**Botium Toys Security Audit:**

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. 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 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 (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, 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.

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

**You receive the following email from your IT manager:**

Hello!

I have completed the audit scope and goals in addition to a risk assessment. At a high level, the main goals and risks are as follows:

**Goals:**

* Improve Botium Toys’ current security posture by aligning to industry best practices (e.g., adhere to the NIST CSF, implement concept of least permissions)
* Provide mitigation recommendations (i.e., controls, policies, documentation), based on current risks
* Identify compliance regulations Botium Toys must adhere to, primarily based on *where* we conduct business and *how* we accept payments
* To review the full report, read the Botium Toys: Audit scope and goals document

**Risks:**

* Inadequate management of assets
* Proper controls are not in place
* May not be compliant with U.S. and international regulations and guidelines
* Current risk score is 8/10 (high), due to a lack of controls and adherence to compliance regulations and standards
* To review the complete list of assets and risks, read the Botium Toys: Risk assessment document

Thank you, Botium Toys IT Manager

**My reply to the IT Manager of Botium Toys**

Hello,

I hope this email find you well.

In what follows I have provided a controls assessment of the company’s network to help secure the company’s infrastructure and help identify and mitigate potential risks, threats and vulnerabilities to critical assets of the entie security program. Moreover I have also included a compliance checklist indicating the specific regulations that our company needs to adhere to according to our company’s infrastructure needs along with an explanation for the required compliance. Since strengthening our company’s security posture is top priority, the following audit is in response to that critical goal. In an effort to achieve compliance, identify weaknesses and vulnerabilities I conducted to following audit for the purpose of Identifying failures in process and procedures to correct them.

Please let me know if you have any questions or concerns.

Regards,

Controls assessment

To review control categories, types, and the purposes of each, read the [control categories](https://docs.google.com/document/d/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview) document.

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 | N/A | N/A |
| 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 | Meduim |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | x | Medim |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | x | High |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | x | High |
| 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 | High |

Compliance checklist

To review compliance regulations and standards, read the controls, frameworks, and compliance document.

**The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

**Explanation:**

**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.

**Explanation:** Since Botium toys does business worldwide including Eurpope  the security team will  need to alter how personally identifiable information (PII) is treated in order to adhere to the European Union's regulations.

**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.

**Explanation:** Since Botium toys does business online worldwide the security team will need ensure the storing, accepting, processing and transmitting of credit card information is comp;eted in a sure environment to be in compliance with this standard.

**The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients’ health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

**Explanation:**

**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.

**Explanation:** Although Botium toys is a small U.S. based business, since the company support user access online both internally and externally the security team will need to furish a report to asses the company’s complainace and level of risk to prevent fraud.

**Stakeholder memorandum**

TO: IT Manager, Stakeholders

FROM: Gibson J Garcon  
 DATE: 11/ 29/2023  
 SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

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

**Scope:** The entire security program of Botium Toys

**Goals:** To achieve compliance, identify weaknesses and vulnerabilities. Identify failures in process and procedures to correct them.

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

* Inadequate management of assets
* Proper controls are not in place
* May not be compliant with U.S. and international regulations and guidelines
* Current risk score is 8/10 (high), due to a lack of controls and adherence to compliance regulations and standards

**Non Critical Findings**

* Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities
* Signage indicating alarm service provider
* Aqequqte Lighting

**Summary/Recommendations:**

**The High proprity controls that need to be implemented ted immediately are:**

* Least Privilege
* Disaster recovery plans
* Password policies
* Access control policies
* Account management policies
* Separation of duties
* Intrusion Detection System (IDS
* Encryption
* Backups
* Antivirus (AV) software
* Manual monitoring, maintenance, and intervention
* Locks

**The Medium to Low  proprity controls that need to be implemented ted immediately are:**

* Fire detection and prevention (fire alarm, sprinkler system, etc.
* Signage indicating alarm service provider
* Locking cabinets (for network gear
* Closed-circuit television (CCTV) surveillance
* Time-controlled safe

Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Three hardening tools the organization can use to address the vulnerabilities found include:   1. Implementing multi-factor authentication (MFA) 2. Setting and enforcing strong password policies 3. Performing firewall maintenance regularly   MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords.  Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts.  Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. |
|

|  |
| --- |
| **Part 2: Explain your recommendation(s)** |
| Enforcing multi-factor authentication (MFA) will reduce the likelihood that a malicious actor can access a network through a brute force or related attack. MFA will also make it more difficult for people within the organization to share passwords. Identifying and verifying credentials is especially critical among employees with administrator level privileges on the network. MFA should be enforced regularly.  Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. The rules that are included in the password policy will need to be enforced regularly within the organization to help increase user security.  Firewall maintenance should happen regularly. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks. |