Botium Toys Internal Security Audit

**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. 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.

My 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.

**Scope**

Botium Toys Internal IT audit will assess the following:

* Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
* Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
* Ensure current technology is accounted for. Both hardware and system access.

**Goals**

* 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

**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

**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, e-commerce, 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

Below, I have marked what controls need to be implemented and how high or low of a priority they should take.

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | Medium |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | Medium |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | Medium |
| 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 | Medium |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | Medium |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | Medium |
| 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 | Low |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Low |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | Medium |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | Medium |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | X | Medium |
| Locks | Preventative; physical and digital assets are more secure | X | Medium |
| 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 | Low |

**Findings & Recommendations**

Botium Toys will need to comply and adhere to the regulations below:

**General Data Protection Regulation (GDPR)**

* GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents’ data and their right to privacy in and out of E.U. territory. For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization. Additionally, if a breach occurs and an E.U. citizen’s data is compromised, they must be informed. The affected organization has 72 hours to notify the E.U. citizen about the breach.
  + Botium Toys has a growing online presence that has now reached a global market, which includes the EU. They’re now responsible for handling the personal and financial information of EU citizens, so it’s imperative to adhere to the regulations of the GDPR to ensure the data is safe.

**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. The objective of this compliance standard is to reduce credit card fraud.
  + PCI DSS sets comprehensive security standards for handling cardholder data during transactions. Adhering to these standards helps prevent data breaches, reducing the risk of customer information being compromised. Botium Toys has frequent online transactions, making it a must to adhere to PCI DSS.

**System and Organizations Controls (SOC type 1, SOC type 2)**

* The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as Associate, Supervisor, Manager, Executive, Vendor and Others. 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.
  + It is favourable for Botium Toys to comply because SOC Type 1 and SOC Type 2 reports are important for businesses to demonstrate their commitment to data security, risk management, and the overall effectiveness of their internal controls. Adhering to SOC standards can help build trust with customers, meet regulatory requirements, improve risk management, and strengthen business relationships. Prioritizing compliance, security and integrity strengthens an organization’s posture.

Botium Toys will ***not*** need to comply and adhere to the regulations below:

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

* FERC-NERC is a regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. They are also legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined by the FERC.
  + These regulations are aimed at organizations that work with electricity or power grids and are required to report security incidents that affect the power grids. Botium Toys does not fall under these requirements.

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

* HIPAA is a U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent. It is governed by three rules: Privacy, Security and Breach Notification. Organizations that store patient data have a legal obligation to inform patients of a breach because if patients' **Protected Health Information** (PHI) is exposed, it can lead to identity theft and insurance fraud. PHI relates to the past, present, or future physical or mental health or condition of an individual, whether it’s a plan of care or payments for care. Along with understanding HIPAA as a law, security professionals also need to be familiar with the Health Information Trust Alliance (HITRUST®), which is a security framework and assurance program that helps institutions meet HIPAA compliance.
  + Botium Toys is not required to adhere to HIPAA because it’s not a business that provides any health care services. The sole purpose of the organization is to sell toys physically and online.