructure. This flexibility and

control, in turn, enables easy implementation of new policies and procedures as recommended by auditing teams for overall regulatory compliance.

Let’s take a closer look at each of these four areas of concern and how LANDesk solutions provide robust support for SOX compliance.

Secure Foundations and a Well-Defined “Front Door”

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. Maintaining control over such a foundational IT system requires that you know what applications you have in your environment, that you leverage existing tools to control access to those applications, and that you maintain overall configuration and security standards to ensure that access controls are properly implemented.

A comprehensive endpoint configuration maintenance solution integrates with asset, process and policy tools to enable IT administrators to create the secure foundations upon which a controlled, accountable application framework can be built. This requires that you identify internal policies and implement the tools to consistently maintain them.

Having created that secure baseline configuration, you need to ensure that only authorized administrators are able to change or modify the automated configuration policies that underpin that configuration. This requires complete role- and scope-based access controls to your configuration management engine—and full logging of actions taken within that tool by each authorized user.

LANDesk® Management Suite provides an active, policy-based configuration control solution along with the extended role- and scope-based access controls necessary to ensure that only authorized administrators can access critical data or make changes to your baseline configuration policies. When used in conjunction with LANDesk® Process Manager, this enables a consistent change control mechanism that requires all baseline

configuration changes to go in through a well-defined, well-documented and auditable front door. This, in turn, gives you the ability to define, implement and maintain the baseline configuration control needed to demonstrate overall control of IT-managed computing devices.

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 LANDesk® Process Manager 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. It allows you to create centralized task checklists and maintain logs of key activities. And it stores process information in a central location—supported by IT access controls—to enable consistent understanding of key processes and policies, and to 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.

LANDesk® Process Manager provides a simple, graphical way to define processes from end-to-end, as well as a powerful workflow execution engine to enforce consistent execution of processes. It allows you to automate processes across all your LANDesk® management solutions—as well as third-party applications and even manual steps—to create and document broad-based controls that simplify SOX compliance while also increasing business productivity and efficiency.

Automated Support for Manual Controls

Many organizations fail to see the role that IT can play in helping to manage and document manual processes—for example, the authorizations and approvals that need to take place in order to initiate and finalize a transaction. The problem with these manual processes is that the chain of dependencies is often poorly understood. Even if a detailed and explicit policy is in place, it's all too easy for humans to misunderstand or even intentionally circumvent the policy. And when policies are followed correctly, companies still have the burden of documenting processes thoroughly and accurately.

Even when these manual processes aren't subject to regulation, failing to follow the established policy and document each process is clearly bad for business. When these processes do fall under the scope of SOX or another regulatory mandate, these failures can have devastating

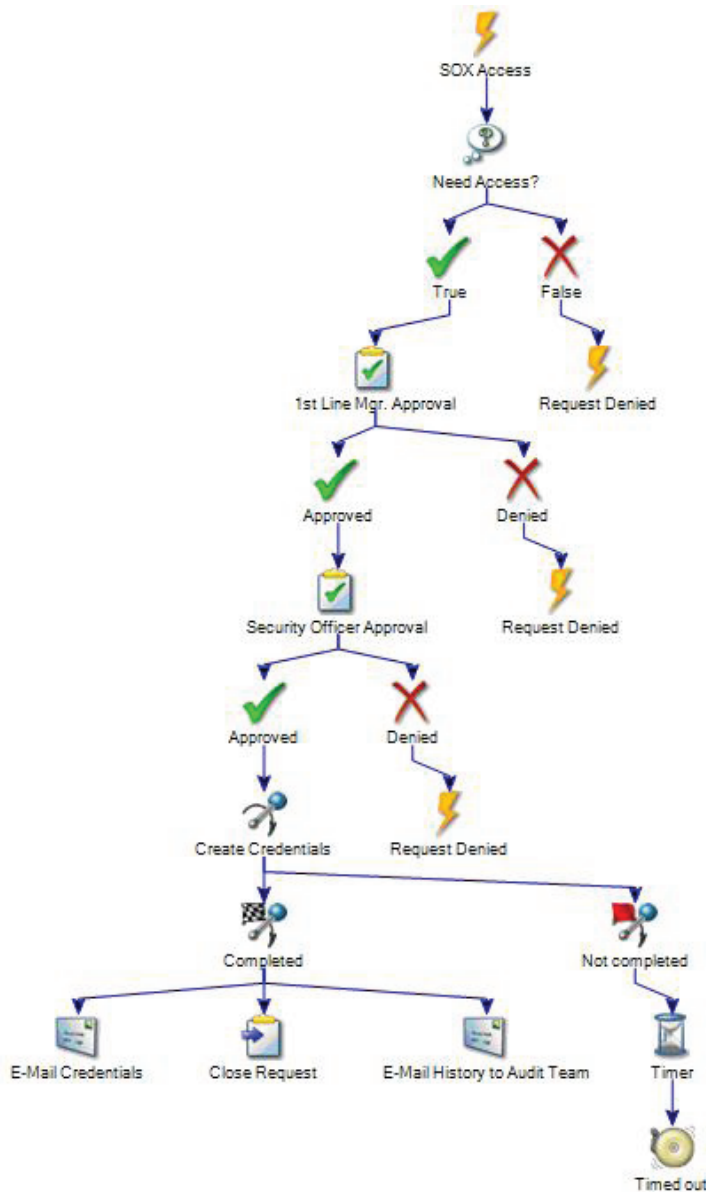
consequences for the audit process and the viability of the business itself. Companies need to create a culture of commitment to control and documentation of manual processes. IT can support this commitment by providing a front-end tool that supports the design, automatic enforcement and documentation of manual processes.

LANDesk® Process Manager adds a layer of intelligent coordination across both human-based and software-based processes—including both LANDesk and third-party solutions. It provides a graphical enterprise workflow designer and workflow execution engine that controls complex business processes—whether manual, automated or a combination—from end to end. This

gives you control of all interrelated processes across your enterprise, as well as an automated audit trail for every action and approval in every business process.

For example, SOX requires you to implement and document processes for controlling access to sensitive applications, such as the company’s financial application. As a first step to compliance, most organizations have created and documented approval workflows specifying who can grant access, how credentials are assigned to the user, and so on. When mapped out, the control might resemble the following screenshot taken from LANDesk Process Manager.

Example of an Access Control Workflow



Most organizations lack a simple, graphical tool such as this for creating and documenting processes, as well as modifying them to meet changing business and regulatory needs. But even more importantly, most organizations lack any truly effective ability to enforce these processes and document compliance—especially insofar as the processes involve manual steps such as managerial approvals.

For any process that touches in any way on a company's financials—whether it's a manual process, an automated process, or a combination of the two—SOX requires that you control and document who has access to data and who can change data. The problem is that, no matter how well a process may be designed, it's easy to circumvent it—whether for criminal purposes or even just in a misguided attempt to be helpful. LANDesk® Process Manager not only provides a powerful tool for process design, but it also acts as a gatekeeper for each step of the process—actually enforcing the entire process exactly as designed.

Even where human steps are involved, LANDesk Process Manager ensures that authorized people verify their completion of each task before the process can move forward. For example, in the access control workflow shown previously, LANDesk Process Manager automatically requires the employee's first-line manager as well as the security officer to vouch for their approvals in accordance with policy, or to document the reasons for any variation from policy. It also automates steps in the policy that don't require human control—such as sending security credentials to the end-user. And when it's time for an audit, LANDesk Process Manager provides all the documentation needed to verify that compliance.

Another example with relevance to SOX might be a policy for revoking access privileges, recovering IT assets and ensuring that all required disclosures are made at the exit interview of a newly terminated employee. LANDesk Process Manager can ensure that the entire process is followed and documented both for the automated steps, such as changing the user's status in Active Directory, to human steps, such as the exit interview checklist. Depending on the company's business model, the opportunities for designing and automatically enforcing policies that support SOX compliance are virtually unlimited.

No matter how well a process may be designed, it's only useful insofar as it's followed. And when it comes to SOX, the inability to demonstrate that processes have been followed properly can have severe consequences. LANDesk Process Manager provides a single technological entry point for every step, ensuring and documenting that each step in the process is followed exactly as designed—even when humans are involved. And if a process is circumvented for any legitimate reason, LANDesk Process Manager ensures there's an audit trail documenting the reason.

Although LANDesk Process Manager can't verify the integrity of financial data itself, it can be used to promote and document the integrity of all processes and data that feed into financial disclosures and demonstrations of regulatory compliance. LANDesk Process Manager provides a tool for defining processes, managing change, enforcing compliance, providing audit trails. It offers front-end control for crucial configuration management tasks, while providing an easy way to demonstrate control to simplify compliance audits.

And perhaps most important, LANDesk Process Manager helps support the creation and awareness of defined processes, instilling the organizational discipline that is the most basic requirement for SOX compliance—and for a healthy business.

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.

Of course, LANDesk® solutions don't provide turnkey SOX compliance. No solution could. But what LANDesk® Process Manager and other LANDesk solutions can provide is powerful support for changing the corporate culture to one of habitual commitment and compliance. And along with this commitment, LANDesk solutions provide powerful tools for automating control frameworks to ensure consistent compliance and support compliance audits. And the same tools can help streamline business processes and manage risk far beyond the scope of SOX itself.

A strong and secure IT foundation will speed compliance activities, enable higher levels of process control and support both internal and external audits. LANDesk Process Manager and other LANDesk® management solutions can help companies manage change while taking charge of IT systems and manual processes. Using these solutions to implement general controls that support the business as a whole, companies can also enable and document 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 Process Manager and other LANDesk management solutions, visit www.landesk.com, or call 1-800-982-2130.

Visit www.landesk.com for more information.