CyberData Pros

7 Essential Tips to Prepare for a Security Audit

As the occurrence of data breaches and other security incidents continues to rise, more and more organizations today are taking their information security seriously. There are a wide variety of accreditations, certifications, frameworks, and regulations to follow and companies are increasingly choosing to (and in some cases being required to) adopt these. Either way, it's a wise decision to make because in addition to various other benefits, the requirements and guidelines established within aim to directly strengthen the security posture of your organization.

One common element included in these engagements is a security audit. Yes, even the word *audit* can be intimidating, but the good news is that the process itself doesn't have to be! The key to a smooth audit is all in the preparation - by properly preparing for a security audit, you might be surprised at just how painless it can go. Unsure where to start? Read on for our 7 Essential Tips to Prepare for a Security Audit:

1. Develop (or update) the Information Security Policy

- This might seem obvious, but in truth it's not that uncommon for this to be outdated or even missing altogether.
- Review the contents to make sure it is detailed and makes sense in the context of your organization.
- If the audit is for a specific regulation or framework, such as ISO 27001, many areas to be addressed in the policy are explicitly defined. Review these requirements, and be sure all the required policy areas are reflected as such.
- A few essential policy subjects to get you started might include: data classification and use, access control and management, acceptable use, and asset management.

2. Take inventory of all your IT assets

- Whether your company is remote, in-office, or hybrid, employees are using devices to access your systems, network, and data.
- Maintaining a current asset inventory is vital for accountability and auditing purposes.
- By performing this process, it will also aid in uncovering any discrepancies such as missing or rogue devices.
- After all, you can't defend what you don't know exists!

3. Employ a consultant or subject matter expert

- Unless you already have an in-house CISO or similar to take on this responsibility, there will be a steep burden to place on staff who likely aren’t experienced with undergoing a security audit.
- Security audits are lengthy and technical engagements, and having an expert to liaise with the auditor is a major advantage.
- Having assisted various other clients across multiple industries, an external consultant will also provide valuable guidance and insight to help you prepare for, and subsequently pass, your audit.
- Last but not least, they can save you hours upon hours of costly time (and frustration!), allowing you to take less time away from your day-to-day responsibilities.

4. Identify and classify sensitive data

- Similar to inventorying assets as mentioned above, you should also evaluate the types of data you’re holding on to and accessing. Marketing materials and business contracts should **not** be handled and stored the same way!
- Make certain that Personally Identifiable Information (PII) and other confidential information has the appropriate security measures in place.
- Doing this not only helps you succeed with the audit, but also greatly reduces the impact and likelihood of a data breach, fines, and lawsuits!

5. Ensure proper access control

- Every role within the organization is important, but not all roles are equal. The access that is granted to each user should be reflective of their job duties and responsibilities.
- Follow the principle of least privilege, which states that any user or entity should have only the minimum access that is necessary to fulfill their specific duties.
- Once this is determined, be sure there are sufficient methods and procedures in place to actually enforce this on a technical level.

6. Make sure everyone is prepared

- Having great policies and documentation is important, but that alone doesn’t equate to having a strong security posture or passing an audit.
- Equally (if not more so) important is making sure that employees are aware of and following the policies.
- There’s a high chance the auditor will want to interview other employees about the organization’s security processes. The last thing you want to do is supply the auditor with a fancy policy that looks good on paper but nobody in the company is aware of!
- Foster security awareness and engagement as a part of the company culture - that way everyone will be prepared for the audit and beyond.

7. **Conduct an unofficial self-assessment to gauge your baseline**
    - While it likely won’t be as in-depth as the real audit, getting an initial measurement of where you stand will reduce surprises.
    - By finding issues proactively, you give yourself that much more time to prepare and remediate them.
    - As an added benefit, this process provides valuable experience and awareness to your team.

This list is not exhaustive, and obviously all the details of preparing for and undergoing a security audit can’t be condensed into a few bullet points. However, by following these crucial tips, your business will be well on its way to success.

Whatever the circumstances may be, CyberData Pros is here to help. For all the expert assistance you need to be prepared for a successful security audit, reach out to us today at 404-919-0859 or info@cyberdatapros.com.