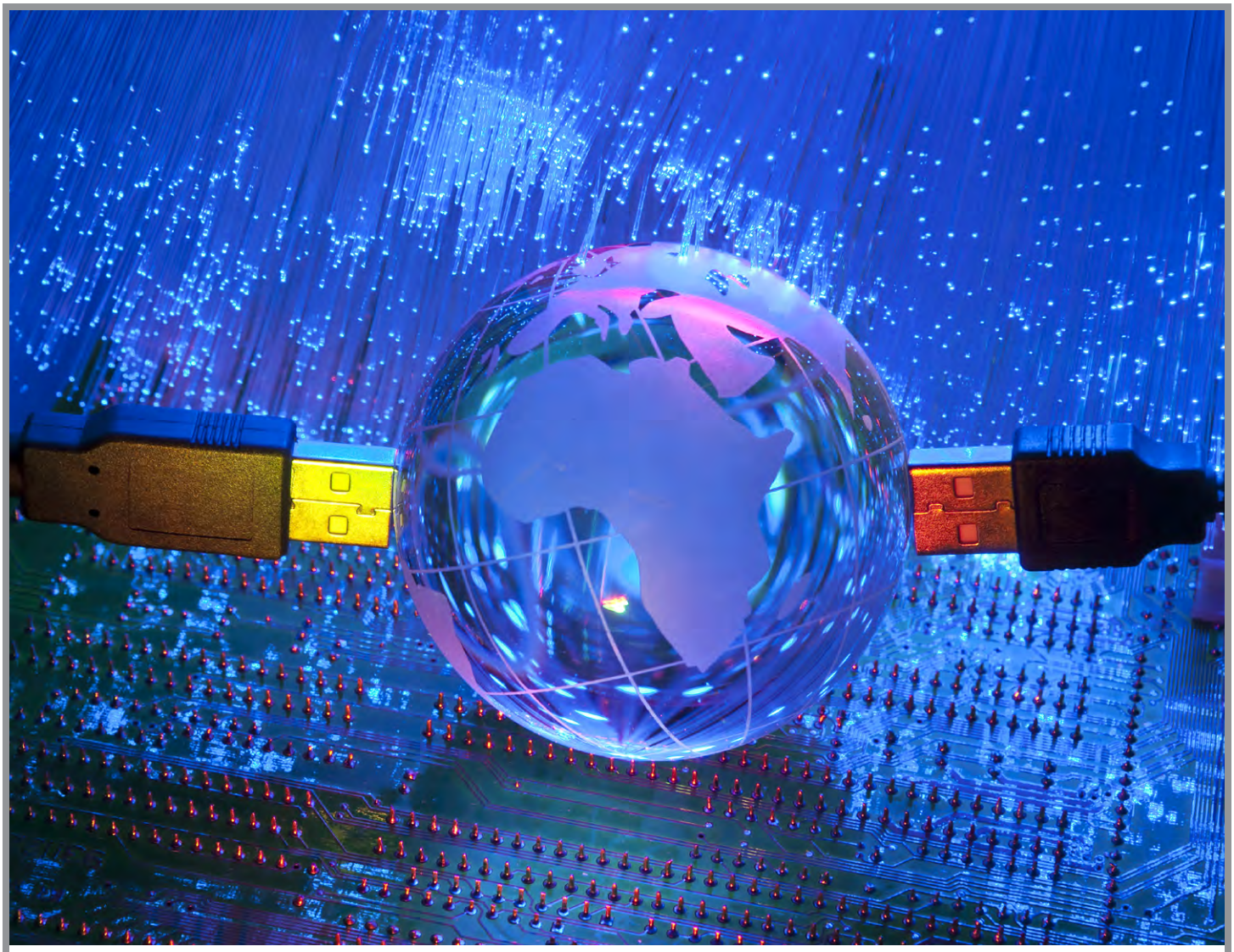
WHITE PAPER



Ensuring your IT Policies Actually Work with Change and Access Auditing

If policy and auditing don't match, neither will serve its intended purpose. Here's how to avoid conflicts and roadblocks.

By Jason Helmick

netwrix
#1 for change auditing

TABLE OF CONTENTS

netwrix
#1 for change auditing

Introduction

Your organization might be reviewing the occasional server log, perhaps even auditing for user account changes to Active Directory, but are you helping your company to create and implement a formal and rigorous auditing policy? This involves more than selecting what to audit; it means understanding and following a process of defining, monitoring, detecting and responding to your business's change and access auditing needs.

Many organizations may already have formal policies in place covering development of infrastructure, as well as mitigation of operational and security risks. The failure to have well-defined controls established to ensure the application of those policies still places the company at risk. These risks could be as nominal as the inability to stay within compliance or as severe as leakage of confidential data.

Many organizations already have formal policies in place covering development of infrastructure.

In a recent interview with Ilia Sotnikov, Director of Product Management at Netwrix, the question of understanding policies versus controls was raised:

> *"A lot of organizations, even if they do not have a formal policy around configuration changes, or on computer use, or on sharing information – there is still some sort of informal policy in place, some sort of expectations on who needs what kind of data to do their jobs—there are still expectations on the level of service from IT and the uptime and availability for different services. Even when formal policies are not in place, there is some sort of expectation between the business, the users, the IT about how the IT infrastructure is being used, how the data is accessed and how the changes are being tracked"*

Elevating the importance of change and access auditing requires a better understanding of the process and controls, and what failure means to your organization.

Is auditing really all that important?

During an outage or security breach, listen to the IT pro begin to diagnose the situation with the one question that itself answers that importance of auditing: "What's changed?"

Regardless of the infrastructure or security failure, that question starts the process of investigation to discover and resolve the current problem. How the investigation proceeds from this point is determined by the policy process and controls in place, or lack thereof, for change and access auditing. If the organization has instituted a solid and well-known process, the investigation can move swiftly to remediation as the IT and security teams have rapid access to the audit information they need. Without this information IT and security must discover the information, using valuable time and resources, and sometimes without a satisfactory resolution for the business.

Being able to quickly answer that one question "what's changed? " will help detect and prevent security breaches along with improving the quality and completeness of investigations to both outages and security breaches. These are the extreme failures that organizations fear the most. By choosing to implement an effective auditing policy, organizations gain a more subtle benefit—a verifiable change management process—which will increase the business continuity and monitor compliance on an ongoing basis.

"Even when formal policies are not in place, there is some sort of expectation about how the IT infrastructure is being used."

– Ilia Sotnikov, Director of Product Management at Netwrix

In response to a security breach scenario, Mr. Sotnikov outlined the importance of not only the mitigation to a breach, but the importance of change monitoring to prevent the breach in the first place:

> *"It's not only detection of the leak itself, we are also talking about detecting the event or the change or the incorrect setting or permission that may lead to a leak in the future."*

Organizations that have compliance requirements such as PCI, HIPAA and SOX are required to ensure that the business remains in compliance on an ongoing basis. This is not only to detect a breach, but also to prevent one from occurring in the future. Change and access auditing, with a formal process of control, can achieve the desired results.

Why organizations fail with auditing

The typical mistake that organizations make is the lack of ensuring that policies are being effectively applied. As Mr. Sotnikov pointed out: "A good policy is not just a web document sitting somewhere on an in

internal portal." Audit policies require implementation and monitoring, which means training and guidance. The work force, especially the departments for IT, security and compliance need to understand their roles and responsibilities regarding the effective application of the policies. To be successful, this often requires someone to be directly responsible for the audit policies, dedicated to ensure its ongoing application.

Many organizations have found it challenging to utilize their auditing process, even after it has been properly implemented. The failure occurs in the selection—or lack of selection—of what to monitor and audit. The business stakeholders working with IT, compliance and security, should be discussing which components are most important to audit. Some organizations will make the mistake of throwing an open net, grabbing every server log along with all access and infrastructure changes. This creates too much overload on people that are responsible for monitoring the audit information due to the excessive amount of irrelevant data. While it is possible to be successful at this, most organizations quickly overwhelm themselves.

During an outage or security breach, diagnose the situation with the one question that itself answers that importance of auditing: "What's changed?"

Resolving the lack of scope requires decisions to be made, from the beginning, to focus on the parts of the data and infrastructure that need to be audited and monitored. For many organizations that have experienced this overload, it quickly makes sense in hindsight that auditing access to a webpage of product features is not as important as access to the database containing customer records.

Who's to blame for failure?

We have all seen the publicized news reports of security breaches and data loss that have affected some of the largest and most well protected companies in the world. These are often highly sophisticated attacks, often exploits that have been discovered in a lower layer of the infrastructure and not necessarily a failure of auditing policy and controls. They should be treated for what they are, unique.

However, many smaller companies, which don't consider themselves to be targets of these types of attacks, will make the mistake of believing they shouldn't be concerned. This casual approach reduces the organization's

ability to know what is happening with their data. A formalized approach reduces the possibility of the organization slipping out of compliance, or a user mistake causing the leak of confidential data. IT will enjoy the benefit of reducing operational outages due to failed change management.

Often, IT is blamed for the outages and security breaches but that answer is much too simplistic. The solution begins with the business stakeholders understanding the cost of reputation and possible legal action due to data loss/leakage. Combine this with the benefit to increased operational continuity—auditing quickly elevates in importance. But the stakeholders can't solve this problem alone.

The solution is a joint effort along with IT, security and compliance, working with the stakeholders to define and implement the best policies for the organization. A failure is not a finger pointing exercise, but a discussion point about something that got missed and now needs to be resolved. It's this combined teamwork that will make the most effective policies and procedures.

By choosing to implement an effective auditing policy, organizations gain a more subtle benefit—a verifiable change management process.

Solving the problem through process

In discussing how to approach a solution with Mr. Sotnikov, successful organizations implemented a process involving the stakeholders, IT, security and compliance members. The importance of reviewing and repeating the process is key to meeting the organization's objectives. The process involved 6 general steps:

1. Define policies and controls
2. Monitor for policy compliance
3. Detection of non-compliant activity
4. Inform stakeholders of incidents, response and remediation
5. Postmortem analysis
6. Return to monitoring for compliance

A person or group, primarily responsible for compliance, is best to own the cycle and ensure that the process is understood, adopted, implemented and reviewed on a consistent basis. Details on each of these areas will vary depending on the organization, however the basic principles are as follows:

1. Define policies and controls

Initially this is often the most complex part of the process, involving all of the team in making the most important decisions. The decisions made here are not carved in stone and should be reviewed and changed on a continual basis. At the heart of this is an understanding of what to audit and how to accomplish the data collection goals.

What you should audit

As discussed earlier, it is possible to collect data on every aspect of all systems but this often leads to failure due to overload requiring too many eyes on the data and many processes and controls. It's better to work together to define a scope of collection—some systems are more important than others, some data is more important than others, and create the process and controls around this scope. The definition of this scope comes from the business teams and the focus should start with the most important and gradually work down to the least, then review and add as experience and resources become available. As an example, auditing access to a user's home folder may not be as important as monitoring the database that holds the company's customer information. Resources should be focused first on the important data.

"It's not only detection of the leak itself, we are also talking about detecting the event that may lead to a leak in the future."

— Ilia Sotnikov, Director of Product Management at Netwrix

Many organizations start with getting control over access such as logons and change management of identities and permissions. For a Microsoft environment this is primarily Active Directory including Group Policies. The next step is often auditing the access and permissions to the data, stored in products such as SharePoint, SQL Server and Exchange. The scope should grow to include not only the systems containing the data, but the systems and processes that have access to the data.

How you should audit

How to collect the auditing data on the defined scopes is not as easy as flipping a switch. While many products provide some sort of logging, it is usually different for each product and difficult to collect in a comprehensive and useful way for investigations and change management.

To build a comprehensive understanding useful to the audit professional, the following questions should be provided by the audit software.

- What was changed?
- Who changed it?
- When was it changed?
- Where was the change made from?

When formal policies have been applied, it helps to have an expectation of the data available when an auditable event occurs. Making sure that this information is collected, easily accessible and searchable by audit professionals is the key to making the audit process useful.

The importance of this data extends directly to IT in the event of a service outage due to change. If all change management is audited, then outages can be investigated quickly. Not all changes directly affect only the local system; some changes negatively impact other systems and without a complete picture of change management may require extended troubleshooting to resolve. As an example, a permission change made by the Storage team could negatively impact the operations of the Exchange server. If the Exchange team has quick access to this change information, a resolution to the problem can rapidly be implemented.

Organizations that have compliance requirements are required to ensure that the business remains in compliance on an ongoing basis.

2. Monitor for policy compliance

While still in this initial phase of defining the policies and controls, a decision on the tooling is required. A hodgepodge of questionable supported tools introduced by IT over time to gather and manage the auditing process is doomed to failure. Lack of support, continuity and training, coupled with product auditing limitations simply sets the stage for a complicated and unused process.

Organizations that have focused on unified auditing platforms that support the products and processes in their system are the most successful. A unified platform simplifies training and usability, helping to ensure that audit processes are followed and monitored. Without this, the rest of the steps in becoming successful become irrelevant.

3. Detection of non-compliant activity

Once formal policies are in place, the auditing platform should be able to assist IT and security in quickly recognizing non-compliant activity

through alerts and search capabilities. Teams will need to react quickly to avoid the risk of data leakage and system outages. Tools that are complicated to use, that don't provide unified search and alert capabilities become unused, causing the entire audit process to fail to achieve the organization's goals.

4. Inform stakeholders of incidents, response and remediation

Many organizations include a process of communication in the auditing process when a non-compliant event occurs. It begins with notification to the stakeholders of an event, regardless of severity and the planned response and remediation. IT and security professionals should not wait till after remediation to inform stakeholders as other compliance and legal processes may need to be initiated. The knowledge of these additional requirements is normally outside the scope of IT and the decisions that stakeholders make in regards to compliance may affect the response and remediation strategy.

Many organizations have found it challenging to utilize their auditing process, even after it has been properly implemented.

5. Postmortem analysis

At the end of any non-compliant event, regardless if detected by the access and change auditing process or a breach/outage has occurred, there must be a review to improve the overall process.

While some organizations use postmortem reviews for finger pointing, realize that mistakes will be made and something will be missed from the audit. The focus needs to be on understanding what event has occurred and if there are changes that need to be made to help prevent future occurrences. This can be as simple as adding a non-audited system to the process or refining an audit scope. An organization that is actively working to efficiently implement and monitor change and access auditing will find the process easier than an organization that hasn't started.

6. Return to monitoring for compliance

There is a cycle that IT and security professionals need to incorporate into the normal daily process of management. It is the continued practice to monitor for compliance, detect and respond to non-compliant events, and perform postmortem corrections.

Many smaller companies, which don't consider themselves to be targets of these types of attacks, will make the mistake of believing they shouldn't be concerned.

There is still the larger cycle, of all six steps that the audit/compliance professional should be driving. Bringing the stakeholders back to review the scope of auditing and discussing the monitoring and remediation processes, bringing IT and security into the room to determine where improvements are needed.

In closing

Many organizations believe they are doing something to monitor their systems but often find out that is not the case. Without formal policies and processes, without the controls and procedures in place, without the right tools to collect and alert—data leakage, unnecessary outages and extended outages affecting business continuity should be expected. The business stakeholders, working along with IT, security and compliance professionals, can implement a successful policy for access and change auditing. ■

Jason Helmick is senior technologist at Concentrated Technology