



IT Director's Reference Series

*Understanding and Managing
Security Audits*

Index

UNDERSTANDING AND MANAGING SECURITY AUDITS	3
Why Audit IT Security	3
IT Security Audit Overview	4
Preparing for an audit	4
Focus on strengths and weaknesses	5
After the audit	5
IT Security -- The View from the Inside, Out	6
Policy Assurance	7
Self-Auditing for Security	7
USING ENTERPRISE AUDITOR'S CHANGE MANAGEMENT AND SCHEDULING FOR SECURITY AUDITS	8
Baselines: Key to Change Management	8
Security Template	8
Creating a "Cycle of Control"	9
Summary	10

IT Director's Reference Series

Understanding and Managing Security Audits

Why Audit IT Security

The IT infrastructure is a corporation's most valuable asset, delivering competitive advantages, processing the bulk of business transactions, and storing confidential information on all areas of the company, including financial data, customer and supplier databases, engineering schedules, business plans, human resource records, and email. Today most of this information is accessible online. And it's all vulnerable. It must be protected constantly and thoroughly without interrupting business.

Failure to do so can result in staggering losses, both tangible and intangible. In 2003 it was estimated that businesses lost \$1 Billion due to viruses. The projection for 2004 is \$2-\$3 Billion. Add to that the intangible, such as loss of competitive advantage and customer trust and it's clear: secure your data or be doomed.

Enterprises invest heavily in infrastructure security, often taking a medieval fortress approach: keep the hackers and bad guys out. More often than not, the enemy is within. The Gartner Group forecasts that in the near future 90 percent of all security breaches will originate inside companies.

And even though employees are not stealing secrets, they may be compromising security by flouting IT operating procedures. In one survey, the Gartner Group found that 56 percent of companies had suffered an abuse of computer access controls, and that 78 percent had employees installing or using unauthorized software.

All such activity occurs in what we call the "soft middle," the sections of the enterprise between the firewalls. Particularly vulnerable in this area "inside the perimeter" are servers, switches, routers, and workstations. Common vulnerabilities include:

- Default configurations that are left unchanged
- Default passwords that are left unchanged
- Configuration of unnecessary services
- Latest security patches are not installed

Today more than ever security audits are a fact of life for IT departments. The better we understand what they are and how to prepare for them proactively, the easier they will become.

IT Security Audit Overview

IT Security audits are frequently perceived with fear and intimidation. Often, it is the culmination of accountability for a year's worth of effort under a magnifying glass, or, an unending series of "spot checks" during the year.

Preparation for security audits includes significant effort, updating systems, checking consistency, and ensuring that all the facts are presented accurately. In place of fear and intimidation, this effort could be embraced with a much more positive attitude. Regular internal audits should be performed to meet specific objectives and used to assist with enterprise security strategy, assessment, and administration.

The work of the auditor is intended to benefit the company as a whole, from shareholders to customers. The effort can provide peace of mind – once it's complete. Increasingly, it is becoming a requirement. Sarbanes-Oxley mandates infrastructure security controls as it relates to a company's financial reporting. The HIPAA guidelines, the Gramm-Leach-Bliley Act, the FDIC, FDA, FTC, and the Federal CIO Council's efforts are just a few more examples... all intending to enforce privacy and accountability requirements that ultimately result in solid IT data integrity. Interestingly, and of significance here, this legislation embraces the audit process.

Security audits can be used by IT administrators and managers to improve or verify their work, but audits can hurt if you aren't savvy about the process.

Security audits can have many facets. Auditors may do ethical hacking to test systems and networks. They may also review projects to make sure they are meeting objectives. Tools and applications being used by an enterprise may also be scrutinized. Source-code reviews of homegrown applications can also be on the agenda.

Security audits are a way of "closing loopholes" within a company's infrastructure and do not pose a threat. Most IT departments do not have the internal expertise to double-check its security, so auditors provide verification.

IT staffers should prepare for audits by becoming aware of the auditing process -- something that, in some cases, could enable them to influence the outcome, expose security issues or push a particular agenda through.

IT managers shouldn't be intimidated by auditors. In fact, most auditors like it when you challenge them, because it shows you really care about your work and processes. Auditors tend to ask for more information than they need. Asking auditors to explain why they are requesting information makes for a better audit.

Preparing for an audit

Before an audit takes place, it's worthwhile to request to see the audit charter so you know the objectives of the audit. It would also be appropriate to ask which documents

and people auditors are going to request access to. This gives you the opportunity to gather information and put things in writing.

Auditors like output. Preparing models and other kinds of data allows you to influence the process by making the auditors' jobs easier. But care has to be used so that the information truly reflects the points you are trying to get across.

Managing expectations is another way of ensuring that the audit goes well. Staff should be aware of the kinds of things auditors are looking to learn from them. And responses should be detailed and specific to the questions asked

Focus on strengths and weaknesses

Of course, showing auditors how some things are running well should be a goal. But letting auditors know about weaknesses has its advantages as well. For example, security staff could highlight certain problems that they know the company has and suggest solutions. These could end up in the auditor's final report, which is usually given a fair amount of attention and weight by management.

Also, letting auditors know what one has learned from security problems gives the eventual recommendations some weight; the recommendations may seem more legitimate if auditors know the real-world experience.

Additionally, one should be aware of how auditors will perceive weaknesses or strengths. For example, telling about how a developer took it upon himself to fix a software bug in seconds flat may seem like a good thing. But to auditors, this could show that the company doesn't have enough change or configuration management and that the developer may have too many privileges.

After the audit

Once the auditors' report comes out, there are few things an IT manager can do to influence the outcome. Things they should look for are recommendations that are too vague or too concise; auditors are not implementation specialists. So if a report casually recommends a single sign-on project that could cost \$1 million, then that should set off warning lights.

Sometimes, there is an opportunity for a manager to submit a written reaction to the audit. But this is not the place to be negative or nitpicky. Don't whine in the reaction, as it will live on long after the details of the audit are forgotten.

IT Security -- The View from the Inside, Out

Enterprise IT security is traditionally managed with a variety of tools. These include firewalls, intrusion detection systems, vulnerability scanning, and penetration testing. Regardless of the quality of perimeter protection and the frequency of external scans, systems are continually compromised. What part of the security solution is being overlooked?

Time and time again it has been shown that an oversight in operating system or application configuration is a contributing factor in the great majority of system compromises. Products such as Ecora's Enterprise Auditor simplify control through configuration management and assessment. They provide automation in discovery and consistent reporting. Preparation time is reduced and consistency improved, which can result in greater acceptance of the audit process. The process should become routine, a component of regular maintenance.

Traditional system security scanning and analysis tools have a single perspective -- assess only what is apparent from the outside. This leaves internal vulnerabilities of a complicated infrastructure completely unassessed. Full IT security audit compliance can only be accomplished with a complete examination of the internals.

There are hundreds of operating system or primary application configuration settings that have implications for security. The manual collection and documentation of the configuration can be a painstaking and time-consuming process -- often a truly Sisyphean effort.

In addition to the size of the task, information can become outdated before the assessment is published. Or worse, a critical configuration changes before a manual assessment is complete. Even the best efforts are prone to error and inconsistency.

Ecora's Enterprise Auditor offers a new perspective from which to view the problem: an inside-out look at network services, interfaces, software feature sets and revisions, and patches and hot-fixes. The resulting documentation includes an evaluation of well-known best practices with tips, notes, and references to additional information. This automation of the process offers a significant advantage in IT assessment, control, and management. It also significantly shortens audit preparation time.

The output you get is a comprehensive collection of configuration data combined with an intelligent assessment and analysis presented in easy to read, plain-English text -- perfect for any auditing process. This output includes the most obscure, yet significant parameters. Workstation-based and agentless, our technology produces immediately useful documentation in browseable HTML and printable formats. A CSV formatted set of configuration parameters is available for export. Visio diagrams of relationship contexts and topologies are provided for overview and holistic analysis.

The feature-rich and accessible documentation is an indispensable security audit deliverable. And it becomes a reference point you can turn to again and again, when you really need to know what's going on inside. Over time, an analyst's knowledge of his infrastructure increases through familiarity of review -- a valuable by-product of the overall assessment effort.

Policy Assurance

IT security audits must correlate with accountability. Enterprise-wide IT policy is an absolute prerequisite. Accountability is an infallible tool in the advancement of security. Without established policy, there is nowhere to begin, nowhere to turn, and no organized flow of ultimate responsibility. A competent IT policy becomes effective only when it is properly promoted throughout the enterprise, with traceable accountability in place at each level. Such policy ultimately defines the influence and effectiveness of audits.

Implement a program to promote IT security awareness and to provide educational material that advocates an understanding of safe computing practices. Educate on what to avoid, define unsafe computing, and demonstrate what users can do should they encounter a potential security breach and how they can avoid unsafe practices. Empower end-users through education, while promoting accountability for their actions.

Once policy becomes established, it does not mean efforts will be consistent and faithful throughout the organization. A process is required to ensure compliance with such policy. This is why it is important to test for policy adherence weekly. A regular, interval-based audit process can only be accomplished with automation.

Self-Auditing for Security

The best way to prepare for security audits is to design and run your own. A closed-loop risk-management audit process is a highly efficient method of advancing IT security and control. This involves a cyclic audit, analysis, and review. Importantly, results must withstand the scrutiny of established policy. Adjustments in system settings, as well as the established policy, should be considered, applied judiciously, and the process must then begin anew.

Cyclic audits are performed at regular intervals; new systems, software, upgrades, and vulnerabilities will appear unpredictably. Issues can be addressed as they are exposed, improving security, control, and response immensely. With a policy review process incorporated, enterprise IT policy



management gains effectiveness. Risk management becomes an established proactive practice. The audit process should become entrenched within routine maintenance. The power of scheduled assessments promises significant and consistent advancements in enterprise-wide security.

Ecora's Enterprise Auditor software provides documentation that greatly simplifies and expedites the audit process. Systems may be organized within HTML format documentation by prioritizing systems through precedence, easing location of prominent and/or sensitive systems. System function classes, by department or other methods within the organization, may then influence the order of resulting documentation trees. Documentation servers are available which allow authenticated access by end-users to relevant documentation, which permits group-based creation and management of documentation with unwavering consistency, centralized control, and supervisory oversight.

Using Enterprise Auditor's Change Management and Scheduling For Security Audits

Ecora's Enterprise Auditor provides options in scheduling and differential comparisons of configurations. Change Management, in its most elemental form, provides a quick analysis of configuration changes between two documentation sets. This exposes modifications and unintended configuration problems or changes instantly. New environments can be developed to precisely duplicate existing implementations and, conversely, proven environments can be replicated more accurately in the field with documentation and the Change Management function.

Baselines: Key to Change Management

Baseline documentation sets can be created and implemented as a standardized reference utilizing the Change Management function. Quickly discover which systems do not comply with standardization and which parameters require adjustments. With scheduling options enabled at specific intervals, comprehensive change management can occur. With a quick reference through the Change Management option, systems can be regularly monitored for parameters that deviate from acceptable values.

Security Template

The first step in implementing Change Management is to develop and use a Security Template. Such a template helps enforce best practices, reduces common vulnerabilities, defines and enforces access rules, and facilitates continuous IT auditing.

A typical security template for a server might include user access and permissions, the disabling of unnecessary defaults, the placement of the latest securities patches, and the monitoring of shared drives. A template for a router would include provisions to address the network's interactive access and the known vulnerabilities of HTTP services.

Resources for creating a Security Template can be found on several Internet sites, including:

CERT (Computer Emergency Response Team) Coordination Center:

www.cert.org

The SANS (Systems Administration, Networking, and Security) Institute:

www.sans.org/newlook/resources/

Vendor websites, including Cisco Systems:

www.cisco.com/pcgi-bin/front.x/csec/csecHome.pl

The limitation of security templates is they become static documents without the means to incorporate them into some type of automated solution that can regularly monitor an infrastructure. To manually configure, baseline, and monitor every server, router, and workstation in an enterprise would require armies of people-resources most companies do not have or cannot spare.

When incorporated into Ecora's Enterprise Auditor, security templates serve as the basis for error-proof maintenance of all the configuration settings in an enterprise.

At user-defined points in time, Enterprise Auditor can track over 100,000 changes in an infrastructure: network devices, servers, workstations, databases, and applications. An automated solution can also track configuration changes that impact security, such as access control lists, system user groups, roles and privileges, and router and switch settings.

With general security templates for specific types of IT devices fully developed, and an automated system in place to monitor the infrastructure, the pieces are in place to create a corporate "gold standard" for security and performance-the baseline report.

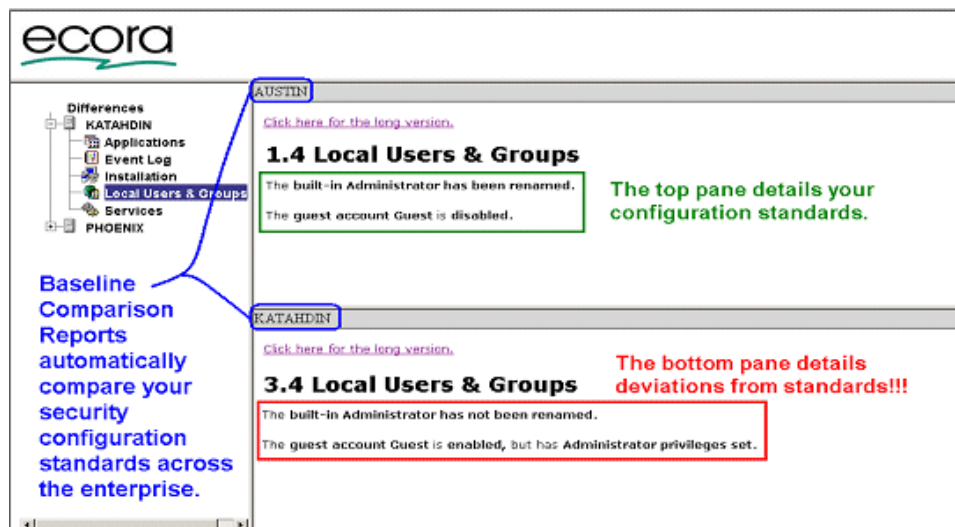
Creating a "Cycle of Control"

Once security templates are integrated into an automated solution, the final step towards total security lies in creating a "cycle of control," in which performance baselines are established, reports are run to detect instances of noncompliance, settings are reconfigured, if need be, and templates updated-all as part of a regularly scheduled security cycle.

Such a Cycle of Control has three phases:

1. Running Baseline Reports
2. Updating Configurations as needed
3. Verifying changes and updating security templates

Baselining sets and enforces standards. A baseline report is divided into two panes. Reports can be scheduled to run to compare like devices against security templates. The top pane shows a configuration standard. The bottom pane details deviations.



With baseline reports, a routine can be established for doing periodic sweeps of the IT infrastructure to verify that security holes have been plugged, that there is compliance with company policies and best practices, and that security patches have been installed.

This straightforward cycle is an efficient way to harden the soft middle of security, especially in today's environments where networks are in a constant state of change due to mergers and acquisitions, employee turnover, and the endless adding, deleting, and modifying of user accounts and permissions.

Most security breaches occur inside the firewall, in an infrastructure's "soft middle." The best way to tighten up this middle is by developing security templates for each type of network device and using documentation and baseline report features on automated solutions to create a "cycle of control" for all key security settings. This also provides fundamental auditable documentation.

For security audits, automated products such as Ecora provide continuous audits and vigilant tracking of hundreds of security related configuration settings, detailed configuration reports across multiple platforms, and change reports on one IT element or groups of elements.

Summary

IT Security Audits are here to stay. They are now a staple of daily IT life. Understanding and proactively managing the security audit process is the first step in successfully passing them.

Any security assessment must include inside/out IT management. Controlling what's behind the firewall is just as important and vital as managing external threats. Baselining and configuration change management using tool such as Ecora's Enterprise Auditor provide Security Audit ready documentation that is constantly updated and relevant.

You can quickly and easily implement configuration management controls across the existing network, with baseline comparative documentation a prerequisite "occupancy permit" for the introduction of new systems. Regularly perform enterprise-wide mapping and scanning to ensure compliance with new system introduction and existing controls. Develop a program to reduce the chance that newly deployed applications will introduce unexpected vulnerabilities, and test regularly for unauthorized installations.

An effective tool for IT security audits, Ecora's Enterprise Auditor compares quite favorably with many of the traditional methods found within the IT assessment process. Personnel-based interval assessments of this nature are prohibitively expensive for nearly any IT budget.

Try Enterprise Auditor in YOUR environment for 2 weeks.

Download a FREE trial:

<http://www.ecora.com/ecora/register/default.asp>

Ecora has helped over 13,000 companies in 45 countries automate reports for disaster recovery, tracking changes, security, IT audits, and meeting compliance standards.