Best Practices Guide for IT Governance & Compliance

Assess, Audit/Alert, and Remediate

Written By Quest Software

QUEST SOFTWARE®
Simplicity At Work®

Contents

Abstract

This white paper details three key steps for maintaining compliance with external regulations and internal security policies: assess the environment and controls; audit and alert on unapproved user activity; and implement remediation procedures. Next, we discuss four important external regulations that are driving companies to prepare for an IT compliance audit. Finally, we discuss best practices for implementing a compliance solution in order to minimize stress during your next IT compliance audit.

Introduction

Federal regulations, such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability Accountability Act (HIPAA), and the more recent Payment Card Industry (PCI) initiative, require businesses to know exactly what changes are being made to structured and unstructured data in their corporate networks. As a result, IT organizations need to provide more detailed monitoring, analysis, auditing, and reporting on the changes being made to this protected data. In fact, auditing of changes made to structured and unstructured data has become a standard business practice for most companies.

This white paper details three key steps for maintaining compliance with external regulations and internal security policies: assess the environment and controls; audit and alert on unapproved user activity; and develop remediation procedures. Then we discuss four key external regulations that are driving companies to prepare for an IT compliance audit. Finally, we discuss best practices for implementing a compliance solution in order to minimize stress during your next IT compliance audit.

While this paper is focused primarily on external regulations that apply to organizations based in the United States or conducting business in the United States, many international regulations have similar auditing requirements that make a compelling case for implementing a comprehensive data protection compliance solution.

Key Steps to Maintaining Compliance

Overview

Once an organization has met initial regulatory requirements, it must maintain compliance. But most companies find that the time and manual effort required to maintain compliance with data protection laws are cost-prohibitive. Thus, automating at least a portion of internal controls is no longer optional; it is required to maintain compliance.

When evaluating the automation of their compliance initiatives, organizations need to focus on three key capabilities:

- Assess
- Audit/alert
- Remediate

Assess

To provide management with visibility into compliance, an organization must assess the internal controls in its IT environment. This includes comparing the organization's processes and policies to industry standards and recommendations, such as security frameworks like COBIT or ISO 17799 as they relate to specific regulations. Such an analysis often results in a well-scoped compliance program that is officially recognized by management.

The organization also needs to perform a risk analysis in order to evaluate which controls it considers to be essential, and determine where gaps exist in implementing those controls. This control identification and prioritization process should be performed until a baseline of controls is established and aligned with the organization's compliance objectives as set forth by the compliance program.

Organizations should evaluate the following areas:

- User rights throughout the network
- Group memberships and the access privileges they provide
- Permissions to access files and folders
- Alternative locations of files, such as Exchange or SharePoint
- Configuration settings of systems

It is important to understand that assessment is an ongoing process for any organization, since the baseline of internal controls will change and require maintenance to meet ever-changing IT requirements. As the demands on IT organizations become more and more complex due to regulatory requirements and other compliance mandates, IT must take steps to ensure that solutions and processes are implemented to minimize risk and complexity. This strategy enables IT to function as a viable business unit, ensure fewer outages, and demonstrate more control over IT infrastructure and services.

Audit/Alert

Once the baseline for internal controls has been established, IT organizations must continually audit the environment and alert stakeholders to changes from the baseline, including violations of corporate policy and security breaches. Alerting provides immediate notification about business-critical offenses and can help mitigate exposure and risk.

Verizon's 2012 Data Breach Investigations Report shows that 97% of breaches were avoidable through simple or intermediate controls, and that 92% of incidents were discovered by a third party. Therefore, to mitigate risk, organizations must track both user and administrator activity from the time of logon to the time of logoff, including what files were accessed, what changes were made to permissions, and what changes were made to established security policies.

Auditors look for evidence that a company has processes and procedures in place to audit its users and their activities. Often auditors will include "spot checks" in their audits that require the ability to find specific data, or data from a specific point in time. Forensic analysis enables organizations to replay a violation as it occurred, which helps the organization learn how to prevent the violation from being repeated in the future.

Audit Log Management

Audit log management is about making sense of the multiple, separate audit logs generated within an organization's infrastructure. An effective audit log management strategy includes managing event logs from servers, workstations, network devices, and applications to collect, store, and report on event data.

Many companies struggle to glean meaningful information from their event logs – information that can be used to support auditing efforts. In most cases, the system administrator must sift through the multitude of event log files using native operating system tools, which is an extremely time-consuming task usually performed on a reactive, ad-hoc basis. These native event viewers are insufficient and not intended to be used as a true event log management solution because they provide no means of:

- Collecting event data from multiple systems and applications
- Generating reports in support of an audit
- Generating alerts on critical violations to organizational policies

Effective audit log management solutions do exist, however, and they will be discussed later.

Remediate

Many regulations require an organization to have a written remediation policy that specifies the actions that will be taken in the event of a corporate policy violation. Informing all internal users of the consequences of a violation can help deter them from committing violations, and specifying the steps to take in the event of a violation can help minimize its impact. Auditors often look at remediation policies very closely; they are a key component of any external audit.

There are at least two forms of remediation: proactive and reactive.

- Most organizations are reactive. Reactive remediation can be achieved through the de-provisioning of accounts based on a violation or inappropriate activity, automatic disabling of an account after a pre-defined action has occurred, or the shutdown of a server due to an unapproved change. This type of policy normally passes an audit because no IT department can effectively control everything.

- Proactive remediation techniques, which more organizations are beginning to implement, prevent unauthorized or unapproved changes. For example, an organization can prevent the modification of business-critical objects in AD, applications, or systems. Proactive remediation can also include pre-defined role management, and provisioning and de-provisioning of accounts. This helps to separate duties among administrators.

Regulations and Corporate Compliance

Overview

There are many government regulations designed to govern the practices of corporations, protect individual's rights to privacy, and spur the adherence to standard best practices. The following sections provide a general working knowledge of four key regulations that affect IT departments in the United States and, to a lesser extent, international organizations doing business in the Unites States:

- The Health Insurance Portability and Accountability Act (HIPAA)
- The Gramm-Leach-Bliley Act (GLBA)
- The Sarbanes-Oxley Act (SOX)
- The Payment Card Industry Data Security Standard (PCI DSS)

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act was signed into law on August 31, 1996. Virtually all health care organizations, including health care providers, are affected by HIPAA requirements. The intention of HIPAA is to enforce standards for privacy, security, and electronic interchange of health information. In particular, HIPAA requires health care organizations to:

- Ensure the confidentially, integrity, and availability of all electronically protected health information organizations create, receive, maintain, or transmit

- Regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

- Establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process

- Monitor login attempts and report discrepancies

- Identify, respond to, and document security incidents

HIPAA dictates the use of security standards, privacy standards, electronic transaction and code sets, and unique employer identifiers when managing and maintaining this critical data. While compliance is federally mandated, compliance also benefits health care organizations by providing patients with confidence that their sensitive personal data is safeguarded from inappropriate use.

With stiff penalties for non-compliance, health care organizations are aggressively working toward demonstrating HIPAA compliance. Meeting these challenges requires the IT department to have systems and processes in place to collect, store, and report on the events occurring within their networks, thus creating the required audit trail.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act was signed into law in November 1999. To comply with GLBA, all organizations in the financial services industry must implement a comprehensive security program specifying how their customer information is protected. In particular, these organizations must implement:

- Dual control procedures, separation of duties (SoD), and employee background checks for employees with responsibilities for or access to customer information

- Monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, customer information systems

Compliance with GLBA is regulated by federal banking agencies such as the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation. Because many organizations have already been audited and found to be out of compliance, GLBA was expanded with detailed instructions for deploying an information security program. In clarifying the new guidance, the Federal Financial Institutions Examination Council (FFIEC) states: "Security is an ongoing process, whereby the condition of a financial institution's controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and other business conditions." Institutions must prove their readiness by conducting regular self-audits of their enterprises and documenting the results.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act was passed in July 2002 as a direct reaction by the U.S. Congress to the accounting scandals of late 2001 and early 2002. It provides additional oversight to the audit process and eliminates conflicts of interest by creating a standard set of criteria that all publically held corporations must adhere to in managing their financial data. SOX also seeks to advance the standards for corporate governance.

Record retention is central to SOX. In particular, companies and their auditors are required to retain more records than before, including all documents and data that relate to an audit. Fines and jail terms are imposed for the deliberate and willful destruction of audit-related data, and an auditor is responsible for oversight of the enterprise's internal documentation surrounding the audit. In addition, the Retention of Records Relevant to Audits and Reviews as directed by Section 802 of the act states that the Securities and Exchange Commission (SEC) will dictate rules and regulations concerning "the retention of records such as work papers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analysis, or financial data relating to such an audit or review."

Companies with a market capitalization greater than $75 million were required to comply with these new rules for fiscal years ending on or after November 15, 2004; other companies have received extensions. Under the law, the retention time for records is generally five years; however, retention periods vary according to a number of variables. IT executives need to formulate and formalize an enterprise-wide strategy to best manage such data now and into the future in order to reduce the enterprise's large exposure and ensure future data integrity.

Payment Card Industry Data Security Standard (PCI DSS)

What Is the PCI DSS?

In September of 2006, five payment card brands (Visa International, MasterCard Worldwide, American Express, Discover Financial Services, and JCB) formed the PCI Security Standards Council to develop a new standard for securing their customers' payment card data. The members of the council jointly require all merchants who process payment card transactions with their brands (credit cards and signature debit cards embossed with a council member's logo) to comply with the new standard, the Payment Card Industry Data Security Standard (PCI DSS). All banks that process payment transactions associated with these cards are responsible for ensuring their merchants meet the standard, and penalties for failing to comply with the standard can be severe.

Who Is Subject to the PCI DSS?

PCI DSS has a broad applicability. In order to know if your company is subject to the PCI DSS compliance, answer the following two basic questions:

- Is your business any of the following?
  - Card acquirer
  - Merchant
  - Processing agency
- Do you store, exchange, or transmit payment card data on any of the following systems and devices?
  - Database or application servers
  - Workstations
  - Firewalls
  - Routers

If your answer to either of the preceding questions is yes, then your organization needs to be compliant with the PCI DSS regulations. One key point to understand is that these regulations apply equally to any size of organization, regardless of whether you have one employee or one million employees.

Key Requirements of the PCI DSS

The PCI DSS version 2.0 took effect on Jan 1, 2011, bringing more clarity to the existing set of requirements and introducing new ones. The PCI DSS is composed of six best-practice areas and 12 high-level requirements for securing protected data. These include strong access controls, user activity monitoring, change tracking, and record retention.

Key requirements of the PCI DSS 2.0 are outlined below.

Establish Reliable & Meaningful Audit Trails

Today, almost all elements comprising organization IT infrastructure – including operating systems, network devices, firewalls, databases, and applications – have some kind of auditing built in. However, native audit trails inherit the following issues that are hard to deal with:

- **Unmanageable volume of generated events** – In a typical IT environment, the various systems log gigabytes of event data daily, and no native log consolidation tools are provided. Therefore, organizations risk losing event data due when logs roll over. Since no one can tell beforehand what log data will be needed when bad things happen, it's absolutely critical to ensure that all audit data is captured and saved in a reliable way.

- **Cryptic descriptions of events** – Most native audit logs were added as an afterthought, when the main functions of the system or application they belong to had already been developed. That's why there is a disconnect between what the system or application puts in its logs, and what administrators would like to see in the logs to understand what specific users actually did in the system or application . Without appropriate tools, administrators are hard-pressed to distinguish the most important events from a myriad of others. Moreover, they must then try to obtain all the information they need from the cryptic descriptions recorded in the logs.

An effective solution must address both of these issues, enabling administrators to use native logs effectively.
It should also cover the gaps in what the native logs record.

Preserve Audit Data in Long-term Storage

The PCI DSS regulations require organizations to collect audit data located anywhere on the network and store it for at least a couple years (two years is the industry average). When it comes to log storage management, organizations often underestimate their log storage needs and run into significant issues down the road when they run out of the storage they allocated upfront.

Track User Access to Protected Data

The PCI DSS requires organizations to prove "who did what" for each user action involving any protected data.
The organization must capture the entire context of each user action, including all of the following:

- **The "before" and "after" values for each change event** – Simply recording that a given user made a change to a particular IT resource is not enough; each change event contains the "before" and "after" state of that resource. For example, each time a critical Active Directory object is changed, the corresponding event has to contain the value of the object attribute before and after it was altered.

- **The origin of the event** – Sometimes, when several people share the same administrative account to do their jobs, it's impossible to trace an action back to a particular individual without knowing which computer the action was performed from. In those cases, it's essential to track the origin of the event down to the particular workstation the user was logged into when taking the action.

Monitor File Integrity

The organization must monitor the integrity of all critical files and folders whose modification can compromise system security. This process must meet the following requirements:

- Staff in charge of system security must be notified of all changes to critical system files. Every time a critical system module or data file is changed, the appropriate personnel should get a notification that kicks off a change review process.
- As part of the change review process, administrators must have tools to distinguish legitimate changes from accidental and unwanted ones that can impair normal business operations.
- If a file change under investigation is deemed as inappropriate and in violation of the established security policy, there has to be a way to roll the change back before it adversely affects the business.

Establish & Enforce Separation of Duties

Organizations must implement the principle of separation of duties in order to separate auditors from administrators whose actions are being audited. In particular:

- Organizations have to make sure that audit trails are tamper-proof and protected from unauthorized modification. Attempts to clear up the log may be a sign of covering tracks after a successful attack to the compromised system. That’s why it’s important to ensure integrity and authenticity of the logs in the first place.
- There has to be a thorough delegation model granting different levels of log data access to different people within the organization. For example, the help-desk personnel might need to have access to only the parts of the audit trail showing account lockout events, while internal auditors will most likely need to have access to all log data to conduct periodic log reviews.

Review Audit Data Regularly

The PCI DSS standards require organizations to carefully review the activity of both regular and administrative users and evaluate that activity against established security policies. Different types of activity require review at different frequency:

- Administrative activity – Daily
- Access to critical system files and folders – Daily
- Failed access attempts – Weekly
- Successful resource access – Monthly

According to the 2012 Verizon Data Breach Investigation report, 96% of victims subject to PCI DSS had not achieved compliance because they had either not conducted regular assessments or had never assessed and validated their controls.

Compliance Benefits

Compliance with any of the four compliance regulations discussed above has broad benefits:

- **Avoiding fines and loss of business** – The costs of noncompliance often exceed the costs associated with maintaining compliance over time. If you fail to comply, not only will there be stiff fines and penalties, but partners and customers may take their business elsewhere, where they can be assured that their interests are protected.

- **Increased security and operational efficiency** – Compliance initiatives often increase security and operational efficiency across the organization. When IT staff starts implementing security best practices described in compliance regulations, they often expose security holes and inefficiencies in internal processes that the organization was unaware of.

- **Visibility into day-to-day IT operations** – Looking into what resources IT staff can access and what actions they are permitted to perform is often quite eye-opening. Organizations often find that employees have access to sensitive data they shouldn't see, or that multiple administrators use the same account and password. Knowledge is power, and this knowledge will empower you to improve the security of your data and IT systems.

Internal Security Policies

We have discussed several external regulations that are driving corporations to perform audits and prove compliance. There are also internal controls that an organization may put into place, typically through its IT, human resources, legal, security, or compliance departments. Many companies put auditing and security policies in place to maintain control over their infrastructures. Some companies capture daily events such as successful logons and logoffs so they can understand who is on their networks at any given time. Another example of an internal security policy is the requirement to track the activity of privileged users – those who have been granted the rights to set up new user accounts or remove users from the enterprise. The rights granted to these users can easily be abused, leaving the organization exposed to an internal security threat.

Summary

Maintaining compliance with external regulations or internal policies means, at a minimum, keeping track of all electronic documents (data files, email, images) that are covered by those regulations and tracking access to those files. Upon request, organizations need to prove, through reporting, that they have established appropriate control of access to resources. With the right auditing solution, organizations can capture, collect, store, and report on events related to security sensitive user activity (such as account creation, group membership changes, and permission changes), and also notify the responsible personnel of events that might indicate an intrusion.

Best Practices for Managing Compliance

Overview

Now let's turn our attention to best practices for implementing a compliance solution. They can be grouped into three key steps:

1. **Planning** – Determine how the regulation affects the organization. What functionality is needed from a solution, and which parts of the infrastructure are involved?

2. **Selecting** – Review vendors and solutions that best meet the requirements.

3. **Deploying** – Consider issues that may occur when rolling out the compliance solution.

Planning

To successfully implement an IT compliance solution, organizations must plan carefully and pay special attention to both technical and business needs. They must also be keenly aware of how external regulations and internal policies affect the organization and IT in general. Here are the recommended steps for planning the deployment of a compliance solution:

Step 1: Define the critical reasons for implementing a compliance solution.

When making this determination, pay special attention to the business and best practice reasons discussed in the Regulations and Corporate Governance section of this paper. Understanding auditing requirements and how they affect an organization early in the process will help in conducting a stress-free audit when the time comes. Don't forget to think about the recipient of the auditing information – is it someone like the CISO or will it be an auditor?

Step 2: Determine what functionality is required from a solution.

Based on a list of reasons defined in the previous step, identify what type of information needs to be collected and reported on. For example, for HIPAA compliance, organizations need to archive logon attempts. For this kind of task, many organizations need to collect and store events from their servers' security logs.

Once this information has been identified, choose the functionality you require from a solution:

- **Caching** enables organizations to provide reasonable assurance that no logs have been lost or tampered with.

- **Archiving** enables organizations to prove compliance with legislative regulations and prepare for forensic investigations.

- **Analysis and reporting** allows organizations to track user activity.

- **Baselining** enables organizations to measure a specific system and compare it against all other servers in the organization for standardization and compliance.

- **Real-time monitoring** provides alerts on events critical to business continuity. In addition, many products can prevent certain actions that might be detrimental – such as domain renames – even when attempted by properly provisioned users who would normally have the right to take the action.

- **Provisioning** automates the process of assigning rights to users and groups based on variables set in their profiles.

It is also useful to rank your requirements by importance. For example, is the ability to select a compatible font as important as the ability to schedule a report?

Step 3: Choose which components of the environment are critical for compliance.

Based on the list of reasons for implementing a compliance solution, organizations can single out the resources involved in the corresponding processes. For example, government regulation requires organizations to track user access to protected data, so organizations need to monitor only those computers that contain protected data, and track who has access to them at any point in time and how those rights change. In other instances, organizations may need to collect information from all servers or even from individual users' workstations.

Performing a technical assessment will help the organization determine which parts of the environment need to be monitored. Knowing this will help in estimating the required scalability of the solution. For example, a regulation might require the collection of the following information about computers on the network:

- Computer roles, such as domain controller, member server, and workstation
- Platforms and operating system versions installed
- Resources, such as file shares, directory objects, and printers, for which access will be reviewed

Step 4: Estimate the volume of information.

Estimating the space required to store events and various configuration data is very important, since the reporting and archiving functions of the compliance solution usually store quite a large amount of data. Estimation can be a time-consuming and laborious task, so it is best handled by automation.

Determining the number of resources, the type of information to be retained, and the retention period help establish the performance requirements of the compliance solution.

Selecting a Solution

Evaluation Criteria

Once the requirements have been defined, it is time to choose the right solution to implement. We recommend a technical evaluation, preferably in a lab environment that closely mimics the production environment. The evaluation process includes determining specific technical criteria and prioritizing them. The most important criteria for evaluation relate to the main functions a solution should perform – that is, the ability to assess, audit/alert, and remediate. The importance of each criterion depends on the type of solution required.

Our recommendation is to evaluate each solution against the criteria presented below and choose the one with the highest scores in the areas most important to your organization.

Regardless of the type of solution that is required, it is important that each function (assess, audit/alert, and remediate) be evaluated. We recommend that organizations consider the following for each function:

	Automation	Analysis and Reporting	Storage
Assess	Collection of data as it relates to configuration information of the server environment should be automated.	Detailed reporting should be provided in categories such as permissions, policy settings, and hardware/software information.	Information should be stored in a secure, streamlined storage area to enable the organization to track changes over time.
Audit/Alert	The capture, aggregation, and storing of events involving user access to sensitive information resources should be automated. Alerting should be available through a choice of technologies, such as email or SNMP, and easily integrated into existing processes and tools.	Detailed reporting and alerting is required to provide both periodic review of user activity and security.	Audit logs can grow quickly, so compression is a key to long-term storage.
Remediate	Provisioning should be automated to ensure that all users are assigned the correct permissions based upon their roles in the organization.	Detailed reporting should be available to ensure that all users are being assigned permissions in accordance with established security policy and business needs.	This information should be stored in a secure, streamlined storage area to enable the organization to track these changes over time.

Assess

Supported Platforms

A solution must be able to collect from a wide breadth of systems and areas, particularly all Microsoft Windows servers and their internal information. Some large enterprises may also want to collect events from Unix systems. You should also identify applications that need to be included in the auditing and compliance reporting solution. Often, this includes things like email or collaboration tools such as Microsoft SharePoint.

Configuration Management

The solution must be able to take a complete snapshot of a system and compare it against a known or recommended state of another system.

It's also important to consider events that track configuration changes to your compliance solution itself. You want to know if users are changing the auditing system.

Scalability

Scalability is the ability of the product to maintain its efficiency when the environment grows in size or volume. There are several features to investigate when determining the solution's scalability:

- **Traffic compression** – The ability to compress traffic across the network and on file storage systems
- **Filters on data sources** – The ability to specify what data to collect at a granular level
- **Compare** – The ability to compare the collected data against a defined list of requirements
- **Distributed collection** – The ability to load-balance the data collection process among several collector servers, which may be spread out geographically
- **Incremental updates** – The ability to update a configuration data store with only the changes that occurred since the last data collection

Audit/Alert

Security

Consider whether the solution provides the following security features:

- **Traffic encryption** – Encryption of traffic between agents and servers
- **Agent/server authentication** – Authentication between agents and servers
- **Optional agent-less collection** – The ability to optionally collect data without agents is required in environments where the use of agents is prohibited on important servers for security reasons
- **Caching of local data** – The ability to cache audit logs as they are being created in a separate, secure location to prevent anyone from tampering with and losing audit log data
- **Guaranteed message delivery** – The ability to withstand network or server outages and maintain a list of events that occurred during the outage. Local agent-based alerting for critical events can also be useful.

Performance

Two important criteria when evaluating performance are the number of events collected by the agent per second, and the maximum number of agents supported by a single instance. Also, the solution has to scale horizontally by adding more management servers and distributing agents among them.

Alerting / Correlation

Delivery of alerts to responsible persons should be fast and reliable and include a number of notification methods. In addition to the notifications, a series of linked response actions should be available.

- **Notification methods –** The product should be able to send alerts via Web, email and smartphone, as well as SNMP, for organizations that have deployed broad monitoring solutions such as HP OpenView.
- **Response actions –** The product should allow the flexibility to link other processes to the event when certain criteria are met. For example, if a policy change occurs, the application should be able to launch another application in response.
- **Correlation –** The product should allow organizations to gather events from different systems and group them into an alert or report to inform the administrator of suspicious activity.

Storage

Consider whether the solution offers the following features:

- **Two data storage types** – A complete product must have two data storage types: a file repository structure for archiving and a database support for analysis and reporting.
- **Backup technology** – The ability to easily back up collected event data is mandatory since some regulations require long-term storage of event data.
- **Granular restore** – The ability to restore selected granular portions of event data is a must.
- **Consolidation technology** – For widespread networks or networks with slow links, the product must be able to automatically consolidate event data from multiple data stores on a scheduled basis.
- **Retention management** – The ability to delete unnecessary granular portions of event data from the data storage is required.

Data Collection Management

Data collection management refers to the resources required to deploy and manage the entire data collection process. Below are criteria by which to evaluate this effort:

- **Configuration flexibility** – It should be easy to specify computers, define event filters, and schedule settings.

- **Agent deployment** – In order to accelerate the deployment process, a product should be able to install agents remotely. Note that a manual installation process may also be necessary when remote access to the target computer is blocked (e.g., by a firewall). Also consider other ways of automating the deployment process, such as using Group Policy.

Agent Management and Troubleshooting

The product should provide for centralized, low-cost agent management, including important features such as remote activation and deactivation of agents; automatic delivery of upgrades to agents; deployment of custom utilities on monitored computers for use by agents; and monitoring of whether the agents are functioning.

Remediate

Automated Provisioning

The solution should enable the organization to set rules for provisioning and de-provisioning all user accounts and associated permissions based on certain variables in the account.

Change Control

The solution should enable the administrator to require a chain of approvals by email before an actual change takes place in the infrastructure.

Adjust Auditing

The solution needs to be able to separate the “wheat from the chaff.” You must be able to exclude events from alerting and reporting that are considered “white noise” or normal operations.

Report

The following reporting considerations apply to each of the preceding sections (assess, audit/alert, and remediate):

- **Predefined expert knowledge** – The solution should either contain reports to meet auditing requirements or should allow the reports that come with the product to be edited to meet the requirements.

- **Data analysis and representation features** – The product should offer well-formatted reports, advanced filtering, drilldown features, charts, and forensic analysis capabilities. Consider that some reports will need to be text-based while auditors may want more visually appealing reports.

- **Report distribution system** – The solution should also enable you to export reports to commonly used formats and distribute them as needed, such as through email or by publication to a Web portal. Automation of the report creation and distribution is also important.

- **Single view** – The solution should take all information from different sources and provide a single view into the organization’s compliance initiatives.

Deploying a Solution

Once the appropriate solution has been selected, the final step is deployment. Two key issues that should be considered before starting the deployment process are :

- Performance
- Audit and event log retention settings

Once you are armed with a comprehensive technical view of the environment, you need to determine the number of management servers and their locations on the network in order to effectively distribute the load. Take into consideration the following issues that may affect the performance of the solution.

Collector Servers

For servers dedicated to collecting the data:

- **Performance rate** – This is defined as the number of events processed per second, the number of changes per day within AD, or the number of objects being managed. This will help you estimate how many monitored computers one collector server can handle. However, for best results, always test the solution in a lab environment as similar to production as possible.

- **Traffic load** – Ensure that the link between the collector server and the monitored computers is sufficient. Otherwise, network bottlenecks may impede data collection or changes being pushed to the environment. In regard to audit log management, we recommend agent-based solutions with compression and alerting as well as the ability to schedule collection during non-business hours.

This information will enable you to deploy one collector server per N computers and run the collections every X hours (or minutes), where N and X depend on the organization’s unique characteristics and needs, including the following:

- Growth rate of the logs
- Collection performance rates
- Periodicity of reporting
- Impact on traffic

Storage Servers

For servers dedicated to storing event data, be sure to make a distinction between storage servers designed for archiving purposes and those for analysis and reporting purposes. Archiving storage servers should be optimized for space consumption, whereas reporting and analysis storage servers should be optimized for fast analysis of data.

- **For archiving**, consider using a long-term storage system rather than a database system. A database system requires several times more space, and therefore has a higher total cost of ownership compared to specialized file-based repositories or native file formats (.EVT, for example). This is simply because of the cost associated with purchasing and maintaining more disks and the cost of underlying database management software.

- **For analysis and reporting**, a database is preferred, since the ability to analyze, correlate, and report is paramount. However, consider keeping the database reasonably small to provide for fast report compilation. This can be achieved by:

  - Keeping data for a defined short period of time (two to four weeks)
  - Having separate reporting databases for different parts of the environment

  Forensic analysis of security incidents and suspicious user activities usually involves digesting large amounts of historical data that cannot fit in a relational database. In such cases, consider alternative audit log data storage and querying technologies. File-based data repositories featuring sophisticated data compression and indexing techniques, as well as powerful interactive querying capabilities are becoming a de-facto standard for dealing with vast amounts of audit log data.

Storage Consolidation

To minimize traffic and performance issues, consolidate storage. Using this technique, which is illustrated below, each collector server has its own local storage, where the frequency collected logs reside. Collections here may occur every one to two hours to prevent the logs from being overwritten. Then, periodically (every night or even less often), these local storages are consolidated into a single global archive, satisfying the need to archive data or for ongoing analysis and reporting.

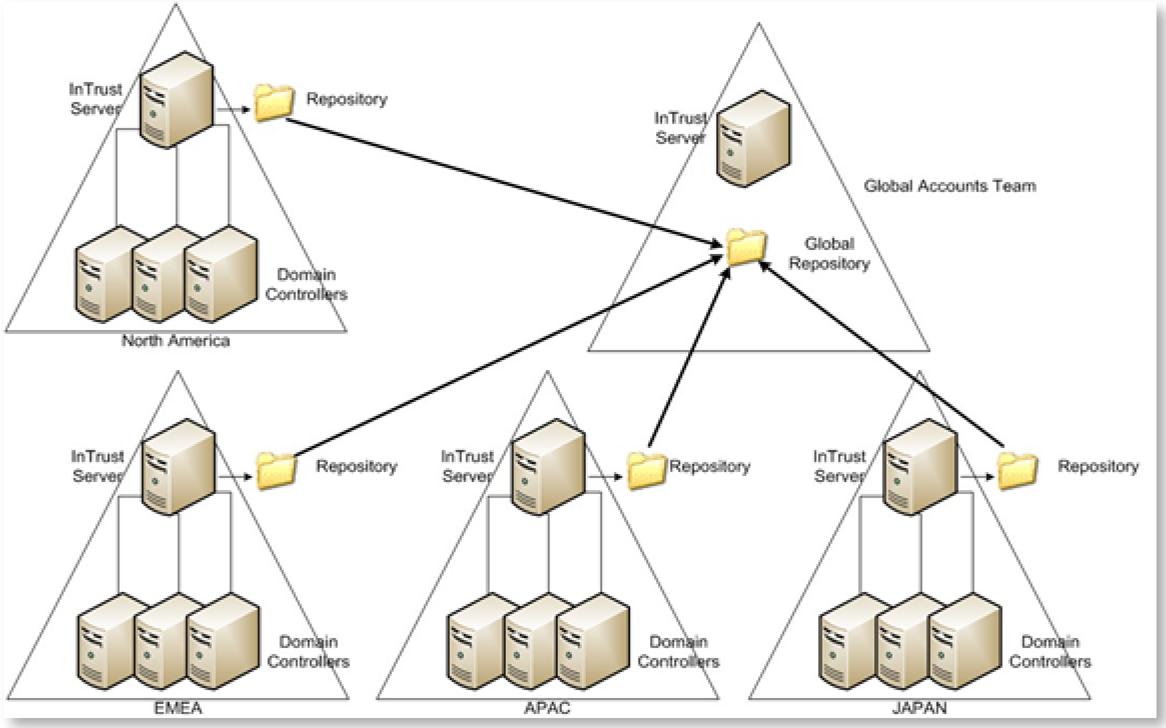

Figure 1. Storage consolidation allows widely distributed networks to regularly collect data locally and consolidate it into a central database.

Audit and Event Log Retention Settings

Another important step of deployment is to verify that the audit settings of the selected part of the environment are appropriate. In other words, confirm that the systems will register only those events that are needed to satisfy the requirements outlined earlier and no more. This will help limit the amount of storage that is required by the solution.

If audit logs of a particular system, application, or device do not provide satisfactory level of detail for critical types of user access or system changes, consider solutions that offer proprietary methods to capture needed audit information, not dependent on the native logs.

Conclusion

Whether trying to comply with federal regulations like HIPAA, SOX, or GLBA, or to meet internal security policies, effectively managing the infrastructure can take the stress out of the equation.

Managing IT governance and compliance has become a standard operating procedure for many organizations. The key to successfully deploying a solution lies in:

- **Defining requirements –** Determine the business need and how that translates into your IT controls and requirements. Assess your risks, assign values to them, and then identify gaps in your current security environment.

- **Selecting a solution –** Be sure the selected solution has sufficient functionality to assess, alert, and remediate in line with your specific compliance and business requirements.

- **Deploying the solution efficiently –** Take into account performance factors for the solution and the environment.

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

Refer to our Web site for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BridgeAccess, BridgeAutoEscalate, BridgeSearch, BridgeTrak, BusinessInsight, ChangeAuditor, ChangeManager, Defender, DeployDirector, Desktop Authority, DirectoryAnalyzer, DirectoryTroubleshooter, DS Analyzer, DS Expert, Foglight, GPOADmin, Help Desk Authority, Imceda, IntelliProfile, InTrust, Invirtus, iToken, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogADmin, MessageStats, Monosphere, MultSess, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Point,Click,Done!, PowerGUI, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportADmin, RestoreADmin, ScriptLogic, Security Lifecycle Map, SelfServiceADmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer, vRanger, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, WebDefender, Webthority, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Updated—July 2012

About Quest Software, Inc.

Established in 1987, Quest Software (Nasdaq: QSFT) provides simple and innovative IT management solutions that enable more than 100,000 global customers to save time and money across physical and virtual environments. Quest products solve complex IT challenges ranging from database management, data protection, identity and access management, monitoring, user workspace management to Windows management. For more information, **visit www.quest.com.**

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)
If you are located outside North America, you can find your local office information on our Web site.

EMAIL sales@quest.com

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

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service.
Visit SupportLink at https://support.quest.com.

SupportLink gives users of Quest Software products the ability to:

Search Quest's online Knowledgebase
Download the latest releases, documentation and patches for Quest products
Log support cases
Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information and policies and procedures.

WPV-BestPractGuidforIT-US-TG-20120712