Botium Toys is a small but growing company with an expanding online presence, so its IT department will have to take steps to safeguard its customers' sensitive information and protect its infrastructure. This security audit will help Botium Toys secure the company’s infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. It will also help the company comply with regulations related to internal processing and accepting online payments, such as PCI DSS, and the rules like the General Data Protection Regulation (GDPR) for conducting business in the European Union (E.U.).

The assets of Botium Toys range from in-house devices to remote employee workstations, products stored in their warehouse, security and accounting software, internal network infrastructure, and end-of-life legacy systems that require human monitoring. Currently, there is inadequate management of these assets and a lack of proper implementation of critical controls to protect sensitive data in accordance with U.S. and international regulations and standards.

The company has several critical gaps in its security posture, which can hinder business processes and the safety of sensitive data. The company currently lacks controls for enforcing the least privilege and separation of duties, which increases the risk of unauthorized access and insider threats. Sensitive customer data, including credit card information, is not encrypted, leaving it vulnerable to breaches. Additionally, the absence of a disaster recovery plan and regular backups heightens the risk of data loss and prolonged downtime in the event of an incident. The organization also operates without an intrusion detection system (IDS), which is essential for identifying and responding to potential threats in real-time. Furthermore, inadequate password policies and the lack of a centralized password management system exacerbate the company's exposure to cyber risks.

Another concern is noncompliance with regulations. Botium Toys does not adequately meet several requirements listed in the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). Customer credit card data is not securely stored or encrypted, which violates the PCI DSS guidelines. In addition, GDPR data security and privacy mandates are unmet, which makes the company prone to potential fines and reputational damage. These deficiencies put the organization at risk of severe financial and legal consequences. Addressing these issues promptly is essential to improving Botium Toys’ security and compliance posture.

The company should implement least privilege access controls and develop a robust disaster recovery plan in order to improve its security posture. Restricting access to sensitive data and systems ensures that only employees with specific job-related needs can access critical resources, reducing the risk of unauthorized access. Additionally, access to critical systems should be monitored and logged to detect any suspicious activities promptly.

It is also essential to develop a comprehensive disaster recovery plan to mitigate the impact of potential incidents. This plan should include strategies for the rapid recovery of systems and data and the implementation of regular backups stored securely offsite. Together, these measures will significantly strengthen Botium Toys' ability to protect its assets and ensure business continuity.

An intrusion detection plan (IDP) should be deployed to monitor and identify suspicious activities or potential intrusions within Botium Toys' network. An IDS can provide real-time alerts, enabling the IT team to respond quickly to threats and minimize possible damage. Additionally, enhancing password policies and implementing a centralized password management system are critical to improving security. Enforcing strong password requirements, such as a minimum of 12 characters with a mix of uppercase and lowercase letters, numbers, and symbols, will reduce the risk of password-based attacks. A centralized password management system will ensure consistent enforcement of these policies, streamline password resets, and enhance overall productivity while maintaining security standards.

Encrypting sensitive data, including credit card information and personally identifiable information (PII), is essential for ensuring its security during storage and transmission. By implementing strong encryption protocols, Botium Toys can safeguard critical data from unauthorized access and mitigate the risk of breaches. This measure is especially important for maintaining compliance with industry standards and regulations, such as PCI DSS and GDPR, which mandate the protection of sensitive customer information.

Botium Toys must comply with industry standards and address gaps in several areas to maintain business continuity and company reputation. For PCI DSS compliance, the company should implement strong encryption to secure cardholder data, restrict access to credit card information to authorized personnel, and perform regular vulnerability scans and penetration tests to identify and address security gaps. In line with GDPR requirements, Botium Toys must classify and inventory all E.U. customer data to ensure it is appropriately secured and private. For SOC Type 1 and Type 2 compliance, developing and enforcing comprehensive user access policies is essential, along with conducting regular audits to guarantee data confidentiality, integrity, and availability.

By addressing these recommendations, Botium Toys will significantly enhance its security posture, ensure compliance with regulations, and mitigate risks to its assets and operations.

**Controls Assessment Checklist:**

| **Control** | **Yes** | **No** |
| --- | --- | --- |
| Least Privilege |  | X |
| Disaster recovery plans |  | X |
| Password policies |  | X |
| Separation of duties |  | X |
| Firewall | X |  |
| Intrusion detection system (IDS) |  | X |
| Backups |  | X |
| Antivirus software | X |  |
| Manual monitoring/maintenance of legacy systems | X |  |
| Encryption |  | X |
| Password management system |  | X |
| Locks (offices, storefront, warehouse) | X |  |
| CCTV surveillance | X |  |
| Fire detection/prevention systems | X |  |

**Compliance Checklist:**

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

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| Only authorized users have access to credit card information |  | X |
| Credit card information is stored, accepted, processed, and transmitted internally in a secure environment |  | X |
| Implement data encryption procedures |  | X |
| Adopt secure password management policies |  | X |

**General Data Protection Regulation (GDPR)**

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| E.U. customers’ data is kept private/secured |  | X |
| Notify E.U. customers within 72 hours of a breach | X |  |
| Ensure data is properly classified and inventoried |  | X |
| Enforce privacy policies, procedures, and processes | X |  |

**System and Organizations Controls (SOC Type 1 & 2)**

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| User access policies are established |  | X |
| Sensitive data (PII/SPII) is confidential/private |  | X |
| Data integrity ensures data is consistent, complete, accurate, and validated | X |  |
| Data is available to authorized individuals | X |  |