Security Auditing: An Eight-Step Guide

Conducting a security audit of your IT policies, procedures, and infrastructure is a critical first step in securing your enterprise. Make Fort Knox jealous - use this A to Z guide to make your IT practice ironclad.
Security Auditing: An Eight-Step Guide

Introduction .............................................................................................................................. 2

Step 1: Conducting a Risk Analysis .......................................................................................... 2

Step 2: Preparation (Time Allotment – 10%) ........................................................................... 4

Step 3: Review Policy Documents and Reports (Time Allotment – 10%) ................................. 6

Step 4: Gathering “People” Information (Time Allotment – 10%) ............................................. 7

Step 5: Testing (Time Allotment – 15%) .................................................................................... 8

Step 6: Evaluating Your Data (Time Allotment – 20%) ............................................................... 9

Step 7: Reporting Your Findings (Time Allotment – 25%) ......................................................... 10

Step 8: Post-Audit Actions (Time Allotment – 10%) ................................................................. 11

Your Security Administrator .................................................................................................... 12

Firewalls .................................................................................................................................. 13

Intrusion Detection Systems .................................................................................................... 14

Antivirus Software .................................................................................................................. 14

Access Controls ....................................................................................................................... 15

Physical Security ..................................................................................................................... 16

Auditing Tools and Services .................................................................................................... 17

Conclusion ............................................................................................................................... 18

Bibliography ............................................................................................................................. 19
Introduction

Security problems are on the rise – this is not news. What is newsworthy, however, is the exponential nature of this increase. The Computer Emergency Response Team (CERT) says there has been an annual twofold increase in the number of vulnerabilities and security incidents reported.

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Vulnerabilities Reported</th>
<th>Number of Security Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>417</td>
<td>10,000</td>
</tr>
<tr>
<td>2000</td>
<td>1,090</td>
<td>21,756</td>
</tr>
<tr>
<td>2001</td>
<td>2,437</td>
<td>52,658</td>
</tr>
</tbody>
</table>


These numbers signify quite clearly the reality of security management for all IT decision makers. The scope of, and urgency for, security management is on the increase. Knowing where your company currently stands on security practice is the first step in proactive security management, and a full security audit is the best way to achieve this goal.

A security audit is a systematic way to test for vulnerabilities or weaknesses in your IT systems, policies, and procedures. When completed, an audit will provide you with a comprehensive picture of your security status. This will help you to:

- Assess your current level of compliance or risk, and
- Compare these levels with where you need or want your security to be.

What you will likely find as the result of your audit is that the most common audit failure points are not grounded in poor technology. Most failures, in fact, can be attributed to poor compliance with practices and procedures. A recent audit of federal government agencies found that the major failing points were poor password control, end-user security practices and policies, and access controls.

This purpose of this paper is to introduce you to the primary steps involved in conducting a security audit, and to provide pointers for auditing specific areas of your security practice and infrastructure. Sections include:

1. An eight-step audit plan.
3. A summary of available security auditing tools and services.
4. A full bibliography and list of additional follow-up resources.

**Step 1: Conducting a Risk Analysis**

The purpose of a risk analysis is to help you prioritize your company’s IT assets and decide the level of “toughness” required to protect it adequately. There will always be some risk, but what is the appropriate level of risk your company is prepared to accept?

A risk analysis is not considered part of the audit – it generally occurs prior to conducting the actual audit. Conducting a risk analysis is essential because it defines the reasons for your audit and the overall scope of your auditing activities. A risk analysis will help you determine:
• What assets your security measures are trying to protect (e.g. data, systems),
• The value of the assets you are trying to protect,
• All potential threats to these assets, and
• The impact of threats, in terms of losses, should they be realized.

Understanding the relative “value” of systems and data will help you decide the level of scrutiny to apply to each audit subject. For example, two sets of data files might have the same levels of security applied, but one may pass the audit and the other not because one is more sensitive and requires tighter security than currently afforded. A risk analysis will help you set the line between security success and failure.

After your audit is complete, you will be able to return to the value parameters set out in your risk analysis and make the following decisions:

• What weaknesses exist in your systems that would allow threats to be realized against specific assets, and
• What security controls and measures can be put in place to reduce or eliminate the threat of loss in these systems or data?

The following steps will help you conduct a risk analysis:

1. Do an inventory of all IT assets and resources, and build a map of your network topology. You need to know what you have and where it is. Ideally, you should be in the practice of conducting regular inventories. See Info-Tech’s previous white paper “A Comprehensive Guide to IT Asset Management” for thorough coverage on how to conduct an inventory.

2. Create a shortlist of key data owners, department managers, and executives. Talk to them to find out which systems and data are the most critical and why. Assets that support critical business processes will likely hold the most value for the organization.

3. Assess the business impact of losing each system or key data set. Impacts could include lost revenues or loss or reputation. From this analysis, you will get an idea of the magnitude of damage should a threat become a reality. Assign a “high”, “medium”, or “low” ranking. You might want to get your finance department or other key executives to help quantify and qualify the impact of these potential losses. See Info-Tech’s “Disaster: Assess the Potential Impact” and “Disaster Preparedness: Put a Price Tag on Your Data” for more on determining asset value.

4. Classify each asset according to its sensitivity and importance based on your business impact analysis. For example, systems can be labeled as having “high”, “medium”, or “low” importance. Data types can be classified as “confidential”, “restricted”, “internal use”, or “unclassified”. This step allows you to prioritize all system and data assets.

5. Identify and itemize all of the potential threats to each asset. These could include hacker attacks, denial of service attacks, misuse by end users, power outages, viruses, and so on.
6. Next, assess the probability of these threats actually coming to bear. Here, you can also assign “high”, “medium”, and “low” rankings.

The probability of a risk occurring, combined with the magnitude of the impact on your organization, is your overall risk factor. Systems and data that are classified as “high risk” should not only have tighter security controls and protection, but should also be subjected to a more rigorous audit procedure.

**Step 2: Preparation (Time Allotment – 10%)**

Audits are systematic in nature. Therefore, they require careful planning to ensure seamless execution and comprehensive coverage. The preparation stage of the audit is where you must:

- Prioritize audit targets.
- Decide on the objectives, depth, and scope of your audit.
- Identify and verify the resources (time, people, tools, information) you will need to conduct your audit.
- Plan your audit procedure.
- Communicate your plans to others in your organization.

From your risk analysis, you should already have a fairly good idea of your audit priorities as far as systems and data are concerned. However, each asset will need to be approached from several angles. These angles include:

- The virtual security of the asset;
- The physical security of the asset; and
- Security maintenance procedures for that asset.

Given the size of a full-scale audit, you may choose to focus on one or two areas at a time. However, most systems are interrelated. Be sure to include assessment of the interconnections between these systems in your plans.

When planning your audit, follow these steps:

1. **Identify systems** to which you will need to restrict access during your tests.
2. **Pick appropriate times** for performing your audit, such as after regular business hours, to minimize disruptions to the business.
3. **Identify key personnel** – data owners, department managers, security administrators, tech support workers, and typical business users – for information gathering interviews. Get your hands on an organizational chart to help you out.
4. **Prepare a series of questions** to ask staff, end users, and other individuals who are exposed to your systems and who you have identified for interviews. See this sample questionnaire from Auerbach for example questions on Web site audits. Focus your questioning on how personnel...
interact with the system, to what they can gain access, and how they perform security procedures (if at all).

5. **Collect and review the manuals** for all security packages. They may contain helpful auditing checklists or even an audit program that you can use.

6. **Assess and acquire established automated audit and utility programs.** Conducting an audit manually can be a painstaking process, and may lead to errors. See the “Auditing Tools and Services” section in this paper for some well-known and proven auditing tools and service providers.

7. **Pick and prepare your auditing platform.**
   - The operating system you choose will affect the auditing tools you can use, and vice versa. Choose wisely.
   - Opt for a notebook computer for your auditing command center due to its portability.
   - Ensure your auditing platform runs no network services and is configured much like any other secure host, such as a firewall.

8. **Verify your audit and testing environment** to ensure that they have not been tampered with. Burn a copy of your secure platform to a CD and store it in a secure location to ensure that you have a “tamperproofed” version at hand.

9. **Develop a prioritized plan.** This plan should itemize all tests, evaluations, and inquiries you intend to make. It should also list timelines and all resources required to perform your evaluations. Attach step-by-step procedures for all tests you intend to perform. When setting timelines, leave adequate room for contingencies — you may run across unexpected elements or problems, or may have an insight into a new way to approach a specific test.

10. **Communicate your plans** to perform an audit to whoever needs to know. This would include executives, department heads, your staff, and others who you wish to interview. Explain why an audit is necessary, and specify the times and dates of any required system downtimes.

Remember that the quality of your findings is important because it will form a comparative benchmark for future audits.

If you do not have the appropriate training for conducting a security audit, or have not experienced one first hand, it may be wise to get some training through self-education or a course.

Another alternative is to outsource to a professional auditing firm. One of the benefits of opting for the latter is that you can ensure an unbiased approach. In-house staff members may have their pride (or perhaps something more sinister) to protect, or may be unable to approach the system being audited with an objective eye. See the section “Auditing Tools and Services” section for a list of auditing firms.
Step 3: Review Policy Documents and Reports (Time Allotment – 10%)

The fundamental question answered by an audit is: Are your systems and procedures in compliance with your policy? Without a clear and comprehensive policy, you can’t be entirely sure of what security problems you’re looking for. A policy provides an important baseline against which your IT systems and practices will be measured.

If you don’t have a security policy in place prior to conducting an audit, you should make some effort to build a policy that addresses the following:

- The overall security goals of your IT installation.
- The scope of security protection offered by your department.
- Ownership over various IT resources, including systems and data.
- Categorization of data according to sensitivity.
- Responsibility for the integrity of these resources.
- Requirements to access resources (passwords, permissions).
- Descriptions of all security system access rules.
- Descriptions of all security procedures, including security maintenance, password handling, violation handling, backup and recovery, and emergency and troubleshooting procedures.
- User rights and accountabilities.
- Remote access procedures.
- Account protection requirements.
- Responsibility for support and enforcement of security direction (i.e. rights and accountabilities of the security administrator).
- Consequences for non-compliance with the policy.

Having a security policy alone isn’t enough. An unclear, out-of-date, unenforceable, or meager policy is a security problem in itself and should be treated as a threat. It is also a threat if it has not been properly disseminated and explained to end users. Consider your policy an extension of your risk management practices.

Perform the following steps in regards to your policies and reports:

1. **Gather and review all existing security policies** and procedures. Key security procedures you should look at are:
   - Security maintenance, including patching and logging.
   - Password handling.
   - Access add/change/delete.
• Violation handling.
• Backup and recovery.
• Emergency and troubleshooting.

2. **Identify weakness or gaps** in your security documentation and policy, and rewrite or expand areas that do not accurately reflect your organization’s current security priorities or views, or are generally unclear. Your auditing goal will be to reconcile your systems and practices to these new policies.

3. **Gather and review all documentation on fixes** installed or performed so that you better understand the current status of your systems. This will also help identify historical high vulnerability areas for each system that may have been overlooked when itemizing threats.

4. **Gather copies of all system and data access rules, access changes, and violation files.** Note any inconsistencies and summarize trends and patterns, if any.

5. **Gather and review all prior audit reports.** Be prepared to use these as comparative baselines when analyzing your audit results and reporting on your findings.

For more help on building tight security policies definitely see NIST’s “[Internet Security Policy: A Technical Guide](#).” This is the most comprehensive resource available on the topic of top-level security policy and practice.

### Step 4: Gathering “People” Information (Time Allotment – 10%)

People, not technologies, are the number one barrier to effective enterprise security. In a recent survey conducted jointly by the FBI and Computer Security Institute, 81 percent of respondents said the most likely source of a security attack was from within a company.

Conducting both formal and informal interviews with those who have access to your systems is an often overlooked, but critical, step. Interviews will help you discover how well personnel understand and adhere to security policies and procedures, as well as uncover what access people actually have to systems beyond what is documented or “sanctioned”.

1. **Talk to your IT staff.** Find out how they actually go about handling security procedures. Next, quiz them about their understanding of documented security procedure, controls, and responsibilities. Compare what they actually do with what is documented, and itemize the gaps.

2. **Interview end users.** Start with data owners and department heads, but also talk to general end users. Find out what they can and cannot do (such as accessing certain resources). Get a take on their understanding of security practices and loopholes. Ask them to show you their copies of security policies and procedures, or have them point out where they can be found (online, in a centralized binder). This will help you determine if they’ve ever even seen them in the first place.

3. **Talk to any other workers that have access to your physical building,** such as maintenance and janitorial staff. They have access to more than you may think, including passwords (written on sticky notes), desktop
computers, and servers. They also have a good idea of the general “comings and goings” of staff, what sensitive material ends up in the garbage instead of the shredder, and the overall physical security of the building.

Conduct your interviews with caution: many interviewees may be concerned about getting themselves, or someone else, into trouble, and may not wish to fully disclose what they know. You may want to ensure them that your conversation is confidential and that their name will not be mentioned in your report. Also, reinforce the idea that your questions are addressing the security of IT systems and data, not their job performance.

**Step 5: Testing (Time Allotment – 15%)**

Running a full battery of tests on your network may be too time consuming to be practical. Prioritize the components that you’d like to test, and choose the most important areas. These could include major routers and servers, platforms, applications, data files, and interconnects.

Be very cautious in pursuing active testing of live applications using real data – you could inadvertently cause damage. Such tests could include mock denial of service attacks or exploits. If you decide to run active tests, do a full backup of the system to be tested and run your tests after hours. If you’re not completely familiar with the testing tools and cannot implement full controls, consider not doing these types of tests at all.

Here are some of the major audits you should perform. Be sure to document any observations you have as you go. For tips on auditing specific applications or areas, see the numerous “Audit Checklists” later in this paper.

1. **Review all systems logs** for patterns and suspicious use.
2. **Search for applications and programs that run as root.** Anyone gaining access to such applications can effectively take them over.
3. **Check for surplus network services.** Every network service enabled presents an exploitable doorway into your network. The fewer enabled network services, the better.
4. **Look for replacement programs,** programs disguised as legitimate ones, and programs that are not supposed to be running.
5. **Look for unexpected changes** – such as modifications, additions, and deletions – in directories and files that are normally restricted.
6. **For applications built in-house, run a full code review.** You might need the original programmer to be available for questions you may have.
   - Look for buffer overflows, backdoors, and poor coding.
   - If there is little in the way of documentation or comments, be suspicious.
   - If the programs are unnaturally large for an application of this type, also be suspicious.
7. **Scan for unauthorized hardware attached to the network,** such as modems. Users may have added insecure equipment without your knowledge, which hackers will use as backdoors to your network,
bypassing preventive measures. Do an unannounced “walkabout” to inspect equipment attached to the network. A surprise inspection leaves no opportunity for employees to hide unauthorized equipment. Using your network topology map and hardware inventory list, look for missing hardware, hardware in unexpected locations, and extra hardware.

8. Verify that all users with access permissions to IT resources are in fact active employees. Also look for user IDs that have not been used in a certain period of time. While an individual might just be on vacation, he or she could also be a terminated employee whose access is still active.

9. Review a list of highly privileged users i.e. users who are able to change or alter access settings or by-pass security checks. This list will usually consist of department heads and/or personnel in your own department. Look for any unusual names on the list. Follow up on each name and ensure the reasons for special security privileges are justified and documented. If not, their special privileges should be revoked.

10. Review all access change control procedures with reference to documented procedure.

11. Review all logging and reporting practices with reference to documented procedure.

12. Assess the interconnects between internal systems.

13. Look for unexpected routes between your internal network and external networks by examining network traffic logs. Compare these logs with those of some individual hosts and/or workstations to find mismatches or discrepancies. Problems could indicate that access to your network is being achieved via unsecured connections or gateways.

14. Check the physical security to all systems. If an unauthorized person has physical access, you have no security.

**Step 6: Evaluating Your Data (Time Allotment – 20%)**

The testing phase will have generated a lot of data and observations. Be sure you’ve left yourself enough time to adequately organize and assess your results.

1. Analyze all data collected by the automated tools you used. Look for trends and irregularities. Separate and analyze your findings by system.

2. Itemize all application backdoors and loopholes.

3. Itemize all areas where security practice does not comply with policy or procedure. A good dividing line to impose is by staff type and/or levels (i.e. separate IT staff procedures from general end user procedures).

4. Label each of your security components (systems, procedures, etc.) in two ways:
   - Indicate level of security compliance: green (compliant), yellow (minor non-compliance), red (major non-compliance).
• Indicate urgency of action required to bring non-compliant components into compliance, prioritized by risk factor: green (not urgent), yellow (moderately urgent), red (urgent).

5. **Create a prioritized list of fixes to be made.** Systems or procedures labeled red for both compliance and urgency should be at the top of the list, followed in order by problems with these rankings:

   - Urgency – red; Compliance – yellow
   - Urgency – yellow; Compliance – red
   - Urgency – yellow; Compliance – yellow
   - Urgency – green; Compliance – red
   - Urgency – green; Compliance – yellow

6. **Finally, assess the time and resources it will take** to make each required change.

The information gleaned here will then be put into a final report, which will serve as the basis for your ultimate action list and work plan.

### Step 7: Reporting Your Findings (Time Allotment – 25%)

As you may have noticed, the reporting phase has the highest time allotment. Not only do you have to assemble your findings and build a clear report, but also you need to meet with the appropriate people to review and explain your findings, decide on a course of action, and develop a work plan.

The purpose of your report is to drive business decisions to invest in securing your IT assets. Aim to create a report that is clear, jargon-free, and speaks to business objectives.

Include the following in your report:

- An executive summary stating the purpose of the audit and high priority action recommendations.
- An explanation of the scope of the audit.
- Details on any changes from the last audit (if prior audits have been conducted).
- A statement of overall compliance of current security with policies, including an overall grade of total system security.
- An explanation of what wasn’t tested and why.
- A detailed, prioritized list of recommended actions, with full justifications and costs to make each fix.

Once you’ve completed your report, book time to discuss your findings with key executives and decision makers. The outcome of this meeting should be decisions on final prioritized action items.
Step 8: Post-Audit Actions (Time Allotment – 10%)

Your audit is complete, your report is in, and the hopefully recommendations on fixes to be made have been approved by senior management. What next?

1. **First, follow up with your staff** to discuss your course of action, resources required, and appropriate due dates for all fixes and changes. This will form the basis for your work plan.

2. **Make copies of all your test data** for future reference. Store these copies securely – they qualify as sensitive information about your company’s vulnerabilities and should be kept away from prying eyes. Preferably, store encrypted copies off site as you would with any other important company data.

3. **Redraft your security policy and procedures**, if necessary, in light of your findings. Make sure they are well communicated to end users and your staff. For better results in your next audit, ensure your new policies and procedures can be monitored and enforced. For more on this subject, read Info-Tech’s article “How To Enforce IT Policies.”

4. **Assess your audit tools and procedures**. Write a debriefing report that includes answers to the following questions:

   - Did you engage in too many manual processes that could have been sped up by using automated tools?
   - What automated tools did you use and why?
   - How effective and easy to use were the tools you selected?
   - Which tools would you use again, which would you replace, and why?
   - Did you have any problems in getting affected parties to comply with your audit requirements, such as participating in interviews or disclosing information?
   - Did you allocate sufficient time and resources to performing your audit?
   - What were the major challenges of conducting your audit?
   - What were the major surprises that surfaced in conducting your audit?
   - What do you plan to audit next time that you didn’t audit this time?
   - What changes would you make to future audit procedures?

At this point, the only thing that remains is making the actual fixes. Plan to repeat your audit on at least an annual basis.
Your Security Administrator

Your security administrator performs one of the most sensitive and crucial roles in your organization. Therefore, this role must be carefully defined, managed, and monitored.

Ensure that whoever handles your security administration reports directly to you or to someone in top management. They must have the ear of key decision makers, have access to key players in other departments, and be aware of organizational priorities.

A typical security administrator’s responsibilities include:

- Developing and implementing your security implementation plans.
- Granting, implementing, and revoking user access privileges.
- Controlling changes to all authorizations and ensuring status changes are accurately reflected in the system.
- Monitoring and following up on all unauthorized access attempts.

When conducting an audit, the security administrator’s compliance with established security procedure will come under great scrutiny. The overall effectiveness of this one staff member will have the greatest overall impact on the results of your audit.

When selecting a security administrator, there are certain character traits that are essential in someone with this level of responsibility. These include:

- Expertise – they must understand your systems and the requisite security tools inside and out. Ideally, they will be very experienced with hands-on security issues.
- Responsibility – they must be prepared to maintain security systems according to set procedures and be willing to accept accountability.
- Political awareness – they must understand how others work and what is important to data owners in other departments in order to meet their needs.
- Trustworthiness and respectability – their reputation must be beyond reproach.
- Good analytical and organizational skills – problem-solving ability is essential, as is the ability to approach things systematically.
- Good interpersonal skills – security touches everyone, therefore the ability to talk with users from the CEO on down is essential.

Ideally, all security-related work should be consolidated to one individual. This may cause a change in the way your department is organized and operates, which may also not be well accepted by staff as they may lose a certain amount of the power they previously enjoyed. Consolidation of responsibility, however, is critical.
Firewalls

Of all of the security applications implemented, firewalls are not only among the most common, but one of the most time consuming to configure and maintain. They are also one of the most important tools in your security arsenal.

When conducting a firewall audit, your goal is to ensure your firewall is correctly implemented, cannot be accessed or modified by anyone inside or outside, and behaves like you expect it to behave according to your security policy.

Use the following tips to audit your firewall. Remember to document all conflicts:

1. **Check the firewall vendor site** and other online vulnerability databases to discover the known security holes of your particular firewall and related components. Note the fixes.

2. **Review how “armored” the firewall’s operating system is.** See these armorng checklists for Unix, Linux, Solaris, and NT to ensure your OS complies.

3. **Scan for open ports** (ICMP, UDP, TCP) from both the Internet and your internal network. Ideally, no ports should be open. If ports are open, disable them. If you need a port open for administration, set a rule that limits what source IPs can connect to them.

4. **Scan every network segment from every other network segment** to see what packets are getting through. This validates that the firewall is accepting only what you have allowed and is denying everything else. The fewer rules you have in your firewall rulebase, the more secure your environment. When in doubt, block it. See Spitzner's “Building Your Firewall Rulebase” for more great information. Test your rulebase in two ways:
   - Place the system from which you are performing your audit on one side of the firewall (using a laptop) and scan another system on the other side.
   - Place the auditing system in the DMZ (demilitarized zone) and attempt to penetrate the internal network. This tests whether the internal network is protected in the event that a DMZ system is compromised. Allow 30 to 60 minutes for this test.

5. **Test authentication and encryption.** Attempt to access information and resources requiring authentication (i.e. password) without authenticating. Do the same thing for encrypted information and resources. Run a sniffer during the test to ensure data that is supposed to be encrypted actually is.

6. **Review your firewall logs.** Did your firewall's logs detect all of your scans and set off all the expected alerts? What did it log and how?

Any third-party service that works with your firewall should be tested, including e-mail virus scanning or Web content filtering software.

For more information on auditing firewalls, see “Auditing Your Firewall Setup” by Lance Spitzner and “Auditing Firewalls: A Practical Guide” by Bennett Todd.
Intrusion Detection Systems

Intrusion detection systems (IDSs) inspect all inbound and outbound network traffic, looking for suspicious patterns that may indicate a break in attempt.

One of the interesting things about IDSs is that they are themselves an auditing tool. This makes them interesting audit subjects – if attacked, they may not be able to detect their attacker before being compromised because their role is to detect attacks on other systems, not themselves.

When auditing your IDS, look for the following vulnerabilities:

1. Look for incomplete IDS coverage. For example, a single IDS on your Internet connection does not protect you against internally-generated attacks. Use IDS products from multiple vendors and/or a mix of host- and network-based solutions for comprehensive coverage.

2. Scan or search your network for computers, modems, and other network elements that the IDS may not be covering, such as lost, idle, or unknown components. These are ideal points of entry into your network. A physical inventory will help you locate components not picked up by scans.

3. Check the amount of information being handled per second. It should be no more than half a gigabyte – if it’s too high, the IDS is overworked and will miss something.

4. Assess the number of false positives reported (e.g. bogus attacks, failed logins). Are they excessive? Look at what the IDS is set to report and what it is set to discard. Hackers can flood the IDS with meaningless signatures (false positives), run CPU usage to 100%, and overfill the disk.

5. Check audit log integrity. It may have been overwritten.

6. Check for Unicode enablement on Web servers and disable. Unicode, like ASCII, maps binary numbers to characters, except that it does so for 1,000s of characters across all languages. Attacks in Unicode are less likely to match signatures in the IDS database and be detected.

Antivirus Software

New viruses emerge nearly every day. Is your antivirus software keeping up? The primary vulnerability found in antivirus software is a lack of currency. This problem should be the focus of your audit.

1. Send a simulated infected e-mail through to see if it is detected and stopped. Make the fix, and resend.

2. Ensure anti-virus software is being run on all Internet, intranet, firewall, and e-mail servers.

3. Check to see if Web-based e-mail is being routed through your e-mail server. If not, it could be bypassing antivirus screening.

4. Check to see if the antivirus software on your servers and desktops is synchronized. This is essential for redundancy. Desktop antivirus solutions are often overlooked when it’s time to update.
5. Check to see if your antivirus software is current. Every antivirus installation should have the latest signature files installed. If you don’t have a live update function, get it. If you do, ensure it’s working by visiting the antivirus vendor’s Web site and confirming the version and all updates.

Viruses are one of the most common forms of security breach. Your primary curtailment methods are up-to-date antivirus software and end user education on not opening attachments. These two steps alone can stop nearly all virus attacks.

**Access Controls**

Access to all IT resources – be they data files, applications, hardware devices, or computing terminals – must be controlled by a set of access rules. A lack of well-constructed, applied, and enforced rules can lead to:

- Access to resources by unauthorized individuals.
- Limitations in access to resources by authorized individuals.
- Modification or destruction of programs and data, either intentionally or unintentionally.

Do the following to determine the rigor of your access rules definition and administration procedures.

1. **Review your access control policies and procedures.** Your policies and procedures must be clear and complete. Ensure your access level classification ratings are current and correct.

2. **Inventory all users of IT resources.** A current organizational chart of your company will help. If you don’t have a current org chart, you will need to build one that shows clear hierarchical definitions.

3. **Check to see that each individual is assigned only the level of access required** to perform his or her job. This cuts down on intentional or inadvertent viewing, deletion, or modification of files. Scope of access should correspond with hierarchical position in the organization. General end users should have the most restricted access, and your security administrator the least.

4. **Look for conflicting security rules.** Two different rules may not be applied to the same individual where one supercedes the other, or creates a conflict of interest. For example, your application programmers should not have the ability to define security access controls.

5. **Review all changes to access privileges.** Ensure that there is a clear paper trail for all access change requests. A near-zero response time to such changes must be in place to ensure that there are no security gaps.

6. **Ensure personnel changes are reflected in the system.** Promotions, re-organization, departures, and terminations are the key obstacles to controlling access. Follow up to check the status of each employee. Also run a report to discover which IDs have not been used in a certain number of days – while these individuals may just be away, they may also be terminated employees who have not been removed from the system.
7. **Review all employees who have exceptional authority to override security rules** or parameters. Make sure the purpose/need of this authority is explained and justified.

8. **List all IDs that are allowed to by-pass security checks.** This list should not include any general end users or programmers. Again, make sure the purpose/need of this authority is explained and justified.

9. **Review the access violations log** for any trends, patterns, or anomalies.

10. **Ensure that no one has used the security administrator’s ID** other than the security administrator.

11. **Check to ensure that common and “easy to guess” passwords are not being used.**

12. **Ensure passwords for security packages,** like firewalls, are being changed frequently.

13. **Ensure that only the security administrator has the authority to make changes to security parameters.**

14. **Look at any policy exceptions** made and get full justifications.

**Physical Security**

Ensuring the physical security of your key network components is paramount. If even one unauthorized person has access to your critical (or even not so critical) systems, your entire security infrastructure has been undermined.

Your server room requires particularly strong physical security. This room should not perform double duty as shared storage space or as someone’s office.

1. **Itemize all physical access points to system resources.** Some resources will need to be highly physically secured (i.e. locked) and others not based on relative sensitivity. All servers and key infrastructure components, for example, should be kept in a locked room at all times.

2. **Itemize all individuals who have physical access to your systems** and equipment, and itemize those who actually require it. Compare the two lists and note discrepancies.

3. **Find out who has key access to all secured IT spaces** (i.e. server room). Key distribution should be carefully administered – track down the control sheet if available. If a control sheet isn’t available, create one. Go to each key holder, have him or her produce their key, and ask them who may have had access to it.

4. **Ensure copies of keys for critical systems are made** and stored offsite in a secure location.

5. **Ensure that smoking and eating/drinking is prohibited** around critical systems. Post this warning and enforce it.

6. **Ensure that critical equipment cannot be seen** from windows or public doorways.
7. **Look for other factors**, such as high voltage electrical boxes or water piping, which could damage critical systems.

8. **Check all means of entrance** to your facilities for tampering or trespassing.

9. **Check locks or seals on hardware** cabinets for tampering and overall functioning.

10. **Ensure no unauthorized hardware is in the building** that can be used to bypass perimeter defenses or copy sensitive information.

11. **Look for unsecured outputs and media**, including printouts, CD-ROMs, tapes, and diskettes. These items may contain sensitive information and are subject to theft or physical compromise.

12. **Check the whereabouts of all sensitive printed reports**, logs, printouts, and other data about your systems. These should be kept locked. If they must be discarded, have them shredded – you never know who is going through your corporate trash.

13. **Confirm that all hardware assets are tagged and documented**.

14. **Ensure that any video surveillance in place is functioning appropriately**. If no video surveillance is in place, it should be installed for sensitive areas. The presence of video cameras alone may be enough of a deterrent to foul play.

If you don’t have physical security, you don’t have anything. Be vigilant – work with department heads and personnel in charge of facilities operation to ensure that physical access to corporate assets is locked down.

### Auditing Tools and Services

Automated tools are the only practical way to create appropriate baselines and measures for your audit. Use this chart to help you identify appropriate auditing tools as well as find auditing outsourcers.

<table>
<thead>
<tr>
<th>Port Scanners</th>
<th>Fyodor’s <a href="#">nmap</a></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ipswitch’s <a href="#">WS Ping ProPack</a></td>
</tr>
<tr>
<td></td>
<td>Packet Factory’s <a href="#">Firewalk</a></td>
</tr>
<tr>
<td>Password Crackers</td>
<td>@stake <a href="#">LC3</a></td>
</tr>
<tr>
<td></td>
<td><a href="#">John the Ripper</a> (Unix)</td>
</tr>
<tr>
<td></td>
<td><a href="#">LostPasswords.com</a></td>
</tr>
<tr>
<td>Vulnerability and Change Scanners</td>
<td>PGP Security’s <a href="#">CyberCop Scanner</a></td>
</tr>
<tr>
<td></td>
<td>BindView <a href="#">bv-Control</a></td>
</tr>
<tr>
<td></td>
<td><a href="#">Flawfinder</a></td>
</tr>
<tr>
<td></td>
<td><a href="#">ISS Scanner</a></td>
</tr>
<tr>
<td></td>
<td>Lumeta <a href="#">Firewall Anlyzer</a></td>
</tr>
<tr>
<td></td>
<td><a href="#">Nessus</a></td>
</tr>
</tbody>
</table>
### Conclusion

Performing a full security audit of your systems, practices, and policies is an essential first step is managing your organization’s overall security infrastructure. Without an audit, you are simply guessing as to your organization’s security weaknesses and appropriate fixes.

1. **Follow the seven-step audit plan** outlined in this paper.

### Table: Network Security Tools

<table>
<thead>
<tr>
<th>Category</th>
<th>Tools/Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packet Sniffers</strong></td>
<td>PestPatrol</td>
</tr>
<tr>
<td></td>
<td>Rain Forest Puppy’s Whisker</td>
</tr>
<tr>
<td></td>
<td>TripWire</td>
</tr>
<tr>
<td><strong>IDS Testing Tools</strong></td>
<td>Ethereal</td>
</tr>
<tr>
<td></td>
<td>Snifft (Unix/Linus)</td>
</tr>
<tr>
<td></td>
<td>tcddump</td>
</tr>
<tr>
<td><strong>Vulnerability Databases</strong></td>
<td>Herve Schauer Consultants' IDSwakeup</td>
</tr>
<tr>
<td></td>
<td>Anzen Computing's nidsbench</td>
</tr>
<tr>
<td></td>
<td>Packet Storm's IDS cracking and testing tools</td>
</tr>
<tr>
<td></td>
<td>Robert Graham's SideStep</td>
</tr>
<tr>
<td><strong>Auditing Service Providers</strong></td>
<td>E-Soft</td>
</tr>
<tr>
<td></td>
<td>IBIS, Inc.</td>
</tr>
<tr>
<td></td>
<td>VIGILANTe</td>
</tr>
<tr>
<td><strong>Auditing Firms</strong></td>
<td>auditek</td>
</tr>
<tr>
<td></td>
<td>Fred Cohen &amp; Associates</td>
</tr>
<tr>
<td></td>
<td>Galileo</td>
</tr>
<tr>
<td></td>
<td>L.E. Boritz Consultants</td>
</tr>
<tr>
<td></td>
<td>Paisley Consulting</td>
</tr>
<tr>
<td></td>
<td>Vigilinux</td>
</tr>
<tr>
<td><strong>Other Audit Tools and Sites</strong></td>
<td>The e-Security Toolkit</td>
</tr>
<tr>
<td></td>
<td>ITAudit</td>
</tr>
<tr>
<td></td>
<td>The Information Systems Audit and Control Association &amp; Foundation</td>
</tr>
<tr>
<td></td>
<td>Pedestal Software’s SecurityExpressions (WindowsNT/2000)</td>
</tr>
<tr>
<td></td>
<td>PricewaterhouseCooper’s TeamMate</td>
</tr>
<tr>
<td></td>
<td>SomarSoft’s DumpSec (Windows NT)</td>
</tr>
</tbody>
</table>
2. **Use the supplementary Audit Checklists** to help you isolate and test specific systems and areas.

3. **Perform an audit annually** to ensure you’re staying on top of your organization’s security status.

If you can’t get your executive to support your audit and take appropriate action, ask them to waive your liability, in writing, for any security breaches and damages that could result from not implementing appropriate security measures. If this doesn’t make them sit up and take notice, then at the very least you’ve protected yourself against liability.

**Bibliography**

- “Investigate unauthorized hardware attached to your organization’s network,” CERT.
- “Inspect physical resources for signs of unauthorized access,” CERT.
- “Inspect files and directories for unexpected changes,” CERT.
- “Allow only appropriate physical access to computers,” CERT.
- “Towards Survivable Intrusion Detection,” CERT.
- “Making Security Management Manageable,” ebizQ.
- “IT security outlook appears gloomy,” InfoWorld.
- “How To Conduct A Security Audit,” PC Network Auditor.

• “Auditing Your Firewall Setup,” Lance Spitzner

• “Vulnerability Assessment Guide,” Symantec.

• “Auditing Firewalls: A Practical Guide,” Bennett Todd.


• “Don’t fail your security audit,” ZDNet.

Info-Tech Articles:

• “Physically Protect Your Servers”

• “Disaster: Assess the Potential Impact”

• “Disaster Preparedness: Put a Price Tag on Your Data”

• “A Six-Step Plan for Auditing Your Firewall”

• “Conduct a Web Site Audit”

• “Using Roles to Define Access Controls”

• “Vulnerability Assessment: Keep it Objective”

• “Penetration Testing: Employ Hacker Tools”

• “How to Enforce Your IT Policies”

• “Routers: The New Favorite Target of Hackerdom”
Practical solutions for IT managers of mid-sized enterprises

Info-Tech Research Group is a professional services firm dedicated to providing premium research and objective advice to IT managers of mid-sized enterprises. Currently, we serve more than 20,000 clients worldwide.

Our purpose is to provide practical and thorough solutions that enable IT managers to bridge the gap between technology and business. Our Web publications, guides & reports, methodologies, and consulting services all help IT professionals to keep current, to effectively manage people and technology, and to achieve professional success.

Products and Services
To serve our growing client base, Info-Tech offers a broad range of products and services. Our two Web publications reach more than 20,000 clients worldwide. Info-Tech Advisor focuses on providing critical and practical information to IT professionals, allowing them to successfully tackle their daily challenges. McLean Report is geared towards the strategic use of technology. It provides a comprehensive look at the interplay between IT innovation and business strategy.

To serve the unique needs of our mid-sized market, Info-Tech offers Consulting Methodologies that we have developed and tested through our past consulting engagements. These step-by-step methodologies have been packaged into user-friendly formats to facilitate clear understanding and independent implementation.

Consulting Services are also available from Info-Tech. Rather than the traditional hourly rate pricing format, we have developed several high-value programs involving clear deliverables and fixed pricing. This ensures our clients will have clear expectations of the results to be delivered, coupled with no hourly rate surprises.

To find out more - visit www.infotech.com