Joshua Farias

Professor Cooper

SEC 605

25th February 2024

Planning an IT Audit

Summary

As a publicly traded financial investment firm, Cooper & Kumar is subject to a myriad of regulations that require regular auditing to ensure the necessary compliance standards are met. Audits play an essential role in ensuring that compliance and security standards are met. This report presents an outline regarding an IT audit plan with a focus on the requirements outlined by the Gramm-Leach-Bliley Act (GLBA) among other laws and regulations pertaining to Cooper & Kumar.

Scope of the Audit

The audit will cover all aspects of Cooper & Kumar's IT environment, including but not limited to:

- IT infrastructure and networks across all 25 sites.
- Policies and procedures related to information security, data protection, and risk management.
- Practices concerning the collection, processing, storage, and transmission of customer information.
- The management of third-party vendors and business associates who have access to C&K's IT systems or sensitive data.

Goals/Objectives of Audit

The primary objectives of this IT audit are to:

- **Ensure Regulatory Compliance:** Confirm that all IT systems and practices comply with the GLBA and other relevant financial regulations.
- **Identify and Mitigate Risks:** Perform a detailed risk assessment to identify vulnerabilities and suggest measures to mitigate these risks.
- **Strengthen Information Security:** Evaluate the effectiveness of current information security controls and recommend enhancements.
- **Protect Customer Data:** Ensure strong security mechanisms are in place for proper handling of customer data in accordance with legal and regulatory standards.

Audit Frequency

To align with best practices and the dynamic nature of IT risks, the following audit frequencies are proposed:

- **Annual Comprehensive Audit:** To perform a thorough examination of all IT systems, policies, and procedures.
- **Interim Reviews:** To be scheduled as necessary, particularly after major IT system updates, policy changes, or any significant security incidents.

IT Audit Checklist

To facilitate a thorough and efficient audit process, Cooper & Kumar will be requested to provide the following documentation and resources:

- **IT Policies and Procedures Manual:** Detailing C&K's information security, data protection, and risk management guidelines.
- **Network Infrastructure Diagrams:** To understand the layout and connections of the IT network.
- I**nventory of IT Assets:** Listing all hardware and software assets in use.
- **Data Flow Diagrams:** Mapping the movement of sensitive information within and outside of C&K.
- **Risk Assessment Reports:** Recent threat, vulnerability, and risk analyses.
- **Security Control Logs:** Access logs, audit logs, and monitoring reports.
- **Compliance Documentation:** Past compliance efforts, audits, and remediation activities.
- **Third-Party Management Policies:** Documents related to vendor management, especially those handling sensitive data.
- **Employee Training Records:** Documenting security awareness and data privacy training programs.
- **Incident Response Records:** Documenting prior security incidents and C&K's response.

Citations

- Federal Trade Commission. (n.d.). Gramm-Leach-Bliley Act. Retrieved from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
- Johnson, R., Weiss, M., & Solomon, M. G. (2022). *Auditing IT Infrastructures for Compliance*. Jones & Bartlett Learning.
- National Institute of Standards and Technology. (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Special Publication 800-122). Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf