Activity: Conduct Security Audits 1 and 2

Part 1: Audit Scope, Goals, Risk Assessment, and Compliance Checklist

Summary: Perform an audit of Botium Toys' cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit team provides mitigation recommendations for vulnerabilities classified as 'high risk' and presents an overall strategy for improving the organization's security posture. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

Scope: Botium Toys' internal IT audit will assess the following:

- Current user permissions set in the following systems: accounting, endpoint detection, firewalls, intrusion detection system, and SIEM tools.
- Current implemented controls in the following systems: accounting, endpoint detection, firewalls, intrusion detection system, and SIEM tools.
- Current procedures and protocols set for the following systems: accounting, endpoint detection, firewall, intrusion detection system, and SIEM tools.
- Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
- Ensure current technology is accounted for, including both hardware and system access.

Goals: The goals for Botium Toys' internal IT audit are:

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

Risk Assessment:

Current Assets: Assets managed by the IT Department include:

- On-premises equipment for in-office business needs.
- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Management of systems, software, and services: accounting, telecommunication, database, security, e-commerce, and inventory management.
- Internet access.
- Internal network.
- Vendor access management.

- Data center hosting services.
- Data retention and storage.
- Badge readers.
- Legacy system maintenance: end-of-life systems that require human monitoring.

Risk Description: Currently, there is inadequate management of assets. Additionally, Botium Toys does not have the proper controls in place and may not be compliant with U.S. and international regulations and standards.

Control Best Practices: The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to managing assets. Additionally, they will need to determine the impact of the loss of existing assets, including systems, on business continuity.

Risk Score: On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to necessary compliance regulations and standards.

Additional Comments: The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be lost. The likelihood of a lost asset or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not adhering to required regulations and standards related to keeping customer data private.

Compliance Checklist: This audit included a compliance checklist covering key regulatory standards to which Botium Toys must adhere based on its business model and operations.

Applicable Compliance Standards:

- **General Data Protection Regulation (GDPR):** Botium Toys must adhere to GDPR because they conduct business and collect personal information from people worldwide, including the EU. Key provisions include data breach notifications within 72 hours, ensuring data protection, and honoring data access and rectification rights.
- **Payment Card Industry Data Security Standard (PCI DSS):** Botium Toys must comply with PCI DSS because it stores, accepts, processes, and transmits credit card information in person and online. Key provisions include securing transaction data and regular compliance reviews.
- **System and Organizations Controls (SOC Type 1, SOC Type 2):** Botium Toys needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.

Part 2: Audit Findings, Recommendations, and Stakeholder Memorandum

Activity Overview

In part two of this activity, you will communicate the results and recommendations of your security audit to stakeholders. This involves preparing a stakeholder memorandum that clearly conveys the findings and proposed actions to enhance security. Including this memorandum in your cybersecurity portfolio demonstrates your ability to communicate technical information effectively for non-technical audiences. For guidance on creating a professional portfolio, refer to the resource: "Create a cybersecurity portfolio."

To complete this activity, you will need the **controls assessment and compliance checklist** completed in part one of the security audit activity. If this has not been completed, revisit the earlier activity to ensure continuity.

Before moving forward, ensure that you answer the reflection questions provided in this activity. Once completed, you will have the opportunity to compare your work to an exemplar provided in the course materials.

Scenario

This activity is based on a fictional company:

Botium Toys: The company's IT manager has requested an internal audit of their assets, controls, and compliance with regulations and standards. After completing the audit, including a controls assessment and compliance checklist, your task is to present the findings and recommendations to the IT manager and other stakeholders. The ultimate goal is to enhance the company's security posture by implementing controls, documenting processes, and ensuring compliance to support business continuity and asset safety.

Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Al Harps
DATE: [Today's Date]
SUBJECT: Internal IT Audit Findings and Recommendations

Dear IT Manager and Stakeholders,

I am pleased to present the findings from our recent internal IT audit at Botium Toys. Below is an overview of our scope, critical findings, and recommended actions.

Audit Scope and Goals

Scope:

- Evaluated systems, including accounting, endpoint detection, firewalls, intrusion detection, and SIEM tools.
- Reviewed user permissions and implemented controls and existing procedures.
- Assessed compliance with PCI DSS and GDPR standards.
- Documented hardware and system access inventory.

Goals:

- Identify and mitigate gaps in security controls to reduce risks.
- Ensure compliance with PCI DSS and GDPR to protect sensitive data.
- Enhance disaster recovery and business continuity planning.
- Strengthen the overall security posture of Botium Toys.

Critical Findings (Immediate Action Required)

Develop and Implement Controls for:

- **Least Privilege and Separation of Duties:** Apply stricter access controls to reduce potential security risks.
- **Disaster Recovery Plans:** Establish and formalize disaster recovery procedures.
- **Password and Access Management:** Strengthen access management through updated password policies.
- **Encryption for Secure Transactions:** Ensure that all sensitive transactions are encrypted to safeguard customer data.
- **IDS, Backups, and AV Software:** Integrate intrusion detection systems (IDS), regular backups, and updated antivirus software.
- **Physical Security:** Secure physical assets with CCTV, locks, and fire prevention measures.

Compliance and Alignment:

- Address outstanding PCI DSS and GDPR compliance needs.
- Enhance policies and practices in line with SOC1 and SOC2 standards.

Additional Recommendations (Address Over Time)

Physical Security Enhancements:

- Install time-controlled safes for high-value items.
- Ensure adequate lighting and secure storage with locking cabinets.
- Use alarm service signage to deter unauthorized access.

Summary of Recommendations

- Prioritize PCI DSS and GDPR compliance.
- Leverage SOC1 and SOC2 guidelines for access management and data protection.
- Establish robust disaster recovery plans and backup systems.
- Integrate IDS and AV software across all systems.
- Secure physical assets with enhanced security measures such as CCTV and lockable storage.
- Gradually strengthen encryption and safety protocols to align with industry standards.

Conclusion

Thank you for your attention to these critical matters. By working together, we can strengthen Botium Toys' security posture and ensure a secure, compliant environment for both our operations and customers.

Best regards,
Al Harps