Internal Security Audit

Botium Toys

Tasks:

1. Review the IT manager's scope, goals, risk assessment
2. Perform an internal audit to complete a controls assessment and compliance checklist

After reading the IT manager's scope, goals, and risk assessment, I was able to answer the following questions:

1. What are the biggest risks to the organization?
    - The biggest risks to the organization is not adhering to the National Institution of Standards and Technology Cybersecurity Framework. This can cause the business hefty fines in the near future. This organization systems are unmanaged in addition to user credential management. There are no policies and procedures in place which need to be established in this organization to create rules and regulations for employees to follow to protect their organization and keep customer data safe.

2. Which controls are most essential to implement immediately versus in the future?
    - Administrative/Managerial Controls and Technical controls are most essential to implement immediately. These two controls work hand in hand. Administrative/Managerial controls address the lack of company policies and procedures that will essentially define how Botium Toys manage data and define employees responsibilities in protecting the organization. Due to the company experiencing high levels of success and its online presence has grown, the technical controls are also the most essential to implement. The technical controls address the organization's network security such as firewalls, IDS/IPS, encryption, and password management just to name a few.

3. Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?
    - **General Data Protection Regulation (GDPR)**
    - **Payment Card Industry Data Security Standard (PCI DSS)**
    - **System and Organizations Controls (SOC type 1, SOC type 2)**

4. **What were the audit scope and goals?**

Audit Scope

- Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
- Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
- Ensure current technology is accounted for. Both hardware and system access.

Audit Goals

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

5. **What were the *critical findings* of the audit that need to be addressed immediately (i.e., What controls and/or policies need to be implemented immediately)?**

- Most of the administrative controls, technical controls, and physical controls need to be implemented immediately. (Please see Control Categories list for high priority implementation). The policies that need to be implemented are password policies and access control policies

6. **What were the *findings* (i.e., What controls and/or policies that need to be addressed in the future)?**

- (Please see Control Categories list for medium/low priority and policy implementation)

7. **How can you summarize your recommendations clearly and concisely to stakeholders?**
    - By explaining the biggest risks to the company and showing the company assets that need to be assessed and implemented based on high, medium, and low priority levels. This will give stakeholders an idea of what has to be addressed immediately in order to protect the organization and keep data safe and secured.