**Internternal audit**

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 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

## **Internal Security Audit Workflow**

The internal security audit can be broken down into two parts each with their own steps to follow.

### **Part 1**

1. Analyse the audit scope, audit goals, and risk assessment
2. Conduct the Audit
   1. Complete Controls assessment
      1. Select controls needing to be implemented.
      2. Rate each selected control on priority (i.e. needing to be implemented immediately or in the future).
   2. Complete Compliance checklist
      1. Explain why selected compliance regulations and standards need to be adhered to.

### **Part 2**

1. Review results and deliverables completed in Part 1, Step #2
   1. make note of findings
   2. consider how to summarize your recommendations clearly and concisely to stakeholders.
2. Send findings and recommendations to stakeholders in a concise format

# **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 centre 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 |

# **Compliance checklist**

To review compliance regulations and standards, read the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) document.

I found that Botium Toys will need to adhere to the following standards:

* General Data Protection Regulation (GDPR)
  + GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.
    - Botium Toys is expanding to offer services and handle the data of customers abroad, GDPR compliance is in scope for the handling of financial and personal information for customers in the European Union.
* Payment Card Industry Data Security Standard (PCI DSS)
  + PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.
    - Botium Toys must adhere to PCI DSS as it accepts payments online and person and They also store and processes customer credit card on an international scale. It's requirements and compliance need to be taken seriously based on possible consequences. The consequences of not complying with this standard is more severe in impact: Monetary fines monthly (ranging from 5,000-100,000 USD), costs of forensic audits upon a data breach, payment brand restrictions, damage to brand reputation, and possibility of lawsuit costs in the event of data breaches.
* System and Organizations Controls (SOC type 1, SOC type 2)
* The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.
  + Botium Toys needs to establish and maintain appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safe.
  + Both standards evaluate the effectiveness of a company's internal controls. While SOC1 I focused on financial reporting controls, SOC2 is concerned with information security controls, including customer data safety.

# **Stakeholder memorandum**

TO: IT Manager, Stakeholders

FROM: Giorgio Barresi  
DATE: 04/05/2024  
SUBJECT: Internal IT Audit Findings and Recommendations

Dear all,

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

**Scope:**

* The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool. The systems will be evaluated for:
  + Current user permissions
  + Current implemented controls
  + Current procedures and protocols
* Ensuring current user permissions, controls, procedures, and protocols in place align with GDPR, PCI DSS, compliance requirements
* Ensure current technology and assets are accounted for both hardware and system access.

**Goals:**

* Adhere to the 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

**Critical findings** (must be addressed immediately):

Multiple controls need to be developed and implemented to meet the audit goals, including:

* Principle of Least Privilege and Separation of duties
* Disaster recovery plans
* Password, Access control, and Account management policies
* Intrusion Detection System (IDS)
* Encryption (secure website transactions wand disk drive(s) containing sensitive information)
* Backups
* Implementation of a Password management system
* Antivirus (AV) software
* Manual monitoring, maintenance, and intervention for legacy systems
* Closed-circuit television (CCTV) surveillance
* Locks
* Locking cabinets (for network gear)
* Fire detection and prevention (fire alarm, sprinkler system, etc.)
* Policies need to be developed and implemented for the following:
  + To meet PCI DSS and GDPR compliance requirements.
  + To meet SOC1 and SOC2 guidance related to user access policies and overall data safety.

**Findings** (should be addressed, but no immediate need):

The following physical controls should be considered in the future once the critical findings have been resolved:

* Time-controlled safe
* Adequate lighting
* Signage indicating alarm service provider for restricted areas

**Summary/Recommendations:**

It is recommended that the critical findings relating to compliance with PCI and GDPR be promptly addressed as Botium Toys accepts online payments is expanding to offer services and handle the data of customers abroad including the European Union. SOC1 and SOC2 guidance related to user access policies should be used to align to the audit goal to adapt to the concept of least permissions to develop the policies and procedures needed to be compliant.

Disaster recovery plans and backups are recommended as they will support business continuity in the event of an incident occurring ranging from a physical disaster such as a fire, or worst-case scenario of a cyber-attack or technical issue impacting business productivity as a part of a data and system resilience strategy. A method of fire detection and prevention systems is worth consideration for protecting against physical attacks.

Integrating an IDS and AV software into current systems will give the ability to assist with intrusion detection and spot and mitigate potential risks while considering the existing legacy systems that need manual monitoring and intervention.

To secure assets at Botium Toys' physical location, locks and CCTV should be used to secure physical assets and to monitor for potential threats. Having a time-controlled safe, adequate lighting, and signage indicating alarm service provider will further improve Botium Toys' security posture.

A follow-up audit in 6 months is recommended.