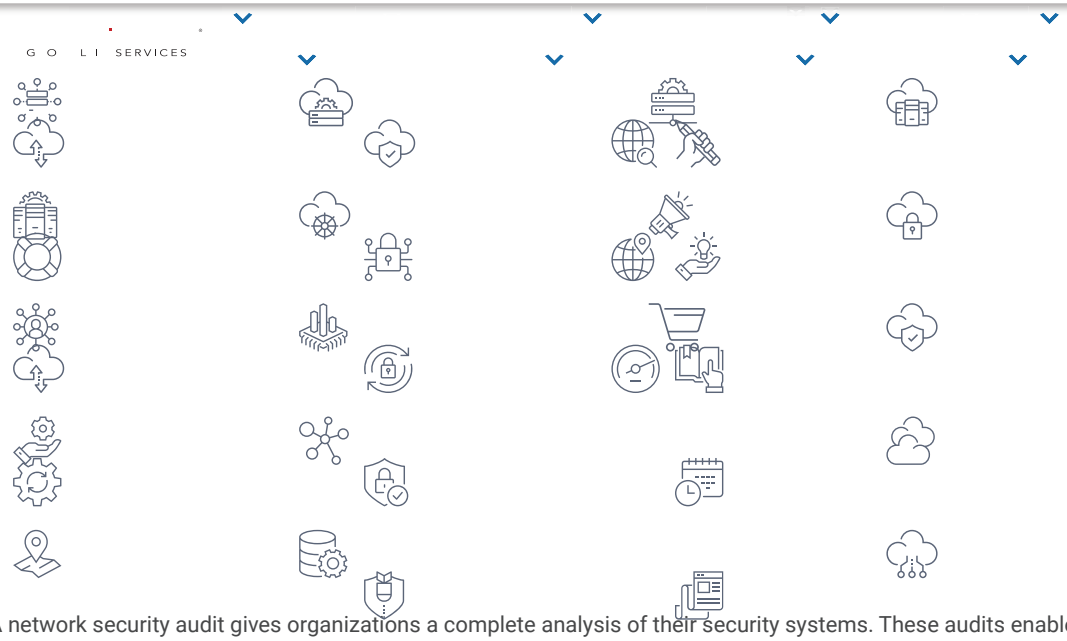


A network security audit gives organizations a complete analysis of their security systems. These audits enable companies to fix faults proactively, protect sensitive data, and design a more reliable IT security plan.

This article teaches **all you need to know about network security audits**. You will also find a network security audit checklist that will help you examine your security practices and measures.

What Is a Network Security Audit?

A network security audit is a technical evaluation of a company's network. The audit checks policies, applications, and operating systems for security faults and risks.

Network auditing is a systematic process during which an IT specialist analyzes five aspects of a network:

- Network security.
- Control implementation.
- Network availability.
- Management practices.
- Overall performance.

If the audit discovers any issues, the company fixes the problem before an attacker can exploit the weakness.

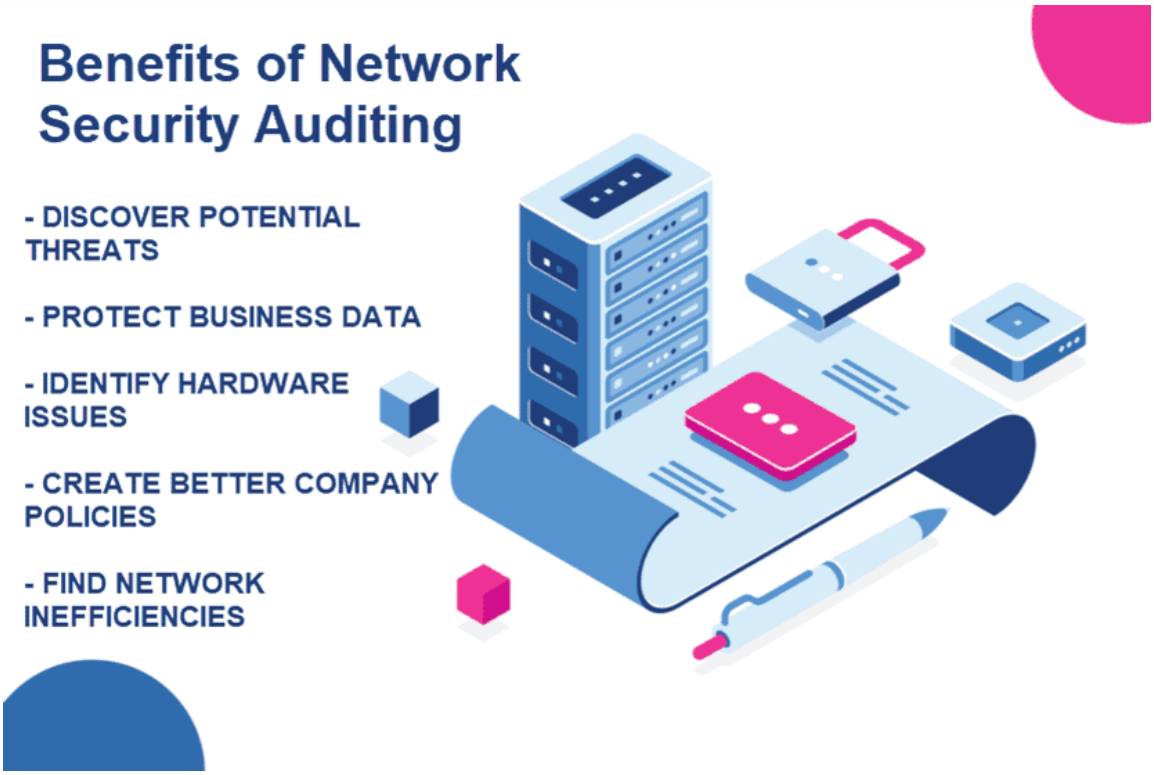
Network security audits can either be **manual** or **automated**. An automated audit typically relies on Computer-Assisted Audit Technique (CAAT) software to analyze the system.

Another common term for a network security audit is an **information security audit**.

Benefits of Network Security Auditing

Security benefits of a network security audit are:

- Identify potential threats to your system.
- Ensure the protection of valuable data.
- Locate hardware problems.
- Improve weak company policies and practices.
- Find network inefficiencies.



What Should a Network Security Audit Report Include?

A typical network security audit includes:

- An in-depth analysis of security measures.
- Risk assessment (processes, applications, and functions).
- A review of all policies and procedures.
- Examination of controls and technologies protecting assets.
- Firewall configuration review (topology, rule-base analyses, management processes and procedures).

Network security audits examine both static and activity-related data. Static data tests focus on policies, systems, and password rules. Activity-related data tests are more dynamic, and they deal with data access, transferred files, and user login activity.

Network Security Audit Checklist

Conduct an audit on an internal level or hire a third-party to assess the state of the system's security. If you opt for in-house testing, the network security audit checklist below will help you get started.

This checklist is editable, so skip the steps that are not applicable to your organization.

1. Define the Scope of the Audit

Identify all the devices on your network, as well as the operating systems they use. For most organizations, the audit needs to account for both managed and unmanaged devices:

- Managed devices are computers that belong to the organization itself.
- Unmanaged devices belong to visiting guests or are a part of BYOD (Bring Your Own Device) policies.

Once you know the endpoints, define a security perimeter. The perimeter keeps unwanted software out, so provide instructions on what classifies as dangerous software. Remember to account for all access layers: wired, wireless, and VPN connections.

2. Determine Threats

Make a list of potential threats to the security perimeter. Common cyber threats you need to account for are:

- Malware (worms, Trojan horses, spyware, and ransomware).
- Employee exposure (phishing attacks and other scams).
- Malicious inside attacks (misuse of sensitive information).
- DDoS (Distributed Denial of Service) attacks.
- Attacks on BYOD and IoT devices.
- Physical breaches.

Once you know what you are trying to prevent, it becomes easier to assess system resilience.

3. Review and Edit Internal Policies

Check internal protocols for systematic faults. Here are the essential policies a company typically has in place to protect its network:

- Acceptable use policy.
- Network security policy.
- Internet access policy.

- Encryption policy.
- Privacy policy.
- Email and communications policy.

Remove any issue you find, see if there is room for improvement, and consider adding new policies if some are missing.

4. Reevaluate Your Password Strategies

Assess your company's password strategy. Here are several ideas to strengthen your password policies:

- Ensure employees are using strong passwords.
- Use different passwords for different accounts.
- Make use of two-factor authentication.
- Make routine changes of passwords mandatory.
- Consider implementing a password manager.

5. Ensure the Safety of Sensitive Data

Identify all sensitive data in your ecosystem. That data is the prime target for attackers, so consider how you should protect that information. Here are some helpful practices:

- Limit as much access to sensitive data as possible. The smaller the access pool (both in terms of users and access methods), the easier it is to protect the data.
- Go with the concept of least privilege. Allow access to sensitive data only to individuals who require the data to perform their tasks.
- Allow read-only access where possible and only give full control to admins.
- Consider keeping sensitive data in separate storage. Such a setup allows extra security controls, such as a separate access log or password management processes.
- Do not store sensitive data on laptops.

6. Inspect the Servers

Most of your company's valuable data resides on your servers. Ensure all network configurations are set up correctly by checking the following:

- Static addr assignments.
- DNS servers.
- WINS servers.
- Binding orders.
- Services on DMZ, 00B management, or backup networks.

Make a server list that details all the servers on your network. Include names, purposes, IP addresses, service dates, service tags, rack locations or default hosts, and operating systems. This information helps locate the right server quickly in case of an emergency.

Servers must have anti-malware software and the latest patches, and they must report to the central management console. If there is an exception to those rules, add that information to the server list to avoid confusion.

7. Check the Procedure Management System

Check the management system and examine the activity logs. See whether users followed the given guidelines. If you see dangerous behavior or potential insider threats, adjust the protocols.

If the company does not have a procedure management system, consider adding one for future network security audits.

Evaluate the scope and depth of the training process. Adopt policies that prevent workers and clients from opening malicious links, using thumb-drives in company computers, and sharing passwords.

You should also ensure all staff training sessions are mandatory.

9. Ensure All Network Software Is Up to Date

Examine all the software in the network and answer the following questions:

- What software version do you have?
- When was the last update?
- What is the current software version available from the provider?

Make sure all your software is up to date. Latest patches and updates protect from the latest cyber threats. You should also ensure all anti-virus and anti-malware applications have the latest updates.

10. Safe Internet Access

Employees must have secure Internet access. Consider adding the following practices into your security policies:

- Data encryption.
- Malware scanning of all content (file downloads, streaming media, and web scripts).
- Bandwidth restrictions.
- Port blocking.

Use up-to-date technology to secure your wireless networks. If some systems are using WEP or WPA, upgrade them to WPA2. If a piece of equipment cannot support WPA2, upgrade the equipment.

11. Penetration Testing

Penetration tests are one of the main methods of finding vulnerabilities in a network. These tests assess the viability of a system and identify security gaps.

Run two types of penetration testing:

- **Static testing:** Static tools review the code while the program is not running. Static testing is comprehensive and gives a high-end overview of systems and applications.
- **Dynamic testing:** Dynamic tools test the code while the program is running. Less predictable, these tests often discover flaws hidden from static testing.

If necessary, review the current penetration testing methods and assess the process for areas of improvement.

12. Assess Backup Strategies

Every company requires a process for backing up business-critical data. Review your backup strategies and see if there are any shortcomings.

13. Reinforce Firewalls

Firewalls are a network's first line of defense that protects from all common threat types. Search for holes in the firewall and its intrusion prevention systems. Review the logs, current rules, and permissions for weaknesses, and then remove any issue you find.

When reviewing firewall security, make sure to check:

- Firewall configurations.
- Types of firewall in use.
- Management processes.
- Rule-based analysis.
- The topology of the firewall.

14. Look for Unauthorized Access Points

Your scan must be comprehensive enough to locate all potential access points. Do not limit the scan to your corporate WLAN.

Log and remove any unauthorized access point you find in the system.

15. Set Up Log Monitoring

Review the process for monitoring event logs. A smart method of minimizing mistakes is to set up a process that checks the logs regularly. Set up software that automatically takes notice of new devices, updates, security patches, and firewall installments.

You should also remove all inactive computers and user accounts from the system.

16. Share the Network Security Audit with the Team

Once you finish the report, send the audit to all relevant stakeholders. The team should then plan on how to implement the suggested upgrades.

Once you finish upgrading the network, ensure all employees know about the new changes. Make the rules and processes transparent to increase the chance of everyone following the guidelines.

17. Have Regular Network Security Audits

Network security audits are not one-time events. To keep your systems secure, turn audits into a regular part of network maintenance. Examine your network on a six-month or yearly basis to keep your assets safe from the latest cyber threats.

Be Proactive when Protecting Your Business

Unlike some other security precautions, a network audit is not expensive. These audits are a fit for any budget, especially if you conduct one on an in-house level. Start auditing networks and protect your organization from malicious activity before hackers get a chance to do any real damage.