2-2 Journal: Systems Thinking in IT Audits

Joshua Merren

Southern New Hampshire University

CYB-400-13637-M01 Security Assessment & Auditing

Professor Jillian Seabrook

5 November 2024

Understanding the laws and standards that affect a company is a significant part of any IT audit. For example, if a company processes payments online, it must follow laws like the Payment Card Industry Data Security Standard (PCI DSS). By reviewing these requirements, a company makes sure it is doing everything the law says it should, preventing it from facing fines or lawsuits. This process involves checking that all systems securely handle credit card information, such as encrypting data when sent over the Internet. Reviewing these laws helps the audit team know what parts of the company's technology need the most attention to stay legal. It also trains staff to follow practices that keep data safe. Therefore, this step is crucial for aligning the company's operations with legal expectations and maintaining a good reputation among customers and business partners.

Deciding what the audit should focus on is critical to using time and resources wisely. For instance, if a company just set up a new email system, the audit might focus on ensuring this new system is secure and does not leak confidential information. You should scan all emails for viruses and encrypt sensitive information. Anything not directly related to the new email system, like checking old databases that have stayed the same, might be out of scope for this audit. This ensures the audit doesn’t spend time on areas less likely to cause problems. Defining the scope helps auditors concentrate on the parts of the company where a security breach or compliance failure could cause the most damage. It also ensures that the audit results remain relevant and improve company practices and security measures effectively.

Setting the main goals and standards means deciding what the audit must check. For example, a hospital using digital records must keep all patient information private, following the Health Insurance Portability and Accountability Act (HIPAA). This would include testing how the hospital’s digital systems store and share patient data to ensure everything is secure and

accessible to authorized personnel. Knowing these critical requirements helps focus the audit on what matters most to keeping the hospital compliant and secure. It also guides the audit in checking whether the hospital meets specific security benchmarks, which can influence future decisions on IT investments and changes. Identifying these needs makes the audit a powerful tool for highlighting areas where the hospital could improve handling sensitive information, ensuring better patient protection and compliance with the law.