



SEVEN SIMPLE STEPS TO SARBANES-OXLEY COMPLIANCE

WHITE PAPER
FEBRUARY 2005

Introduction

IT departments play a significant role in making sure their organizations are in compliance with Sarbanes-Oxley. Yet some managers aren't sure what they have to do. This document describes the role intelligent Network Change and Configuration Management (NCCM) plays in Sarbanes-Oxley compliance, as well as outlines seven steps that can be implemented to help achieve compliance at the network device level.

Sarbanes-Oxley: What it means to IT

To protect investors by improving the accuracy and reliability of corporate disclosures, the U.S. Congress enacted the Sarbanes-Oxley Act of 2002, requiring financial institutions to establish and maintain adequate internal control structures and procedures for financial reporting, and to contain an assessment of the effectiveness of the internal control structure for financial reporting.¹ Sarbanes-Oxley applies to every part of the corporate environment, including its network device change and configuration policies.

Faced with a looming deadline, CIOs, CFOs and IT executives are puzzling over how to deal with the demands and costs of complying while finding ways to squeeze business value from these efforts. Often it is the IT department who gets tasked with coming up with a viable solution. An important component in defining the solution is creating and maintaining internal control across complex, heterogeneous networks.

To help implement Sarbanes-Oxley policies in the enterprise network, AlterPoint provides compliance capabilities in its DeviceAuthority Suite solution. Using DeviceAuthority Suite, network managers can continually detect and automatically remediate violations of Sarbanes-Oxley policies in real time. For example, those responsible for network compliance must ensure that security is not compromised, that access to network devices is granted only to appropriate staff and that the flow of data is restricted to the appropriate areas of the network. The DeviceAuthority Suite provides a way to rapidly and seamlessly enforce those poli-

cies with the certainty that all of the devices in the enterprise network achieve compliance and maintain it.

Achieving End-to-End Sarbanes-Oxley Compliance in Device Configurations

To ensure Sarbanes-Oxley compliance in device configurations, DeviceAuthority provides a fast, scalable and adaptive solution that automatically detects and remediates compliance violations in all of the network devices in the enterprise, even as the network continues to grow and change. Using DeviceAuthority monitoring, compliance, update and reporting capabilities, network managers can monitor devices for configuration changes, apply rules that detect policy violations, automatically remediate the violations and then report on the violations and remediations.

Users of DeviceAuthority Suite currently are gaining immediate benefit from following these seven simple steps to Sarbanes-Oxley compliance:

1. **Identify.** The flexible DeviceAuthority integration capabilities dynamically incorporate the ever-changing device inventory into the DeviceAuthority inventory management view providing an accurate, comprehensive inventory of all network devices.
2. **Understand.** DeviceAuthority configuration management capabilities provide a comprehensive understanding of the current state of all device configurations in the network.

¹ H.R. 3763, Section 404, "The Sarbanes-Oxley Act of 2002"

3. **Implement.** DeviceAuthority Suite allows Network Managers to define the rules that enforce the Sarbanes-Oxley policies.
4. **Detect.** DeviceAuthority compliance capabilities continually scan devices looking for policy violations, providing real-time alerts when violations are detected.
5. **Compare.** DeviceAuthority automatically compares the devices in violation with the ideal configuration model.
6. **Remediate.** DeviceAuthority Update Module automatically remediates the device configurations that do not meet the ideal to bring them into compliance.
7. **Report.** The reporting feature of DeviceAuthority Audit Module provides reports that list changes in policy status of devices over time to ensure that all compliance issues are tracked for accounting purposes.

Following these seven simple steps, you will be able to ensure that your network devices comply with the Sarbanes-Oxley Act of 2002.

Enterprises that have taken IT/business alignment seriously, and have already implemented enterprise-wide configuration and change management solution such as DeviceAuthority Suite, find complying with the regulations much faster and easier than their reactive counterparts. The reason is that DeviceAuthority Suite provides answers to the question central to compliance:

“How do I proactively control my constantly changing infrastructure so that the resources to the regulation remain in compliance?”

Hancock Bank relies on DeviceAuthority Suite to meet audit requirements and the directives of legislation such as Sarbanes-Oxley, Gramm-Leach-Bliley, and the Privacy Act. DeviceAuthority Suite’s out-of-the-box compliance rules, real-time change reporting and automated scripting capabilities, have enabled them to immediately and proactively address compliance issues as they happen.

Conclusion

Automated network change and configuration capabilities allow companies to ensure, and document, that their change and policy management processes are followed consistently. Through DeviceAuthority Suite, CIOs now have the opportunity to use a tactical issue—Sarbanes Oxley compliance—to implement a strategic configuration and change management solution that provides benefits beyond reducing the manual effort required for annual compliance auditing. Service-level management, problem resolution, patch management, capacity planning and security management issues are all related to the control of infrastructure configurations. They all need answers to the same question raised by Sarbanes-Oxley—how do I control all of the changes occurring across the IT infrastructure? Thus, it is recommended that IT organizations use their Sarbanes-Oxley budgets and resources to kill several birds with one stone—intelligent Network Change and Configuration Management.

DeviceAuthority Suite from AlterPoint provides the configuration control required for Sarbanes-Oxley compliance, in addition to providing the foundation for all other Network and System Management competencies. Intelligent NCCM is the new way to manage complex IT networks and provide results with immediate benefit to the entire organization.

For additional information, visit www.alterpoint.com or call 888.228.3422.