Introduction:

As part of my cybersecurity portfolio and Google's Cybersecurity Professional Certificate on Coursera, I have conducted an internal security audit assessment for Botium Toys, a fictitious toy company. The primary objective of this audit was to evaluate the cybersecurity program of Botium Toys and align it with industry standards and best practices. The audit aimed to identify and provide mitigation recommendations for high-risk vulnerabilities and develop an overall strategy to enhance the organization's security posture. The audit team documented their findings, created remediation plans, and communicated the results to stakeholders.

Scenario:

Botium Toys is a small U.S. toy company with a growing online presence, serving customers both domestically and internationally. The company's IT department is facing increasing pressure to support the expanding online market. The IT manager recognized the need for an internal IT audit to ensure business continuity, compliance, and security as the company grows. The audit was seen as an opportunity to strengthen the company's infrastructure, identify potential risks and threats to critical assets, and ensure compliance with online payment and European Union (E.U.) business regulations.

Audit Goals:

The key goals of the internal IT audit for Botium Toys were:

1. Adherence to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

2. Establishment of an improved process to ensure compliance with relevant regulations.

3. Strengthening of system controls.

4. Implementation of the concept of least permissions for user credential management.

5. Development and enforcement of policies and procedures, including playbooks.

6. Ensuring compliance with relevant standards, including GDPR, PCI DSS, and SOC1/SOC2.

Internal Security Audit Workflow:

The internal security audit comprises two distinct parts, each with its own set of steps to follow:

Part 1:

1. Analyze the audit scope, audit goals, and risk assessment.

2. Conduct the audit, thoroughly examining the organization's cybersecurity program.

3. Complete a controls assessment to identify existing security measures.

4. Select controls that need to be implemented for enhanced security.

5. Rate each selected control based on priority, indicating whether it requires immediate implementation or can be addressed in the future.

6. Create a comprehensive compliance checklist, detailing the chosen regulations and standards, and explain the reasons for adhering to them.

Part 2:

1. Review the results and deliverables completed in Part 1, specifically focusing on Step #2.

2. Make detailed notes of the findings obtained during the audit process.

3. Consider the most effective way to concisely summarize the recommendations for stakeholders.

4. Prepare a concise format and communicate the findings and recommendations to stakeholders.

# Controls 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, ecommerce, 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.

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative: reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs | X | High |
| Disaster recovery plans | Corrective: business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration | X | High |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | High |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | X | High |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | High |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Firewall | Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network | NA | NA |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | X | High |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | High |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X | High |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | High |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | High |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X | High |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Time-controlled safe | Deterrent; reduce attack surface/impact of physical threats | X | Medium/Low |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Medium/Low |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | High/Medium |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | High/Medium |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | X | Low |
| Locks | Preventative; physical and digital assets are more secure | X | High |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc. | X | Medium |

Critical Findings and Recommendations:

The audit revealed critical findings that require immediate attention:

1. Development and implementation of controls for the principle of least privilege and separation of duties.

2. Establishment of disaster recovery plans and regular backups.

3. Implementation of robust password policies and access control measures.

4. Deployment of an Intrusion Detection System (IDS) and encryption for secure website transactions and sensitive data.

5. Implementation of a password management system, antivirus software, and manual monitoring for legacy systems.

6. Enhanced physical controls through CCTV surveillance, locks, and locking cabinets.

Compliance Requirements:

To ensure data safety and compliance, Botium Toys needs to adhere to the following standards:

1. General Data Protection Regulation (GDPR): Compliance with GDPR is necessary for handling the personal data of customers in the European Union and reporting data breaches within 72 hours.

2. Payment Card Industry Data Security Standard (PCI DSS): Adherence to PCI DSS is crucial for the secure handling of credit card information, online payments, and international transactions. Non-compliance can result in severe consequences, such as monetary fines, forensic audits, payment brand restrictions, and damage to brand reputation.

3. System and Organizations Controls (SOC1/SOC2): Implementation of appropriate user access policies and data safety measures is essential to mitigate risk and comply with these standards, which evaluate the effectiveness of internal controls.

Stakeholder Memorandum:

To: IT Manager, Stakeholders

From: Chris Jabbour

Date: 06/09/2023

Subject: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please find below the findings and recommendations from the Botium Toys internal audit, covering the audit scope, goals, critical findings, and a summary of our recommendations.

Scope:

The audit focused on the following systems: accounting, endpoint detection, firewalls, intrusion detection systems, and security information and event management (SIEM) tool. Our evaluation encompassed:

1. Current user permissions

2. Current implemented controls

3. Current procedures and protocols

4. Alignment with GDPR, PCI DSS, and compliance requirements

5. Accountability for technology assets, hardware, and system access.

Goals:

1. Adherence to the NIST CSF.

2. Establishment of a robust process for compliance with industry standards.

3. Strengthening of system controls.

4. Implementation of the principle of least privilege for user credential management.

5. Development and enforcement of policies and procedures, including playbooks.

Critical Findings (Must be addressed immediately):

We recommend immediate action to address the following critical findings:

1. Implementation of controls for the principle of least privilege and separation of duties.

2. Establishment of disaster recovery plans and regular backups.

3. Robust password, access control, and account management policies.

4. Deployment of an Intrusion Detection System (IDS) and encryption for secure transactions and sensitive data.

5. Implementation of a password management system, antivirus software, and manual monitoring for legacy systems.

6. Enhanced physical controls through CCTV surveillance, locks, and locking cabinets.

Policies to be developed and implemented:

1. To comply with GDPR and PCI DSS requirements.

2. To align with SOC1 and SOC2 guidance related to user access policies and data safety.

Findings (Should be addressed, but no immediate need):

We suggest considering the following physical controls once critical findings have been addressed:

1. Time-controlled safe

2. Adequate lighting

3. Signage indicating alarm service provider for restricted areas

Summary/Recommendations:

Addressing the critical findings related to PCI and GDPR compliance is essential, given Botium Toys' acceptance of online payments and expansion into international markets, including the European Union. Utilizing SOC1 and SOC2 guidance to develop policies and procedures will help in adapting the concept of least permissions and achieving compliance.

Additionally, implementing disaster recovery plans and backups will ensure business continuity in the face of potential incidents. Integrating IDS and AV software will aid in intrusion detection and mitigation. Legacy systems requiring manual monitoring and intervention should be closely monitored.

For securing assets at the physical location, implementing locks, CCTV, and a time-controlled safe is highly recommended. Adequate lighting and signage indicating alarm service providers will further enhance the security posture.

Conclusion:

I hope this comprehensive security audit write-up proves valuable and enlightening. I am open to constructive feedback or suggestions for improvement. It has been a challenging yet rewarding experience, putting my knowledge and skills to the test.

Lessons Learned:

I have realized the importance of conciseness and precision in presenting findings in the stakeholder's memorandum. Additionally, I have improved my ability to explain how the System and Organizations Controls standard relates to various aspects of organizational security and risk assessment beyond financial compliance during the audit process.

Thank you for your attention, and I am available to address any further questions or concerns.

Best regards,

Bredell Mitchell