

Surviving an Identity Audit

What small and midsize organizations need to know about
the identity portion of an IT compliance audit

Whitepaper

NetVISION™

Contents

- Executive Overview 2**
 - Introduction 2
- Business Drivers for Identity Audits 3**
 - Regulatory Compliance 3
 - Risk Management 4
- Identity Audit Overview 6**
 - Identity Audit Project Lifecycle 6
 - Identify Identity Policies 6
 - Multi-Regulatory Approach 6
 - Frameworks for a Culture of Compliance 7
 - Implement Identity Controls 8
 - Perform Identity Audit 8
 - Identity Controls Audit 9
 - Identity Behavior Audit 9
 - Identity Power Audit 9
 - Achieving Audit and Compliance Goals 10
- Creating a Culture of Compliance 10**
- About NetVision 11**

Surviving an Identity Audit

Executive Overview

Organizations of all sizes share many of the same challenges in terms of IT risk and compliance. While industry and government regulations might not apply to all organizations, all can benefit from the reduced organizational risk that results from developing a culture of compliance. Key to creating such cultures of compliance is the leveraging of industry best-practice frameworks for information security. With identity management playing a prominent role within these security frameworks, successful implementation depends on an organization's ability to audit its identity controls, identity behavior, and identity risk.

Introduction

When it comes to the governance of information technology and security solutions the size of an organization doesn't matter. Small to mid-size organizations face many of the same challenges that large enterprises confront every day. Over the past several years, government and industry regulations have become increasingly more stringent in regards to the management of organizations' user identities. Even in unregulated environments, security experts recognize the significant value of voluntarily adhering to industry best-practice frameworks for information security. This value derives from the fact that the implementation of these best-practice frameworks, along with other methods used to develop a culture of compliance, creates an atmosphere that greatly minimizes organizational risk.

While regulatory compliance projects typically span across organizations, with information technology often comprising only a portion of those overall projects, the management and control of user identities is almost always a central component of any compliance project. As a vital part of the IT systems that run an organization's day-to-day operations, identity management needs to be a major focus for any organization seeking to minimize organizational risk and to ensure regulatory compliance, especially in terms of preparing for identity audits.

Policing the Power of Identity

Digital identity powers individuals ability to move in and out of IT systems, accessing information and driving business forward.

As organizations continuously streamline their ability to interact with information, it's more important than ever to put effective policing mechanisms in place so that people are granted appropriate permissions and that sensitive information isn't abused or exposed.

NetVision makes policing the power of identity a reality with simple and effective tools for identity audit.

Read the NetVision whitepaper on policing the power of identity and find more information on NetVision solutions at www.netvision.com.

Surviving an Identity Audit

Business Drivers for Identity Audits

Identity audits are typically driven by two forces—regulatory compliance and risk management (security). Compliance may come as a result of governmental or other external regulations, or due to internal policies. Even if there are no compliance requirements, the primary goal of an identity audit is simply to provide a more secure environment and mitigate risk, which is ultimately the driver behind the regulations as well.

Over the past decade, identity management has emerged as its own industry, with organizations seeking to realize the business benefits promised by identity management systems. Unfortunately, not all identity control systems successfully address organizations' ultimate objectives in this regard, falling short of meeting the burden of proof required by IT auditors.

For example, some identity management systems can generate activity reports based on internal logs, but lack an effective means to report on identity activity that occurs outside of the management system. Some of these systems have the ability to pull logs from different external systems, but don't provide a method to cross-reference and correlate data across logs, let alone easily locate specific incidents.

Ultimately, to reduce organizational risk to the level that comes as a result of being compliant requires an identity audit solution that can provide state-based reporting and real-time monitoring of an organization's identity systems.

Regulatory Compliance

Organization's across many industries face an alphabet soup of regulatory requirements. SOX (Sarbanes-Oxley Act of 2002) regulates corporate governance and financial reporting for public companies. HIPAA (Health Insurance Portability and Accountability Act of 1996) regulates the privacy of consumer health care information. GLBA (Graham Leach Bliley Act), also known as the Financial Services Modernization Act, was primarily enabled in 1999 to allow investment, commercial banking and insurance companies to merge, but it includes important consumer privacy, safeguarding and anti-pretexting rules as well. 21-CFR-Part-11 (Title 21, Part 11 of the Code of Federal Regulations) deals with FDA guidelines on electronic records and electronic signatures in the United States. These represent only a few government and industry regulations that organization's must deal with on a regular basis.

NetVision provides industry-leading solutions for identity system audit reporting and real-time monitoring.

NetVision solutions provide complete audit capability for organizations that leverage Microsoft Active Directory or Novell eDirectory for identity and access management, as well as the ability to map specific security controls to ISO 27002 and related government and industry regulations.

Surviving an Identity Audit

Even in environments where no external regulations apply, many organizations choose to embark on compliance projects that put in place internal policies or leverage best-practice frameworks as a means to achieve specific goals. For example, many organizations seeking to provide an easier path toward mergers, acquisitions and outside investments, or that simply want to improve overall business risk levels rely on compliance with ISO 27002 (formerly ISO 17799) as a means to accomplish those objectives.

Whether the goal is to achieve compliance with governmental and industry regulations or to comply with best-practice standards and frameworks, identity audit solutions can reduce the time, effort and cost required to achieve compliance. Identity audit solutions eliminate the need to manually attempt to collect information from various systems and cross-reference that information with policies and regulations.

Risk Management

The Privacy Rights Clearinghouse (PRC) indicates that since 1995 over 167 million identities have been compromised. Throughout the first three quarters of 2007 the PRC has recorded data breaches on almost a daily basis. Industry reports show that organization insiders perpetrate a significant portion of these data breaches.

Some insider attacks, driven by malicious intent, are carried out by frustrated or revenge-driven employees. Others are opportunistically carried out by those who are intent on making a sale in the underground market of information trading. Many insider breaches are crimes of convenience or circumstance as people encounter sensitive information during the course of their daily routine. Still other internal breaches occur as a result of having security policies that conflict with an organization's business goals or expectations. Often people are asked to adhere to policies that restrict their productivity, and instead choose to ignore secure practices in the name of pursuing higher productivity levels.

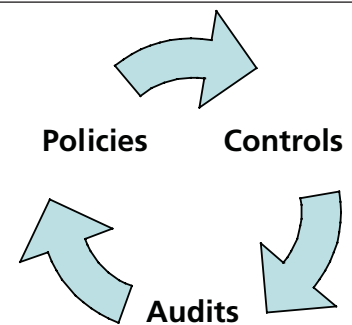
Whether these breaches are malicious, opportunistic, convenient or circumstantial, inappropriate access to documents outlining company financial performance, employee salaries or other sensitive information can lead to lawsuits, employee morale issues and even lost opportunities with customers, partners or investors.

Identity audit solutions reduce organizational risk by providing reports and monitoring of the identity systems which grant or deny system access and the user accounts empowered to act within the environment. Having effective audit and monitoring in place also has the additional benefit of acting as a deterrent for system users who might otherwise attempt to subvert policy.

Surviving an Identity Audit

Identity Audit Overview

Identity audits play a vital role in minimizing organizational risk and ensuring regulatory compliance. Many organizations turn to ISO 27002 for guidelines on how to achieve information security best practices. There are subsections of ISO 27002 that correlate to identity audit. While many requirements of ISO 27002 can be satisfied with documentation or clearly defined processes and policies, those related to identity account creation and management are best implemented via automated solutions.



For example, it's not sufficient to have a policy that states that administrators can only create a new account if approved by management. There needs to be an effective means to actually ensure and verify that accounts are only created in accordance with stated policies. Likewise, the ability to provide system reports directly from the source, along with real-time system monitoring can serve as a reliable means to demonstrate to auditors that appropriate steps have been taken to ensure that best practices are being implemented and regulatory requirements are being met and exceeded. In many cases, that demonstration of focus and attention on identity audit is the difference between passing and failing an information security audit.

Identity Audit Project Lifecycle

Identity audit projects consist of the following three primary phases that comprise the identity audit lifecycle:

- Identify identity-related policies
- Implement controls to enforce those policies
- Audit controls to verify that they enforce the policies as intended

To be successful, this lifecycle continuously repeats as identity policies are defined and redefined over time.

Identify Identity Policies

The organization's objectives in terms of risk management, compliance and business enablement need to be driving factors during the identity policy definition phase. A clear understanding of the organization's ultimate business goals makes it easier to pick and choose the best practice standards and frameworks on which its IT security and identity policies should be based. Many organizations choose to leverage the ISO 27002 framework, which maps nicely to COBIT and ultimately to COSO or governmental and industry regulations. Other organizations look for practical policies that enable as much freedom as possible while securing sensitive materials.

Multi-Regulatory Approach

Trying to comply with multiple regulations, each open to different interpretation and change, can be overwhelming for any size organization. This is particularly true when organizations attempt to handle each regulation or framework on an individual basis. As individual regulations change or new requirements are introduced, the on-going management from this type of approach becomes extremely difficult to manage.

Surviving an Identity Audit

A more practical and easier to manage tactic is to instead leverage a multi-regulatory approach. This involves working within commonly accepted standards and frameworks that can ultimately map back to specific regulations. For example, certain information security controls often satisfy requirements within multiple regulations.

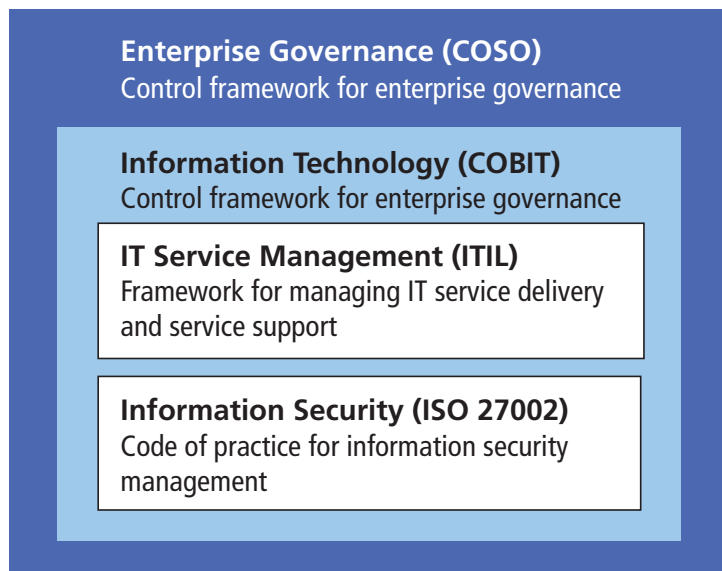
The following represent a few commonly used standards and frameworks for minimizing organizational risk:

- **COSO (Committee of Sponsoring Organizations of the Treadway Commission)**
Widely accepted (non-IT) control framework for enterprise governance and risk management.
- **COBIT (Control Objectives for Information and related Technology)**
IT-specific framework for IT governance that is designed to fit into the COSO and similar compliance frameworks.
- **ITIL (Information Technology Infrastructure Library)**
An approach to managing IT service delivery and service support.
- **ISO 27002 (Code of Practice for information security management)**
Best practice recommendations for Information Security management.

Frameworks for a Culture of Compliance

These standards and frameworks often complement each other. COSO focuses on enterprise governance. IT, governed by COBIT, is a subset of the enterprise. Within IT, there are services and there is information security each with its own specific standards framework.

These frameworks provide core building blocks for a culture of compliance. At a minimum, they make it easier to comply with specific regulations and standards. When fully leveraged, they can be used to complete one-to-one mappings from information security standards to relevant subsections within regulation guidelines. But even more importantly, when these frameworks are implemented in conjunction with employee education and compliance-focused policies and processes, a culture of compliance can be developed that minimizes organizational risk and inherently results in compliance with governmental and industry regulations.



Surviving an Identity Audit

Implement Identity Controls

Identity-related security controls can be implemented in a number of ways. Generally speaking, controls can be a combination of people, processes, physical structures, tools and software. A policy may require that a certain group of people meet on a regular basis to review information security practices. While software mechanisms can be put in place to facilitate the convening of such meetings, an automated control cannot be implemented that ensures that such meetings actually take place. However, controls can be put in place for a significant number of other types of policies that can be easily automated with software.

For example, in Microsoft network environments its common to build policies into Active Directory that leverage Microsoft Windows's built-in system security. Access to systems outside of the Windows file system can also be granted or denied based on identity data stored within Active Directory such as security group memberships or user attributes. Similar directory-based identity management techniques can be used in Novell environments as well. Organizations can also leverage third-party or in-house solutions that implement identity controls for a wide variety of other functions, from facilitating user provisioning to implementing two-factor authentication policies.

When considering the implementation of identity controls, the following factors should be considered

- Preventive vs. Detective vs. Corrective
 - Preventative controls prevent policy breaches from occurring
 - Detective controls detect events that have occurred
 - Corrective controls can take action to remediate a situation in the event of a breach
- Automated vs. Manual
 - Automated controls are implemented as software or as some other self-sufficient solution
 - Manual controls require user intervention

It should be noted that controls that are preventative and automated provide the highest level of return for organizations since they prevent breaches from occurring without human intervention.

Perform Identity Audit

Once policies and controls are in place, organizations need to be able to test and audit those controls. The goal of these audits is to ensure that the controls are keeping the organization in compliance with its defined policies. If policies are driven by regulation, then proving that the policies are being properly controlled also confirms that the organization is in compliance with that regulation. Ultimately, this is the goal of an identity audit solution – to ensure that the identity systems that implement the controls are effectively enforcing adherence to an organization's identity-related policies.

An identity audit verifies this adherence through the combination of three key audit categories:

- Identity Controls Audit
- Identity Behavior Audit
- Identity Power Audit

Surviving an Identity Audit

Identity Controls Audit

Identity controls represent the security mechanisms that enforce policy. A common example of this is a password management tool that forces users to select a complex password. If the control is effective, users will not be able to select a simple password like "123". Another example is an Access Control List (ACL). An ACL determines which users have rights to view, modify or delete a file. If the ACL is implemented correctly, it can enforce policy by disallowing any non-authorized personnel from taking action on that file.

In order to ensure compliance and minimize organizational risk, identity audit solutions must be able to identify, report on and verify the effectiveness of identity-related security controls.

Identity Behavior Audit

User behavior is probably the most important component of an identity audit. Proper controls and user rights assignments are important, but what users actually do within the environment is a more telling sign of whether there are security issues that need to be addressed.

Identity audit solutions must be able to provide real-time monitoring of user behavior based on identity policies. Examples of behavior monitoring include file access, user account creations and directory rights changes. Identity audit solutions need to be able to report who is accessing sensitive files, who created accounts outside of policy and who made changes to rights on a directory object. It should be able to identify these actions in real time and send alerts, write logs or even kick-off remediation tasks.

Identity Power Audit

Identity power is what gives people the digital accounts, rights and privileges that enable them to act within the environment. Their actions may be in accordance with policy or outside of policy. While identity behavior auditing allows you to see what people are actually doing, identity power auditing provides reports of users' assigned rights and privileges. It indicates which users make up different security groups and what file and folder rights have been granted to users or security groups. Identity power audit reports must be able to allow managers to review the rights assigned to their personnel and verify that those permissions are appropriate. Ultimately, identity power audits indicate what potential risks organizations have in their environments.

The Power of Identity is a function of identity controls, identity behavior and identity power.

NetVision provides state based reporting and real-time monitoring of directory infrastructures and file systems that automate the process of generating audit and compliance reports for:

- *Identity Controls*
- *Identity Behavior*
- *Identity Power*

Surviving an Identity Audit

Achieving Audit and Compliance Goals

To significantly improve the efficiency of achieving audit and compliance goals identity audit solutions not only need to be able to effectively audit identity controls, identity behavior and identity power, but they should also be easy to install and simple to manage and use. They should be able to integrate within an organization's existing infrastructure without requiring huge investments for deployment.

Even though an identity audit solution will typically be managed by IT professionals, the solution needs to be able to cater to the needs of the compliance professionals within the organization who will be relying on its generated compliance reports. The evidence it collects should be easily consumable by compliance management systems. Audit reports should also be able to map back to specific regulatory or framework requirements, providing evidence that it adheres to those frameworks and regulations.

Creating a Culture of Compliance

When organizations align IT with proven security practices and create environments where secure practices are adhered to on a daily basis, compliance happens by default. A culture of compliance does not come about by reacting to individual breaches or by satisfying the needs of one particular audit. Rather it occurs when organizations leverage industry-proven, best practice security frameworks to put in place the proper policies and processes, followed by the deployment of effective identity audit tools to ensure the adherence to those policies and processes.

NetVision offers the only identity audit solution on the market that addresses the three core components of identity audit—identity controls, identity behavior and identity power—in a cross-platform and easy-to-deploy framework. It's simple to manage and easily integrates into organizations' existing infrastructures. It facilitates the ability to ensure and verify compliance through audit reports and evidence that map to industry regulations and frameworks. Whether driven by security and risk mitigation or compliance with governmental or industry regulations, NetVision offers identity audit solutions that help organizations develop cultures of compliance that reduce organizational risk and ensure overall compliance.

NetVision.... Policing the Power of Identity

About NetVision

Founded in 1995, NetVision is a pioneer in identity management and security. NetVision released the first directory synchronization and password management tool 12 years ago. Today we continue to provide best practices in identity auditing. With patented real-time technologies NetVision provides critical security information which helps maintain secure compliant environments. Over 600 customers in 20 countries use NetVision products to reduce the costs of managing a heterogeneous identity environment.

© Copyright 2007 NetVision, Inc. All rights reserved.
NetVision is a trademark of NetVision, Inc. All other company and product names may be trademarks or registered trademarks of their respective companies.