



Understanding Compliance from an IT Point of View

Technical Brief

© Copyright Quest® Software, Inc. 2005. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Updated — September 7, 2005

CONTENTS

- ABOUT QUEST INFRASTRUCTURE MANAGEMENT..... III**
- ABOUT QUEST SOFTWARE, INC. III**
 - CONTACTING QUEST SOFTWARE..... III
 - CONTACTING CUSTOMER SUPPORT IV
- INTRODUCTION 5**
 - WHAT ARE ORGANIZATIONS DOING ABOUT COMPLIANCE TODAY? 5
- HOW DOES COMPLIANCE IMPACT IT? 6**
 - SETTING A BASELINE AND SECURING THE ENVIRONMENT..... 7
 - TRACKING USER ACTIVITY..... 7
 - ALERTING TO POTENTIAL VIOLATIONS 8
- IMPORTANT STEPS TO PREPARE FOR AN AUDIT 9**
- LEVERAGING THE QUEST COMPLIANCE SUITE 10**
 - QUEST REPORTER..... 10
 - QUEST ACTIVEROLES SERVER 11
 - QUEST INTRUST FOR WINDOWS..... 11
 - QUEST INTRUST FOR ACTIVE DIRECTORY 12
- SUMMARY 14**
- BIO - LANCE MASTEN, PRODUCT MANAGER..... 15**

ABOUT QUEST INFRASTRUCTURE MANAGEMENT

Quest Software, Microsoft's 2004 Global Independent Software Vendor Partner of the Year, provides solutions that simplify, automate, and secure Active Directory, Exchange, and Windows, as well as integrate Linux and Unix into the managed environment. Quest's Infrastructure Management products deliver comprehensive capabilities for secure management, migration, and integration of the heterogeneous enterprise.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)

Email: info@quest.com

Mail: Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Web site www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Customer Support

Quest Software's world-class support team is dedicated to ensuring successful product installation and use for all Quest Software solutions.

SupportLink www.quest.com/support
E-mail at support@quest.com.

You can use SupportLink to do the following:

- Create, update, or view support requests
- Search the knowledge base
- Access FAQs
- Download patches

INTRODUCTION

There are a variety of compliance-related regulations affecting organizations and industries today. These regulations affect publicly traded companies in different ways, and require that differing initiatives be put in place to meet a myriad of requirements. Many of the regulations are vague and cause confusion as to what IT organizations actually need to do to address compliance.

In this paper, you will learn how compliance requirements impact the IT environment, what procedures and policies organizations need to implement to address compliance, and what steps are necessary to meet these objectives. Also, you will see how you can use Quest Software's Compliance Suite for Windows in your organization to secure internal controls, automate reporting, and prepare for remediation—all critical components for addressing a compliance-related audit.

What Are Organizations Doing About Compliance Today?

Many organizations have created compliance teams that are tasked with determining which regulations affect them and how. These teams have developed internal applications and processes to meet compliance requirements. This has had a big impact on IT budgets. Many organizations have spent 30 percent more than budgeted on compliance in the past year through building these manual applications and procedures.

Also, some organizations are taking a wait-and-see approach to regulatory compliance, meaning they're waiting to be audited in order to see where they fail, before implementing procedures. This has proven to be an expensive decision, as many times these organizations have faced stiff fines and penalties. The chance of reducing these fines is often offered through remediation, if solutions to ensure future compliance are put into effect.

Above all, organizations today are learning that compliance is not a one-time event. IT professionals now realize that the manual procedures they may have put in place to pass the first round of audits will not provide a cost-effective, long-term solution. Compliance is now a way of life, and the time and money spent this year to meet compliance initiatives manually will continue to be spent until processes and procedures are automated.

HOW DOES COMPLIANCE IMPACT IT?

To the IT department, compliance means that from now on you need to know exactly who has what kind of access to what data and who has made what changes and when. You also need to be able to prove and report on user activities, and if you can't, you need to be able to take corrective action to avoid serious penalties. Depending on the size and complexity of your organization, meeting these requirements can seem daunting. But if you break them down into three primary tasks—setting a baseline and securing the environment, tracking user activity, and alerting to violations to defined policies—you can better understand and undertake the necessary steps for compliance.

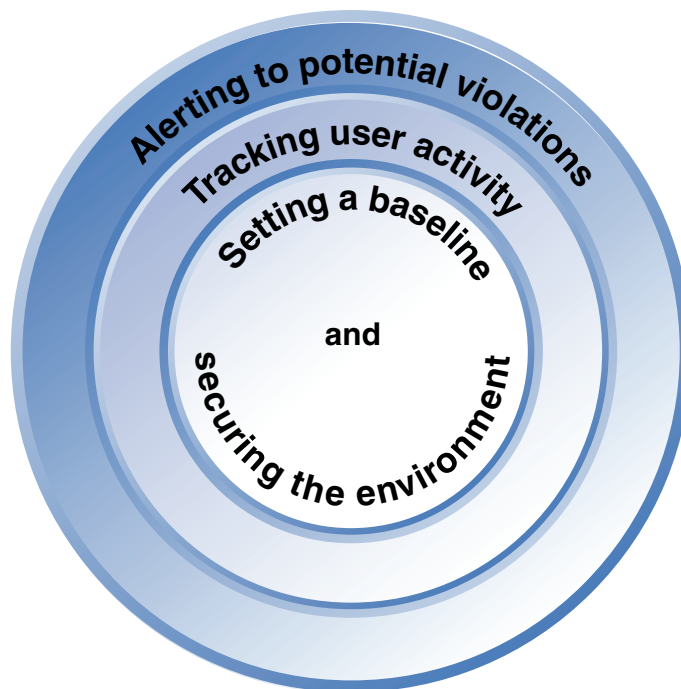


Figure 1: Necessary tasks in addressing compliance requirements

Setting a Baseline and Securing the Environment

To address compliance, IT departments are required to implement tighter security in their environments. First, however, data should be collected to establish a baseline of existing settings. This includes gathering and documenting user data, group memberships, share level permissions and domain security settings. Next, modifications should be made to meet the recommended security requirements. For example, segregation of duties must be established and enforced for administration of the environment. This ensures that no one person has total administrative control. And roles must be defined within the operation to make clear who is responsible for specific operations. These roles must be documented and approved by management.

Reports based on security settings that have been applied to the environment must be readily available in order for organizations to prove due diligence. Without proof that proper network security settings are in place, organizations may face monetary fines, or worse.

Finally, a protective boundary must exist between the Active Directory (AD) database and the administrators/users who have the control in order to granularly assign rights in the domain and to segregate duties in the organization. Limiting views and access to objects in AD improves internal controls by removing the need to assign elevated rights. Granular, detailed rights must be assigned for only the job at hand.

Tracking User Activity

The next compliance requirement is user activity tracking. Tracking must now be enabled to monitor such areas as:

- User and group management
- File and object access
- Logon/logoff activities

Permissions that have been applied to critical shares must be monitored and checked for changes in the compliance-aware environment. An administrator no longer should apply changes to permissions without approval. Critical client information or employee data often is contained on file servers, and access to this data must be secured.

Also, changes to group memberships and user rights must be tracked, as this may impact a user's ability to access, modify, or delete critical files and shares. And users' computing actions must be audited, collected, and reported on, in order to track what they are doing and how they are using their rights.

The ensuing data from the audit logs must be collected on a continual basis, stored for extended periods of time, and protected so the data is not lost due to mismanagement, as can happen when a rogue administrator is on the prowl. This ensures that organizations can produce information for historical and forensic analysis when necessary.

Alerting to Potential Violations

While many organizations that are beholden to regulatory requirements never face an investigation, some will. If your organization undergoes a review of the data within your environment, both the data itself and the practices you use to secure that data will be carefully examined.

If your organization is found to be non-compliant, a remediation process must be documented and undertaken, to resolve any issues and provide information on how you will eliminate future risks.

Having the proper tools in place for this process is an important step in the remediation of any problems. This will help your organization to avoid a potential material weakness. If financial spreadsheets or client information is compromised, a material weakness is realized, and a public announcement must be made to this effect. Obviously, this could have severe ramifications, from lawsuits to loss of future revenue. Remediation, through real-time alerting within the environment, will help to define and establish a process for correcting violations when necessary.

IMPORTANT STEPS TO PREPARE FOR AN AUDIT

With the above-mentioned tasks in mind, the following is a synopsis of the steps you should take to prepare for an audit:

- Collect environmental data and set a baseline of your configuration.
- Make any necessary modifications to meet minimum security requirements, which might include the granular delegation of rights, enabling automatic provisioning and limiting views into the Active Directory.
- Once the baseline has been determined, begin tracking daily activity of users. Authenticated users are responsible for approximately 78 percent of company theft and 50 percent of those users have an internal accomplice. Tracking must be turned on throughout the network to monitor what users are doing.
- Provide for long-term storage of all data collected in case of an audit, compromised information, or a lawsuit that requires presentation of an historical audit trail. Audit logs can become very large in a short period of time, so proper management of this data is critical to keep costs under control.
- Finally, through real-time alerting, prepare remediation procedures in the case of violations.

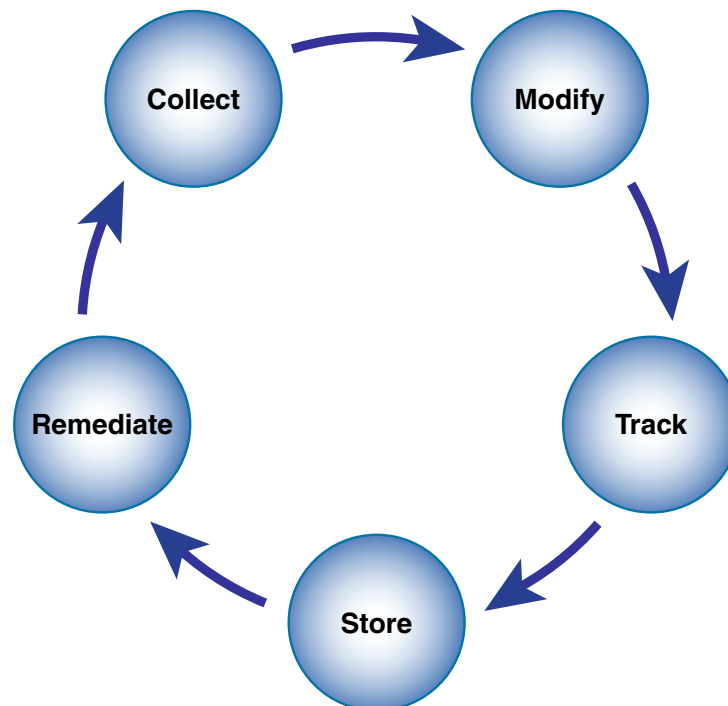


Figure 2: Preparing for a compliance-related audit requires several integrated steps.

LEVERAGING THE QUEST COMPLIANCE SUITE

An investment in products like Quest Software's Compliance Suite for Windows can help you automate your compliance processes, so you can ensure that your organization is prepared for any inquiry—without taking staff away from other projects.

Quest Software's Compliance Suite for Windows brings together products designed to help organizations solve the problems of implementing tighter internal controls, automating the collection of audit logs, producing reports, and enforcing policies. The Quest Compliance Suite for Windows—currently including Quest Reporter, Quest ActiveRoles Server, Quest InTrust for Windows and Quest InTrust for Active Directory—combines the abilities to baseline and secure the configuration of your existing network, track and alert on user activity, retain audit logs, and enforce the lockdown of business critical objects in AD in a highly scalable fashion.

Quest Reporter

Quest Reporter may seem to be a simple product at first glance—used to collect, store, and report network security and share- and folder-level permissions-related information—until you try to gather this information in an automated, scalable fashion. Reporter allows administrators to collect snapshots of the Active Directory environment, including users, groups, computers, and the attributes associated with these objects. Other types of information that can be gathered are domain and local security settings, share permissions, and audit policies.

Reporter's data collection can be scheduled and stored in a database, or it can be collected on-the-fly against the live network. Predefined reports can be modified and filtered for specific information, and new reports can be created through an easy-to-use wizard.

Baselines of your Active Directory environment can be discovered through this product. Once established, on-going reviews can be performed using Reporter, through the scheduled collection and reporting of data at intervals determined by administrators.

The output of the collected data is presented in an easy-to-read format, which can be saved in a number of other formats and delivered in many different ways, including through e-mail messages, on an intranet site, or within the console itself.

Quest ActiveRoles Server

In many corporations, Active Directory holds the keys to the kingdom since administrators can create, modify and delete user accounts as well as grant rights and permissions to users across the enterprise. The more people accessing the database the more chances there are that someone could corrupt it.

Quest Active Roles Server enables organizations to granularly assign rights and views within AD while retaining the pristine structure of the database since all administrative permissions reside outside AD.

Administrators can assign, to a single person, the ability to unlock accounts and change passwords, for example, to specific objects in AD such as a group or Organizational Unit (OU). Limiting this single users' view of AD is also a key feature in that the user is not able to view the entire directory, only what they have access to. These features can also aid in the ability to segregate the duties of authenticated users, a key to meeting compliance initiatives.

Automatic provisioning of users, their rights and properties is included in ActiveRoles Server. This enables organizations to ensure that all users and their access are created and/or changed in a uniform fashion. Consistency is a key to meeting rigid compliance standards.

Quest InTrust for Windows

Quest InTrust for Windows, at a high level, is an event log management product for Windows servers. But when you look a little closer, you'll see that it adds much more value and functionality than a simple event log collector. InTrust for Windows allows organizations to:

- Collect large amounts of local audit log data in a scalable fashion
- Store data for a long period of time at an inexpensive cost
- Report against this stored data
- Alert on business critical activity

Native event (.evt) files on Microsoft Windows computers are large in size and are being generated on a continual basis. Collecting and storing these files is extremely expensive when considering bandwidth and storage management. InTrust schedules the collection of this data, and through the use of agents, compresses it before sending it across the network, to preserve network bandwidth. Once at its final destination, the data remains compressed to save valuable disk space. The data is encrypted, yet remains in its original state, therefore making the data admissible in a court of law.

Automation of this process is critical to organizations, and InTrust for Windows provides administrators the ability to collect, consolidate, import, report, and notify on the entire process. The ability to manage the database is also handled through automated processes built into the product, thus creating a set-it-and-forget-it application.

What's more, InTrust for Windows provides remediation through an internal knowledge base that allows administrators to document steps to take when a violation occurs, as well as through real-time, action-enabled alerts.

Finally, easy-to-read, automated reports are provided in a number of different formats, and delivery methods including e-mail, Web portal, share location, and Windows SharePoint Server.

Quest InTrust for Active Directory

Quest InTrust for Active Directory allows administrators to collect, report, and alert on domain-level activity by collecting detailed native and custom audit logs from domain controllers. Through unique technology, InTrust for Active Directory enables administrators to report and alert on granular changes to AD objects including:

- Who made the changes
- What time the changes were made
- What objects or attributes were changed
- The before and after values of the changes

InTrust for Active Directory helps automate the collection, correlation, and distribution of domain-level activity by both authenticated users and administrators. Changes to user rights, permissions, and group memberships are just a few of the reports and alerts that can be distributed to users in the organization. Reports include:

- Group membership changes
- User activity list
- Logons (both successful and failed)
- User behavior anomalies

InTrust for Active Directory also enables administrators to lock down business-critical objects in the directory, such as organizational units (OUs) and/or groups, so they can't be deleted or modified. This functionality improves the stability and security of the organization, and helps you meet due diligence requirements.

InTrust for Active Directory offers the same storage and automated reporting functionality as InTrust for Windows, and it extends that power to your domain. It also extends your ability to create granular change logs and lock down objects within Active Directory.

SUMMARY

In order to meet regulatory requirements, organizations need to understand how compliance impacts the IT environment and then take the necessary steps to mitigate risk within their environments. Quest Software has helped many organizations automate their internal controls procedures to meet the requirements of external regulations. In order to better document and secure internal controls, track user and administrative activity, and reduce risk within their environments, organizations need to take a proactive approach to compliance-related activities. Quest's Compliance Suite for Windows provides a quick return on investment and allows staff to continue to work on other projects.

Quest Software is dedicated to helping organizations realize profits in their investments while meeting difficult and sometimes vague audit requirements through innovative, focused solutions. For more information about the products available in Quest's Compliance Suite for Windows, visit <http://wm.quest.com/products/Compliance/>.

BIO - LANCE MASTEN, PRODUCT MANAGER

Lance Masten, MCSE, has planned and deployed audit and security solutions at more than a dozen organizations with operations worldwide. Most notably, he spent a year on-site with one of the world's largest insurance companies, deploying Quest InTrust for Windows across 25,000 servers in an environment supporting 90,000 users. Lance applies his technical and industry knowledge to guiding the product direction of Quest's solutions for audit and regulatory compliance in the Windows environment.