Internal Security Audit

Introduction

This is an internal security audit assessment conducted on Botium Toys, a small U.S. business, as part of my cybersecurity portfolio completed for the Google Cybersecurity Professional Certificate.
The audit assesses the business' security program, aligning it with industry standards and best practices. The goal is to provide mitigation recommendations for vulnerabilities found to be "high risk", and present an overarching strategy for enhancing the business' security posture. The audit documents the findings, provides remediation plans and efforts, and effectively communicates with stakeholders.

Scenario

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location. However, its online presence has grown, attracting customers in the U.S. and abroad. Its information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. She believes an internal audit can help better secure the company's infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to accepting online payments and conducting business in the European Union.

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, and completing a risk assessment. The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.

Scope and Goals

Scope: All assets including equipment, devices, internal network, and systems. In addition, current internal controls and compliance practices will be reviewed.

Goals:

- Adherence to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF): Ensure that the business aligns its security practices with the NIST CSF to establish a robust foundation for cybersecurity and improve the security posture.

- Compliance Assurance and Process Improvement: Ensure that the business is meeting all necessary compliance requirements to safeguard sensitive data and maintain regulatory standards. Further develop effective processes for the organization's systems to guarantee compliance.

- Policy and Procedure Establishment: Establish and document comprehensive policies and procedures to provide clear guidance on cybersecurity practices and incident responses.

Workflow

Part 1

1. Analyze the audit scope, goals, and risk assessment.
2. Conduct the audit to thoroughly examine the business' cybersecurity program.

- Controls Assessment
  1. Complete controls assessment to identify existing security measures.
  2. Select controls that need to be implemented for enhanced security.
  3. Rate each control on its priority, indicating whether it requires an immediate implementation or it can be addressed in the future.
- Compliance Checklist: Provide details on the selected regulations and standards, and explain the reasons for compliance.

Part 2

1. Review the results and deliverables completed in Part 1.
2. Make detailed notes on the findings during the audit process.
3. Share the findings and recommendations with the stakeholders in concise format

Controls Assessment

Existing Assets:

- On-premise equipment for in-office business needs
- Employee equipment including end-user devices (desktops, laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking station, surveillance cameras, etc.
- Management of systems, software, and services: accounting, telecommunication, database, security, e-commerce platform, 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	Need to be implemented (Y)	Priority
Least Privilege	Preventative. - Access controls related to least privilege have not been set. The business needs to implement the controls to ensure employees have the	Y	High

	minimum privilege required to perform their job functions. - This principle helps limit the potential damage caused by unauthorized access from staff and vendors.		
Password Policy	Preventative. - Current password policy is not in line with minimum complexity requirement (e.g. at least 8 characters, a combination of letters and at least one number, and include special characters) - The updated password policy should establish password strength which would improve confidentiality and integrity of data, and reduce the likelihood of account compromises via brute force	Y	High
Disaster Recovery Plan	Corrective. - Currently, there's no such plan. The company needs to develop and implement the plan to ensure business continuity in case of emergency. This should include regular scheduled backups of critical data. - It would help limit productivity impact to system components including: - computer room environment (air conditioning, power supply) - hardware (servers, equipment) - connectivity (network, wireless) - applications - data and restoration	Y	High
Separation of Duties	Preventative. - This has not been implemented. - This would prevent conflicts of interest and unauthorized access.	Y	High
Account Management Policy	Preventative. - Reduce attack surface and limit impact from dissatisfied employees/former employees.	Y	High

Technical Controls

Control Name	Control type and explanation	Need to be implemented (Y)	Priority
Manual monitoring, maintenance, intervention	Preventative/corrective. - While legacy systems are monitored, there is no regular schedule in place for these tasks, and intervention methods are unclear.	Y	High

	- For legacy systems, this is required to identify and mitigate potential threats, risks, and vulnerabilities		
Encryption	Deterrent. - Encryption is not currently in place to ensure confidentiality of customers’ payment transaction data that are accepted, processed, transmitted, and stored in the company’s internal database.	Y	High
Backup	Corrective. - This is not in place. - It’d support ongoing productivity in the case of an event, and align with the disaster recovery plan.	Y	High
Firewall	Preventative. - Need to ensure that the firewall is configured with appropriate security rules to protect the network from unauthorized access and malicious threats.	Y	High
Password management system	Corrective. - There is no centralized password management system. This would help processes related to password recovery, reset, and lock out.	Y	High
Intrusion Detection System (IDS)	Preventative. - The IT department has not installed an IDS.	Y	High
Antivirus software	Corrective. - This is installed, and it’s monitored regularly by the IT department to detect and quarantine threats	N/A	N/A

Physical Controls

Control Name	**Control type and explanation**	**Need to be implemented (Y)**	**Priority**
Badge access system	Preventative/Detective - This is in place already to prevent unauthorized personnel	N/A	N/A
Locks (e.g. office, store, warehouse, network gear)	Preventative. - The store’s physical location, which includes the main office, store front, and warehouse of products, has locks in place - This would prevent unauthorized personnel from physically accessing and modifying the infrastructure.	N/A	N/A
CCTV surveillance	Preventative/Detective.	Y	High/ Medium

	- Reduce the risk of certain events from occurring - Its records can be used for investigation following incidents		
Fire detection and prevention	Preventative/Detective. - Detect fire in physical locations to prevent damage to inventory, servers, and systems. Examples are fire alarm and sprinkler system	Y	Medium
Adequate lighting	Deterrent. - Limit dark hiding areas in order to deter threats	Y	Medium
Time-controlled safe	Deterrent. - Reduce attack surface/impact of physical threats	Y	Medium
Signs indicating alarm service provider	Deterrent. - Reduce the likelihood of potential attack	Y	Low

Compliance Checklist

General Data Protection Regulation (GDPR)

- GDPR is a European Union general data regulation that protects the processing of EU citizens' private data and their right to privacy in and out of the EU territory. When a breach or compromise of EU citizen's data occurs, the EU must be informed within 72 hours of the incident.
- As the business of Botium toys is expanding abroad to Europe, it needs to adhere to the GDPR compliance for handling financial/personal information of customers residing in the European Union.

Best Practice	**Explanation as per Scope, Goal, Risk**	**Need to be implemented (Y)**	**Priority**
The EU customer data is kept secure and private.	Currently, EU customer data is not kept secure and private.	Y	High
In the event of security breach, there is a plan to notify the EU customers and the authority within 72 hours.	The IT department needs to establish the notification procedure.	Y	High
Ensure data is properly classified and inventoried.	Currently, the data can be accessed by all employees internally.	Y	High
Enforce privacy policies, procedures, and processes to properly document and maintain data	The business does not have all the necessary controls in place, and it is not fully following the best practices related to the regulation.	Y	High

Payment Card Industry Data Security Standard (PCI DSS)

- PCI DSS is an international security standard that intends to ensure a secure environment for storing, accepting, processing, and transmitting credit card information.

- The business of Botium Toys must adhere to the PCI DSS as it accepts online payments. The business stores and processes customer credit card information at an international scale. Non-compliance can result in severe consequence, such as monetary fine (ranging from 5,000 to 100,000 USD), forensic audits, payment brand restrictions, damage to brand reputation, and possibility of lawsuits.

Best Practice	**Explanation as per Scope, Goal, Risk**	**Need to be implemented (Y)**	**Priority**
Only authorized users have access to customer's credit card transaction data.	Currently, all employees have access to the internally stored data and they could access sensitive cardholder data and customers' PII/SPII.	Y	High
Credit card data is accepted, processed, transmitted, and stored internally in a secure environment.	The lack of access control and encryption means that the business does not meet necessary requirements.	Y	High
Secure password management policy is implemented	Currently, there is no centralized password management system that enforces the minimum password strength and administers password reset, recovery, and lock out.	Y	High

System and Organization Controls (SOC1/SOC2)

- The SOC1 and SOC2 are a series of reports that focus on organization's user access policies and data safety measures at different organizational levels. They cover confidentiality, privacy, integrity, availability, security, and overall data safety.
  1. The business of Botium Toys needs to establish and maintain appropriate user access for internal and external (3rd party vendor) personnel to mitigate risk and ensure data safety.
  2. The SOC1 and SOC2 standards evaluate the effectiveness of an organization's internal controls. The SOC1 focuses on financial reporting controls. The SOC2 is concerned with information security controls including customer data safety.

Best Practice	**Explanation as per Scope, Goal, Risk**	**Need to be implemented (Y)**	**Priority**
User access policies are established.	Currently, no user access policies are established.	Y	High
Sensitive data especially PII/SPII are kept confidential and private.	PII/SPII data are not guaranteed to be confidential and private.	Y	High
Data is consistent, complete, accurate, and has been validated.	The IT department needs to review its current practices related to the data integrity.	Y	High
Data can only be accessed by authorized users.	Access control is not in place; data is available to all internal employees.	Y	High

Stakeholder Memorandum

To: IT Manager, Stakeholders

From: Kwang Yeon Lee

Date: 02/01/2025

Subject: Internal IT Audit Findings and Recommendations

Dear colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, findings, and recommendations.

Scope:

- The audit is focused on all technology assets including equipment, devices, network, and systems. The evaluation encompassed current implemented controls, procedures, and protocols as well as the business' alignment with key compliance requirements.

Goals:

- 1. Adherence to the NIST CSF
- 2. Establishment of a robust process for compliance with industry standards and regulations
- 3. Strengthening of system controls and development of policy/procedures

Critical Findings (must be addressed immediately):

- We recommend immediate action to address the following critical findings:
- 1. Implementation of robust Password Management, Access Control, and Account Management policies
- 2. Implementation of controls for the Principles of Least Privilege and Separation of Duties
- 3. Establishment of Disaster Recovery Plan and Regular Backups
- 4. Deployment of an Intrusion Detection System (IDS) and Encryption of critical data
- 5. Implementation of firewall, antivirus software, and manual monitoring of legacy systems
- 6. Strengthened physical controls through CCTV surveillance, locks, and fire detection and prevention

Policies to be developed and implemented:

- 1. Comply with GDPR and PCI DSS requirements
- 2. Align with SOC1 and SOC2 guidance related to user access policies and overall data safety/privacy

Findings (should be addressed, but not immediately):

- We suggest the following physical controls to be considered in the future once the critical findings have been addressed.
- 1. Adequate lighting
- 2. Time-controlled safe
- 3. Signs indicating alarm service provider for restricted areas

Summary / Recommendation:

- 1. We recommend immediately addressing the critical findings related to the GDPR and PCI compliance as the Botium Toys business accepts online payments and expands into international markets including the EU. Utilizing SOC1 and SOC2 guidance to develop policies and procedures would strengthen user access policies and further aid in achieving the compliance.
- 2. In addition, implementing disaster recovery plans and backups would ensure business continuity as part of data and system resilience strategies when faced with potential physical disasters, cyber-attacks, and technical issues impacting business productivity. Integrating IDS, firewall, and AV software would improve intrusion detection and mitigation of potential risks. Continuous monitoring and intervention of the existing legacy systems should also be taken into consideration.
- 3. For securing assets and monitoring for potential threats at the physical location, implementing locks and CCTV surveillance is highly recommended. Fire detection and prevention system, adequate lighting, time-controlled safe, and signs indicating alarm service provider would further enhance the security posture.