What is a Cybersecurity Audit?

A cybersecurity audit involves a comprehensive analysis and review of the IT infrastructure of your business. It detects vulnerabilities and threats, displaying weak links, and high-risk practices. It is a primary method for examining compliance. It is designed to evaluate something (a company, system, product, etc.) against a specific standard to validate that the exact needs are met.

What is the main purpose of a Security Audit?

There are several reasons to do a security audit. They include these six goals:

- Identify security problems and gaps, as well as system weaknesses.
- Establish a security baseline that future audits can be compared.
- Comply with internal organization security policies.
- Comply with external regulatory requirements.
- Determine if security training is adequate.
- Identify unnecessary resources.

It detects vulnerabilities, risks, and threats that organizations face and the effect of such risks causing across these areas.

- Data Security – involves a review of network access control, encryption use, data security at rest, and transmissions
- Operational Security – involves a review of security policies, procedures, and controls
- Network Security – a review of network & security controls, SOC, anti-virus configurations, security monitoring capabilities, etc.
- System Security – This review covers hardening processes, patching processes, privileged account management, role-based access, etc.
- Physical Security – a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

7 Tips for Preparing for a Cybersecurity Audit

1. Create a Diagram of Your Network Assets

While part of the goal of any audit is to identify potentially unknown assets on your business network, giving your auditor a network diagram can help them save time and get a head start on their cybersecurity assessment. A network diagram is basically a chart showing the overall structure of your network—what assets are on there, how they're connected, and what protections exist between different assets.

Having this diagram helps to streamline the auditor's assessment by letting them get a basic idea of how your business network is structured so they can modify their cybersecurity framework to match.

2. Ask the Auditor Whom They Need to Connect:

Probabilities are, the auditor will need to speak to a subject matter expert or two within your organization to get a complete picture of your cybersecurity policies and architecture. So, before the audit begins, ask the auditor which of your key stakeholders they will need to talk to during their audit, and set aside some time for these stakeholders to attend a meeting.

Additionally, these experts should show up to the meeting with all of the tools they need to access your business network and show things to the auditor if asked (such as their laptop computers, tablets, or other devices).
Having the right perspectives from within your company can help smooth out the cybersecurity auditing process and save time.

3. Review Your Information Security Policy:
Every organization should have an information security policy in place to establish clear rules regarding the handling of sensitive data. It highlights security controls that are put in place to keep data secure and layout the responsibilities people within the organization have regarding the handling of that data. The information security policy should be made available to all employees so they understand their ethical and legal obligations when managing data in the course of their work.
Information security policy focuses on three key aspects of data management:

- Confidentiality: This clarifies the privacy controls surrounding data, identifying who is authorized to access information and what data may not be disclosed.
- Integrity: This aspect describes the controls for keeping data intact, complete, and accurate. It also details how the IT systems managing the data should be kept operational.
- Availability: This defines how data is to be accessed by authorized users and under what conditions.

The policy should break down all classifications of data stored in the network to determine the level of security that should be put in place to safeguard it. While some organizations may group data into any number of classifications, they generally fall under three categories.

- High-Risk Data: Any information that falls under compliance or legal restrictions, such as financial or personal health information, is considered high risk. Failing to protect this data with the appropriate security controls could carry severe fines or expose an organization to legal action.
- Confidential Data: While this data may not be protected by law, it is protected from unauthorized access or disclosure. This category is typically used for any form of proprietary data or knowledge that could cause harm to an organization should it be compromised.
- Public Data: Not all data requires the utmost security. Information that can be freely distributed throughout an organization or shared with people outside the organization is considered public.

An auditor will likely want to review your information security policy and may even quiz unsuspecting employees about cybersecurity threats. Of course, if an information security policy is implemented correctly, everyone in the organization should have detailed knowledge about their responsibilities when it comes to data. Ongoing education can help ensure that every employee is prepared to answer questions regarding threat management and data privacy.
4. Organize Your Cybersecurity Policies into a Single, Easy-to-Read Resource
While your cybersecurity audit team will probably conduct interviews with your staff to get a feel for their grasp of security, it can be helpful for them to know what your business' codified cybersecurity compliance policies are in the first place. Here, taking all of the documentation regarding your business' cybersecurity strategy and procedures and organizing them into a single resource can be massively helpful.

Some documents to consider including are:

- Password policies — password creation rules & enforcement information;
- User account restrictions in place—how users are defined in the system by role, what roles can access what systems/information, etc.;
- Details about access controls — whether or not you have dual-factor authentication, what authentication rules are in place, etc.;
- Internet use policies at work — what websites are restricted, how you monitor web use by employees, restrictions on downloading files from the internet, etc.);
- Your incident response plan (IRP) — your list of steps to take and tools to use in the event of different types of cybersecurity events; and
- Bring-your-own-device (BYOD) policies — documents detailing if/how employees can use personal devices at work.

5. Review All Applicable Compliance Standards Prior to the Audit

Most organizations have one or more compliance standards that they strive to meet, such as PCI DSS, HIPAA, GDPR, and the like. Prior to your cybersecurity compliance audit, be sure to go over the requirements of whichever standards apply to your business, and inform your cybersecurity audit and compliance team of which standards your business needs to meet.

Having this information helps your auditor adjust their assessment criteria to better meet your needs. Without this information, the auditor may either have to:

- Guess which compliance standards apply to your company; or
- Make generalized recommendations that are not based on any regulatory compliance requirements.

By educating yourself about your compliance requirements, you can put yourself in a position to work more collaboratively with your cybersecurity audit & compliance team as well as verify that the suggestions they make are sensible.

6. Try to Fix Down the Project Scope with the Auditor:

- One of the most disturbing problems companies face is being quoted one price at the start of a project and another price at the end. While some creep in the scope of a project may be inevitable because there are always unforeseen events that can disrupt things—such as a large number of unidentified assets that need to be examined, missing documentation that was previously promised, or finding a major software vulnerability that needs immediate fixing—an experienced auditor should be able to anticipate these events to some extent.
- While many of the prep tasks listed above can help avoid scope creep by giving your cybersecurity assessment team the resources they need, it is still helpful to go over the scope of the project in detail with an auditor before signing off on an agreement.
- When discussing the project scope for an audit, be sure to ask questions about why the auditor needs certain resources, or if there are any resources they need that you haven't provided yet. Get details about why specific assessment steps are necessary and what they entail.
- Additionally, if you're using a third-party cybersecurity audit service, be sure to ask around with their previous customers about whether their security assessments stayed within scope. If not, ask why the scope of the project changed.

7. Conduct an Internal Security Audit

- Once all preliminary steps have been taken to prepare for the audit, it's a good idea to conduct a self-assessment as a trial run. An internal security audit can combine a manual review of policies, processes, and controls as well as automated reviews of key infrastructure and other security systems.
- When carried out just like an external audit, an internal cybersecurity assessment not only identifies potential gaps and security risks that might have slipped your attention during the initial preparation but also gives everyone a taste of what to expect during the real thing. Even if your team has been working hard to prepare for an audit, they may not be prepared to answer difficult questions an auditor may ask on the spot. Performing a test run will help them work out their anxiety and provide a better sense of what to expect when the real auditor shows up.
- If the internal security audit reveals gaps in security controls or methods, you'll still have time to remediate them before the external audit takes place. This helps to avoid failing the audit (which would be costly in its own right), and also ensures that problem areas are fixed to reduce risk immediately.
- After the Cybersecurity Audit Starts
- When the auditor begins making their assessment of your organization's cybersecurity strategy and architecture, be sure to ask them to bring any major issues to your attention as soon as possible. This keeps these issues from being a surprise at the end of the audit and gives you a chance to start remediating these flaws sooner rather than later. Besides, there's no need to wait for the whole cybersecurity audit program to finish before starting to look for ways to fix things.

Also, be sure to take any alerts from the auditor seriously and ask for suggestions about how you can fix these issues. Many experienced auditors are familiar with numerous cybersecurity tools and quick fixes for common issues that you can implement fairly easily. However, they may want to complete their full audit before making some suggestions so they can suggest the most comprehensive solution possible.