# Control Auditing Process

# Tyler Lown

# Oregon Institute of Technology

4/18/2021

# **Introduction:**

While there is no silver bullet for cybersecurity, auditing computer systems can be a vital task to minimize the risk for businesses with online exposure. Having a thorough auditing plan is vital, but the types of cybersecurity audits can vary depending on the client. Businesses in the same industry can have different goals and standards for IT infrastructure. As a note, IT infrastructure is a generic term that includes the software and hardware supporting the business’s workflow. With that in mind, this document will discuss the process involved when preparing, conducting, and then responding to a control audit of an existing IT infrastructure.

**Background:**

A cybersecurity audit involves a range of tasks, objects, and datasets to ensure that a certain level of network security is consistently achieved. Before planning an audit can begin, the auditor must have a thorough understanding of existing design as well as the stakeholder security goals. As mentioned previously, security practices can vary depending on the client, but the intent of maintaining a level of security and control over the network is often the same. This document will focus purely on logical access control management, however full computer network audit can extend far beyond just devices and users. A breakdown of the overall audit process can be seen in figure 1 below.

Figure . Full Security Audit Overview.

# **Audit Planning**

Auditing the controls of an IT infrastructure includes considering the environmental, user, and resource controls. The auditor must first meet with the stakeholders to develop a thorough understanding of the network and outline a precise scope of the audit. The auditor must also take the business security standards into account. For example, ideally, passwords should meet a high level of security, however, the complexity can be counterproductive when users are constantly locked out of an account. Each of the factors considered in the audit will be explained in more detail below.

## Environmental controls

Logical environmental controls are focused on device configuration and options that maintain user device security while also facilitating workflow. Environmental controls can include options such as if the device will ask for a password or how often a password will be requiring a reset. This is an important consideration to ensure that all devices on the network are following their designated security policies and standards.

## User Controls

Logical user controls aim to ensure that the user is only able to access the devices and resources needed to perform a job duty. This is another important step when planning the audit and helps ensure users are not either unintentionally or intentionally accessing devices or device resources that could compromise the system or network. This might include a server room where only administrative accounts can log into the device.

## Resource Controls

Logical resource controls are another important part of the control auditing process and provide another level of security for important components of the clients’ network. In this client’s case, a QuickBooks server that maintains database confidential financial records. The financial records on a server used as a database will have permissions distributed in three ways; Read-only where the user can only view the data, write which allows the user to read and make edits to the data, and finally no access to the database at all.

# **Data Gathering, Analysis, & Reporting**

With those three controls in mind, the auditing process is relatively easy to imagine. The technical side will revolve around the auditor accessing a network device, preferably the managing server called the domain controller, to perform a series of tests and computer commands to gain the data needed for security grading. The tool involved with receiving device and user reports is Microsoft’s PowerShell application framework. With this tool, reports can easily be generated about users’ access, file access, device configurations, and other standards of the audit.

After the audit is complete the obvious next step is to report back about the findings and results. If there are grounds for remediation, then the report should focus on how the business can implement the correct changes to improve security. At this point, stakeholders can decide to implement new control methods such as implementing Multi-factor Authentication, which is a relatively new security to require more than a password for login. Figure 2 below demonstrates the control auditing process.

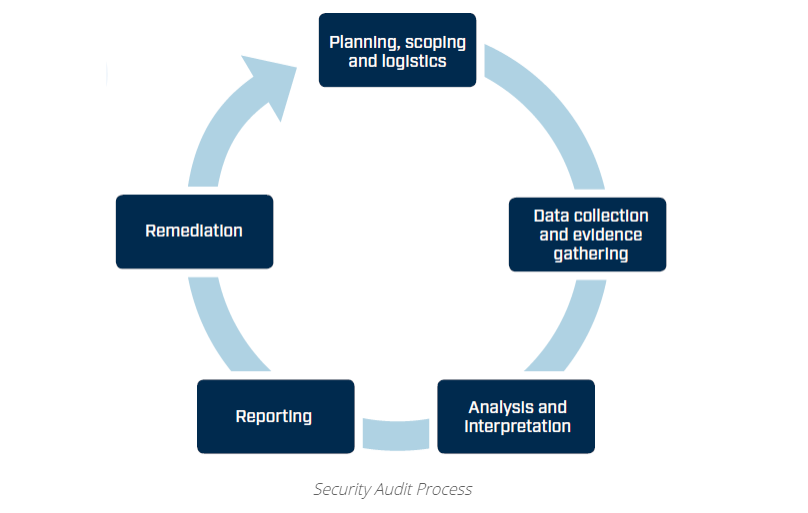


Figure . Security Auditing Life Cycle Source: Huntsman. (2020, May 29). Security audit Process. Huntsman security. https://www.huntsmansecurity.com/solutions/cyber-security-solutions/security-audit/

# **Conclusion:**

Performing a logical control audit is one of several important steps to identify potential risks and vulnerabilities. This type of cybersecurity audit focuses on logical environmental, user, and resource controls that aim to mitigate unauthorized access to various parts of the supporting IT Infrastructure. Performing the auditing process involves several tasks and tools generate data and help highlight areas of concern. A meeting to inform the stakeholders of the results is crucial after the audit because this is where decisions can be made on how and when to proceed.

References

Huntsman. (2020, May 29). Security audit Process. Huntsman security. <https://www.huntsmansecurity.com/solutions/cyber-security-solutions/security-audit/>

Simpson, B. (2012). An Introduction to Computer Auditing. <https://www.academia.edu/download/54636567/IntroductionComputerAuditing.pdf>