How to Effectively Audit Your IT Infrastructure

www.netwrix.com | **Toll-free**: 888.638.9749

Table of Contents

Changes Ahead: IT Auditing

The way in which IT provides value to the organization is rapidly changing. New requirements and challenges are everywhere. From compliance, security, mobile innovations to employees bringing personal equipment into the workplace, IT has now more than any other time been pushed to the limits. Compounding these problems are threats arguably more advanced than the commercially available defenses on the market today as well as threats from trusted individuals from within the organization even including human errors that can cost organizations their reputations, trust and money.

CIOs and senior leadership everywhere are beginning to acknowledge that the traditional way of doing business as an IT organization needs to change with the times to reflect these realities. Those organizations and their leadership that are prepared to take the necessary steps to revise the dynamics between them and the organizations they serve stand to benefit and thrive in the years ahead.

Enterprise auditing is a strategic and cultural shift that when implemented successfully can help satisfy regulatory compliance, improve overall security and promote efficient infrastructure oversight in the face of all these changes and challenges.

The Need to Audit the IT Infrastructure

IT professionals from the help desk to the CIO have been charged with implementing mechanisms both native and third-party to address their enterprise IT auditing needs. This task up close appears daunting to many and with good reason. The enterprise of today operates 24x7x365 and is subject to stresses of access and modifications invoked by hundred and sometimes hundreds of thousands of people each day. This growing need to audit the enterprise should come as no surprise to anyone who has been in an IT role for the past 5-10 years.

Knowing **who** changed **what**, **when** and **where** throughout the organization can save hours of troubleshooting, satisfy compliance needs, better secure the environment and permit administrators to manage multiple resources that frequently outnumber staff that are now at the critical core of operations.

What's most challenging is the diversity of platforms, systems and tools employed over the years just to sustain these daily operations. Now, various regulatory entities combined with a heightened awareness on IT security, the demands presented by auditing all of these systems around the clock in all corners of the enterprise may seem as though it were a perfect storm.

Adding to this challenge are IT operations that are required to function on tight budgets under constant watch even more so than revenue-generating functions of an organization. Leaders keep asking for more while tightening budgets and the only way to successfully secure, manage and maintain the infrastructure is to implement enterprise-wide IT auditing.

Planning

To successfully audit the enterprise, there needs to be a priority list and a methodical approach to implementation that takes into account the various aspects to be addressed along the way. IT security and compliance auditing are perhaps at the top of the organizational IT priority list and therefore can expect to have some degree of senior management support.

This can greatly help transform the organization because there will likely be changes that need this support to be successful. IT departments can use these follow steps to achieve their IT enterprise auditing goals:

1. Take an inventory and establish preliminary priorities

Start with an inventory of systems and hardware that are owned and managed by IT including computers, servers, mobile devices, file storage platforms and even network appliances such as firewalls, switches, and routers. During the inventory, place a value on the data which they store or the role they serve and place a value on their need.

Your goal here is to quickly give an estimated assessment of risk to each asset for further evaluation later. Involve Human Resources and Legal early in the process throughout to help identify those key areas that need ongoing auditing. This helps to further gain support and increase awareness across the organization. Document everything for future reference as this will form the foundation of your written plans and efforts auditors will want to see.

2. Eliminate waste, consolidate and replace assets

Find opportunities to retire or replace aging equipment and platforms. These decisions will be tied to the existing budget and may be cost-prohibitive. Estimate the time required to implement any replacements or consolidations in the context of the final objective which is to audit your environment.

The benefit of this assessment will be to provide awareness of what can readily be audited versus what assets may require additional effort to facilitate ongoing auditing. Document everything to measure progress and have a reference as you move forward which will also serve to satisfy auditors.

3. Categorize remaining resources from most auditable to least

Looking at the systems that remain and keeping in mind what those resources represent in terms of data storage or access control, look to categorize these based on expected capacity for auditing. Some systems and hardware will more readily facilitate auditing. Best case scenario, the more auditable systems will contain the information most at-risk.

Strategically, consider shifting at-risk information and resources to systems that will more readily permit auditing. Some adjustments to the environment may be justifiable before implementing any auditing solution so as to audit the most resources in the least amount of time accurately and effectively.

A good example is Windows servers. These have limited native auditing built in and this can be quickly enabled to start auditing events such as file access and logon/logoff events. Many storage appliances also have some form of built-in auditing capabilities.
Again, document everything so that everyone involved in IT and these goals begin to become intrinsically aware of the cultural changes that are taking place as a result of auditing the enterprise.

4. Look for an auditing solution that will cover the most assets in the least amount of time

Implementing enterprise auditing is an ongoing, long term effort. It will become an integral part of daily IT life once the transition has been made from little or no auditing to widespread auditing. Expectations should be balanced with what can be done in the allotted time frame versus what will need to be done over the longer term. The objective when starting out or improving upon existing efforts is to make measurable progress.

The absolutely most critical goal here is to select a reputable vendor with a broad set of tools that has a good record of helping customers and a proven track-record of delivering product enhancements and updates to service the constantly changing nature and requirements of enterprise auditing. Doing so will require fewer contacts, support arrangements, and licenses to maintain and manage moving forward. This will also require flexible licensing, scalability and centralized long-term data storage as your needs and environment change over time.

Auditing will need to be flexible, easy to setup and operate in parallel to most major IT initiatives moving forward. The audit store will also need to be equally flexible and reportable for as long as 7 years per certain regulatory requirements. A solution that can move with rapid change will save time, money and reduce overall stress. Document and expect needs will change quickly as more information is gathered and weighed against priorities and timelines.

Implementation and What to Expect

The amount of time to implement an effective IT auditing solution in the enterprise will vary. It's difficult to quantify time and every environment is different. Some may have equipment that is many years old and may present special challenges to auditing while others may have a narrow assortment of technologies. These considerations will need to be mapped out in advanced and documented.

To deliver auditing to the enterprise could result in 50% of the total time taking inventory and consolidating, 25% prioritization, and system/platform preparation, and 25% implementation. Don't forget to account for documentation as this will be a measurable part of the overall effort. Starting out with the end result in mind will help establish realistic, attainable short term goals that will roll up into larger, longer term goals.

Keeping a balance will help the IT department and those involved in the project including Human Resources and legal staff looking forward to each stage of the implementation while building the cultural and behavioral competencies that will be required to sustain auditing and compliance as well as security practices for the long term. Be prepared to be flexible and adjust as conditions change.

Scope of Challenges

Implementing enterprise auditing in diverse IT environments is common. Most IT departments have a wide array of platforms and services to serve end-users and customers. Here is a typical list of critical resources IT departments must consider and the types of information and access control they represent:

- Windows Active Directory (2000-2008R2, 32 and 64-bit platforms) – Manages access control, permissions, and serves as the central directory for the organization.
- Windows Group Policies – Access control mechanisms critical to security of information and to limit risks to systems and servers bound to Active Directory.
- Exchange servers – Messaging data contains confidential information from senior management, product management, marketing, production, engineering, human resources, legal, etc. Many regulations speak directly to monitoring access to messaging services.
- SQL servers – Primary data storage for customer data including credit card information, patient data, social security numbers, banking information, web applications, sales data and more. Like, messaging, database access will need auditing to comply with regulations.
- File servers and storage appliances – Data storage for financial statements, trade records, contracts, legal documents, agreements, business and marketing plans, proprietary information, reports, collateral. These can include Windows file servers with DFS shares and clustering as well as platforms such as NetApp Filer and EMC Celerra.
- VMware – Virtualized systems require equal protection to that of physical systems that store data, SQL servers, Domain Controllers all serving file and data storage as well as access control systems.
- SharePoint – Document and data sharing across business groups, departments and units similar to SQL and file server systems and storage devices.
- Servers – Physical systems with local access controls, services and business critical applications and web services for sites both internal and external also to be considered a sub-requirement to all of the above.
- System Center Virtual Machine Manager – Virtualized systems performing access control and file storage as well as SQL storage functions.

All of the above systems likely represent what most organizations will face when implementing auditing in the enterprise. Each asset behaves in a unique way and depending on the types of information stored on them or the extent to which these systems facilitate access control will carry individual priorities with regards to auditing.

Solutions

Solutions exist to address these challenges quickly and easily. These come in a wide variety of options to suit a wide range of needs. The Netwrix Auditor solutions can address all of these auditing needs, provide complete visibility into your on-premises or cloud-based IT environment, and help sustain compliance in the enterprise quickly, easily and cost-effectively.

Netwrix Auditor is a visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments to protect unstructured data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

The Netwrix Auditor platform utilizes an efficient, enterprise-grade architecture that consolidates audit data from multiple independent sources with agentless mode of operation and scalable two-tiered storage (file-based + SQL database) allowing the retention of audit data for 10 years or more.

Download a Free Trial of Netwrix Auditor

About Netwrix Corporation

Netwrix Corporation provides a market-leading visibility and governance platform for on-premises, hybrid and cloud IT environments. More than 150,000 IT departments worldwide rely on Netwrix to detect insider threats on premises and in the cloud, pass compliance audits with less expense and increase productivity of IT security and operations teams. Founded in 2006, Netwrix has earned more than 90 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Valuable Resources

netwrix.com	–	Netwrix provides purpose-built change auditing solutions, and free tools to help secure and maintain the IT enterprise.
infosecisland.com	–	Compliance and security professionals present today's most compelling arguments and solutions for network security and facing organizations today.
petri.co.il	–	The Petri IT Knowledgebase community of experienced IT professionals with articles, reviews, how-to instructions and technology updates.
itil-officialsite.com	–	Information Technology Infrastructure Library provides IT service management focusing on aligning IT services with business needs.
4sysops.com	–	Great online resource geared towards Windows administrators. You'll find articles about Windows technology, reviews of admin tools, tips, and news for admins.
windowsitpro.com	–	Provides in-depth articles, news and support for IT professionals supporting a Windows environment.
spiceworks.com	–	Vibrant and growing IT professional community and toolkit for help desk and network monitoring.

Netwrix Corporation, 300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618, US

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-318-0261