



Sarbanes-Oxley: A System Security Perspective

White Paper

October 6, 2005

ABOUT ALTIRIS

Altiris, Inc. is a pioneer of IT lifecycle management software that allows IT organizations to easily manage desktops, notebooks, thin clients, handhelds, industry-standard servers, and heterogeneous software including Windows, Linux, and UNIX. Altiris automates and simplifies IT projects throughout the life of an asset to reduce the cost and complexity of management. Altiris client and mobile, server, and asset management solutions natively integrate via a common Web-based console and repository. For more information, visit www.altiris.com.

NOTICE

The content in this document represents the current view of Altiris as of the date of publication. Because Altiris responds continually to changing market conditions, this document should not be interpreted as a commitment on the part of Altiris. Altiris cannot guarantee the accuracy of any information presented after the date of publication.

Copyright © 2005, Altiris, Inc. All rights reserved.

Altiris, Inc.
588 West 400 South
Lindon, UT 84042

Phone: (801) 226-8500
Fax: (801) 226-8506

BootWorks U.S. Patent No. 5,764,593.
RapiDeploy U.S. Patent No. 6,144,992.

Altiris, BootWorks, Inventory Solution, PC Transplant, RapiDeploy, and RapidInstall are registered trademarks of Altiris, Inc. in the United States.

Carbon Copy is a registered trademark licensed to Altiris, Inc. in the United States and a registered trademark of Altiris, Inc. in other countries.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other brands and names are the property of their respective owners.

Information in this document is subject to change without notice. For the latest documentation, visit www.altiris.com.

CONTENTS

Introduction..... 1
Accurate Financial Data..... 2
Financial Audit 3
**Failed Audit Implications: System Security Policy Management
Driver..... 4**
**Ensure Sarbanes-Oxley Compliance: Seven Steps to
Desktop/Server Lockdown 5**
Altiris® SecurityExpressions™ 6



INTRODUCTION

The intent of Sarbanes-Oxley is to ensure that an organization's chief executive officer (CEO) and chief financial officer (CFO) understand how their organization's financial data is prepared and that, to the best of their knowledge, the specified process is implemented and the financial data is correct. Sarbanes-Oxley is a regulation mandated by the federal government that applies to all public companies and is designed to protect the interests of shareholders and potential investors. CEOs and CFOs must sign legal documents stating that, to the best of their knowledge, the financial process is sound and the financial data is accurate. If the CEO or CFO is aware of any reason why the financial data may not be 100 percent correct and chooses not to disclose that information, then he/she may be convicted of regulatory wrong-doing and subject to penalties including personal fines or prison time. Because the possible penalties personally affect the CEO and CFO, there is added incentive for them to be highly attentive to corporate audits designed to ensure financial accuracy.

ACCURATE FINANCIAL DATA

Public financial data could be incorrect or incomplete for a number of reasons, some of which include:

- The process to prepare the financial data was flawed.
- The process to prepare the financial data was not accurately followed.
- Human error was made during the financial preparation process.
- Software applications, such as SAP, used to prepare the financials were not configured properly.
- Employees or third-party consultants who should not have had contact with the financials had authorized access.
- Unauthorized parties accessed and/or manipulated financial systems or data.
- Financial data was knowingly altered to defraud the public by inflating revenue, under estimating expenses and other such misrepresentations in order to portray an organization's financial success as greater than actuality.

FINANCIAL AUDIT

A financial audit is designed to evaluate the people and processes that prepare an organization's public financial data. These audits are quite thorough and can take days or weeks to complete. At a high-level, some of the key steps in a financial audit include:

- Ensure that the financial process is sound.
- Ensure that the financial process is employed as documented.
- Ensure that all relevant software applications are configured and used properly.
- Ensure that human error is not prevalent in the financial preparation process via random spot checks of financial data.
- Review the list of all authorized personal who have access to financial data or financial applications to ensure that all are require that access.
- Perform random system security audits to see if any unidentified or unauthorized personnel have access to the financial data and thereby have the opportunity to manipulate it.

If a financial audit shows that systems are vulnerable to security penetration, then it is possible that the financials are inaccurate because there is often no way to tell whether sabotage took place or not. The only way to decrease the chance of sabotage is to secure all key systems.

Key systems are defined as desktops that have access to domains and servers where financial data is stored. Other key systems are servers where the data itself is stored. To prevent unauthorized access, both desktops and servers need to be securely locked down in such a way that perpetrators cannot access desktops or servers either directly or indirectly (that is, via other access avenues).

**FAILED AUDIT
IMPLICATIONS: SYSTEM
SECURITY POLICY
MANAGEMENT DRIVER**

If a CEO or CFO is notified of a failed system security audit, they have essentially been informed that an unauthorized entity could gain access to the financial data. When system audits fail, CEOs and CFOs must create instant security projects to secure their systems before they can legally sign Sarbanes-Oxley documents. The combination of a failed audit and the potential penalties associated with Sarbanes-Oxley infractions (that is, personal fines and personal jail time) currently drives the creation of system security policy management projects at the majority of publicly traded companies.

**ENSURE SARBANES-
OXLEY COMPLIANCE:
SEVEN STEPS TO
DESKTOP/SERVER
LOCKDOWN**

In order to ensure system security compliance with Sarbanes-Oxley regulatory requirements, a comprehensive system security policy management process is needed.

To secure a desktop/server, there are seven basic steps:

1. Run a host-based/system vulnerability scanner against a database of thousands of known system vulnerabilities.
2. Identify key missing software patches, and patch critical systems to remove vulnerabilities due to software design or development defects.
3. Choose an industry-standard system security policy such as SANS, Microsoft, NIST, NSA, or other system security policy that is considered best practices for securing systems. These policies dictate the configurations for all key settings, thereby removing all vulnerabilities that are not fixed through patching. These settings include: registry keys, registry settings, users, groups, permissions, password settings, and many others. Most policies contain 60 to as many as 300 system settings.
4. Audit all systems against the system security policy to determine compliance status.
5. Bring all systems in compliance with the system security policy.
6. Perform additional audit checks/actions that are critical to ensuring good system security, but are above-and-beyond implementing an industry best practices system security policy and patch management solution. These audit checks include identifying and eliminating unauthorized software and hardware, as well as other vulnerability risk settings.
 - a. Identify unauthorized modems or modems with auto-answer set to "on."
 - b. Identify file sharing programs (for example, Kazaa), desktop sharing collaboration tools, and others that may have back door access into systems.
 - c. Identify programs (for example, Instant Messenger) that may carry viruses, worms, and so on.
 - d. Find old and unused administrator accounts.
 - e. Determine if the virus detect setting is "on," and if virus detection software versions and definitions are up-to-date.
7. Continuously audit systems against the overall system security policy to ensure compliance and alter systems as necessary to maintain compliance.

**ALTIRIS®
SECURITYEXPRESSIONS™**

Altiris® SecurityExpressions™ is an agentless system security audit and compliance software solution that allows companies to quickly and easily bring systems into compliance with a system security policy.

Altiris SecurityExpressions:

- Is 100 percent agentless for Windows and UNIX
- Supports system settings, patch updates, and software and hardware inventory
- Includes industry system security policies such as Microsoft, SANS and more than 20 others
- Provides ability to customize system security policies
- Offers comprehensive reporting and querying functionality
- Scales to tens of thousands of systems

To learn more about system security policy management, visit www.altiris.com.