Introduction

As part of my cybersecurity portfolio and Google's Cybersecurity Professional Certificate on Coursera, within the *Play It Safe: Manage Security Risks* course, I completed a security audit assessment for Botium Toys, a fictitious toy company.

The objective of this audit was to assess Botium Toys' current cybersecurity practices and ensure alignment with industry standards and best practices. The focus was on identifying high-risk vulnerabilities and providing detailed mitigation recommendations. Additionally, the audit outlines a comprehensive strategy to enhance the company’s overall security posture.

Our audit team documented findings, proposed remediation plans, and outlined efforts for mitigating risks. We also communicated these findings and strategies effectively to stakeholders to ensure transparency and cooperation in improving Botium Toys' cybersecurity program.

**Scenario**

*This scenario is based on a fictional company:*

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy’s online presence has grown, attracting customers in the U.S. and abroad. As a result, their 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's worried about maintaining compliance and business operations as the company grows without a clear plan. 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 internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

Your task is to review the IT manager’s scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

The objectives of Botium Toys' internal IT audit are as follows:

1. **Adhere to the NIST Cybersecurity Framework (NIST CSF):** Align the company’s cybersecurity practices with the guidelines set by the NIST CSF to enhance security and resilience.
2. **Improve Compliance Processes:** Establish streamlined processes to ensure that all systems consistently meet regulatory and industry compliance standards.
3. **Strengthen System Controls:** Enhance internal system controls to minimize vulnerabilities, safeguard against cyber threats, and improve overall security posture.
4. **Implement Least Privilege Principle:** Enforce the principle of least permissions in user credential management, ensuring users have access only to the resources necessary for their specific roles.
5. **Develop Comprehensive Policies and Procedures:** Formalize policies, procedures, and incident response playbooks to standardize security operations and responses.
6. **Meet Compliance Requirements:** Ensure all activities and processes align with compliance regulations to avoid penalties and maintain operational integrity.

The internal security audit is divided into two parts, each with specific steps to follow.

**Part 1**

1. **Analyze Audit Scope, Goals, and Risk Assessment**
   * Define the scope of the audit.
   * Clarify the audit goals.
   * Conduct a risk assessment to identify potential vulnerabilities.
2. **Conduct the Audit**
   * Execute the audit according to the defined scope and objectives.
3. **Complete Controls Assessment**
   * Evaluate existing security controls.
   * Identify controls that need to be implemented or enhanced.
4. **Select and Prioritize Controls**
   * Choose the necessary controls to implement.
   * Prioritize each control based on urgency (immediate implementation vs. future consideration).
5. **Complete Compliance Checklist**
   * Ensure all compliance requirements are met.
   * Document adherence to relevant regulations and standards.
6. **Explain Compliance Necessity**
   * Provide justifications for adhering to selected compliance regulations and standards.

**Part 2**

1. **Review Results and Deliverables from Part 1, Step 2**
   * Re-examine the findings from the audit conducted.
2. **Document Findings**
   * Note all observations and identified issues.
3. **Prepare Recommendations**
   * Summarize recommendations clearly and concisely for stakeholders.
4. **Communicate Findings to Stakeholders**
   * Send the findings and recommendations in a concise format to stakeholders.

**Controls Assessment - Current Assets**

The IT Department manages the following assets:

* **On-Premises Equipment**
  + Hardware for in-office business operations.
* **Employee Equipment**
  + End-user devices: desktops, laptops, smartphones, remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* **Systems, Software, and Services Management**
  + Oversight of accounting systems, telecommunication, databases, security software, e-commerce platforms, and inventory management systems.
* **Internet Access**
  + Provision and maintenance of internet connectivity.
* **Internal Network**
  + Management of the company's internal networking infrastructure.
* **Vendor Access Management**
  + Control of third-party access to systems and data.
* **Data Center Hosting Services**
  + Management of data hosting services, whether on-premises or cloud-based.
* **Data Retention and Storage**
  + Policies and infrastructure for data storage and retention.
* **Badge Readers**
  + Systems for physical access control using badge readers.
* **Legacy System Maintenance**
  + Oversight of end-of-life systems requiring manual 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 |

In reviewing Botium Toys’ compliance obligations, I examined relevant controls, frameworks, and compliance documents. The following key standards are identified as necessary for the company to adhere to:

**General Data Protection Regulation (GDPR)**

The **GDPR** is a regulation from the European Union (EU) aimed at protecting the personal data and privacy rights of EU citizens, both inside and outside EU borders. A key requirement of GDPR is that, in the event of a data breach affecting EU citizens, those affected must be informed within 72 hours of discovery.

Since Botium Toys is expanding internationally and will handle the personal and financial data of customers in the EU, **GDPR compliance** is required. This means the company must ensure that customer data is securely processed, stored, and managed in accordance with GDPR’s strict guidelines on privacy and data protection.

**Payment Card Industry Data Security Standard (PCI DSS)**

**PCI DSS** is an international security standard that ensures organizations handling credit card data do so in a secure environment.

Botium Toys must comply with **PCI DSS** due to its acceptance of payments both online and in person, as well as its storage and processing of customer credit card information globally. Non-compliance could result in severe consequences, including monthly fines ranging from $5,000 to $100,000, the cost of forensic audits after a data breach, restrictions on payment processing, potential lawsuits, and significant damage to the company’s reputation.

Given these risks, strict adherence to **PCI DSS** standards is essential for Botium Toys to maintain secure payment systems and avoid costly penalties.

**System and Organization Controls (SOC 1, SOC 2)**

**SOC 1** and **SOC 2** are auditing standards that evaluate an organization’s internal controls, particularly around user access, risk management, and financial reporting. These reports also assess security, availability, privacy, and the integrity of data.

To ensure data security, Botium Toys must enforce strict user access policies for both internal staff and third-party vendors. Strong internal controls are vital to mitigating risk and safeguarding sensitive information.

* **SOC 1** focuses on the effectiveness of financial reporting controls, ensuring that financial data is accurate and protected against fraud.
* **SOC 2** is more concerned with information security, including the protection of customer data, and evaluates how well an organization maintains security, system availability, and data privacy.

Botium Toys must comply with both **SOC 1** and **SOC 2** to demonstrate strong internal controls over financial and data management processes.

**TO:** IT Manager, Stakeholders  
**FROM:** John Russell  
**DATE:** September 27, 2024  
**SUBJECT:** Findings and Recommendations from the Internal IT Audit

Dear Colleagues,

I am writing to present the findings and recommendations resulting from the internal audit conducted on Botium Toys' systems. The following sections outline the audit scope, goals, critical findings, and actionable recommendations aimed at enhancing the security posture of the organization.

**Audit Scope**

The internal audit encompassed the following systems:

* **Accounting Systems**
* **Endpoint Detection Systems**
* **Firewalls**
* **Intrusion Detection Systems (IDS)**
* **Security Information and Event Management (SIEM) Tools**

The evaluation focused on:

* Current user permissions
* Implemented security controls
* Existing procedures and protocols
* Alignment with GDPR, PCI DSS, and other compliance requirements
* Accurate inventory of technology and assets, including hardware and system access

**Audit Goals**

The primary objectives of the internal audit included:

* Alignment with the **NIST Cybersecurity Framework (CSF)**
* Improvement of processes to ensure compliance
* Strengthening of system controls
* Implementation of the **principle of least privilege** in user credential management
* Establishment and formalization of company policies and procedures, including playbooks

**Critical Findings (Immediate Attention Required)**

The audit revealed several critical areas necessitating immediate action to achieve the outlined goals:

1. **Control Implementation:**
   * Establishment of the **Principle of Least Privilege** and **Separation of Duties**
   * Development of comprehensive **Disaster Recovery Plans**
   * Implementation of **Password, Access Control, and Account Management** policies
   * Integration of an **Intrusion Detection System (IDS)**
   * Implementation of **Encryption** measures for secure website transactions and protection of sensitive data stored on disk drives
   * Establishment of robust **Backup Systems**
   * Deployment of a **Password Management System**
   * Installation of **Antivirus (AV) Software**
   * Manual monitoring and maintenance protocols for legacy systems
2. **Enhancements to Physical Security:**
   * Deployment of **CCTV Surveillance**
   * Installation of **locks** and **locking cabinets** to secure network equipment
   * Implementation of **Fire Detection and Prevention** systems (e.g., alarms, sprinklers)
3. **Policy Development:**  
   Policies are required to address:
   * **Compliance with PCI DSS** and **GDPR**
   * Adherence to **SOC1** and **SOC2** guidelines concerning user access controls and overall data security

**Findings (To Be Addressed in Future)**

Following the resolution of critical issues, the following physical security enhancements should be considered:

* Implementation of **Time-Controlled Safes**
* Improvement of **Lighting** in key areas
* Installation of **Signage** indicating the alarm service provider in restricted zones

**Summary & Recommendations**

**Immediate Action Required:**  
It is imperative that Botium Toys prioritizes the remediation of issues related to **PCI DSS** and **GDPR** compliance. As the company manages online payments and expands its services to international markets, including the European Union, adherence to these regulations is crucial.

The adoption of **SOC1** and **SOC2** guidelines related to user access controls should facilitate the implementation of the principle of least privilege, along with the development of necessary policies and procedures.

**Business Continuity Measures:**  
The establishment of **Disaster Recovery Plans** and robust **Backup Systems** is vital for ensuring business continuity in the event of incidents, ranging from cyberattacks to physical disasters. Additionally, fire detection and prevention systems should be implemented to safeguard against physical threats.

**Enhancing Security Infrastructure:**  
Integrating an **Intrusion Detection System (IDS)** and **Antivirus (AV) software** into existing systems will significantly enhance Botium Toys' capacity to detect and mitigate potential threats, particularly in light of legacy systems that require ongoing manual monitoring.

**Physical Asset Security:**  
To bolster the security of Botium Toys’ physical assets, the installation of **locks** and **CCTV systems** is recommended. Furthermore, the implementation of **time-controlled safes**, improved **lighting**, and appropriate **signage** will enhance the security of restricted areas.

By addressing these findings and implementing the recommended actions, Botium Toys can strengthen its overall security posture and ensure compliance with critical regulatory standards.

Sincerely,  
John Russell

Conclusion

This concludes my mock security audit write-up. I trust you found it informative and insightful. I welcome any constructive feedback or suggestions for improvement.

**Self-Evaluation**

Overall, I successfully identified the key priority controls that require immediate implementation to mitigate risks. I also articulated the necessity for Botium Toys to comply with the selected regulations and standards effectively. I truly appreciated the challenge this assignment posed, as it allowed me to apply the knowledge and skills I have gained through my studies and practical experiences.

**Lessons Learned**

One area where I faced challenges was in articulating detailed findings within the stakeholder memorandum while maintaining conciseness. I dedicated substantial time to refining this aspect, learning the importance of using lists, proofreading my work, avoiding redundancy, and filtering out unnecessary information.

Additionally, I initially struggled to clarify how the System and Organization Controls (SOC) standards relate to organizational user access policies, as well as the concepts of confidentiality, privacy, integrity, availability, security, and overall data safety. Throughout the audit process, I gained a more nuanced understanding of how these standards encompass not only financial compliance but also broader considerations related to risk management.