Botium Toys: Scope, goals, and risk assessment report

Scope: The scope of the internal audit at Botium Toys includes assessing the company's information technology infrastructure and processes related to maintaining compliance and securing the company's online market worldwide. This includes evaluating the current state of security posture, identifying potential risks, threats, or vulnerabilities to critical assets, and ensuring compliance with regulations related to processing online payments and conducting business in the European Union (E.U.). The audit will focus on areas such as securing infrastructure, protecting data, managing access, monitoring and detecting incidents, and responding to security events.

Goals: The goals of the internal audit at Botium Toys are:

1. To assess and improve the company's information technology infrastructure to better secure online operations and critical assets.

2. To identify and mitigate potential risks, threats, or vulnerabilities that may compromise the company's security posture.

3. To ensure compliance with regulations related to processing online payments and conducting business in the European Union (E.U.).

4. To provide an overview of the risks and potential fines that Botium Toys may face due to its current security posture.

5. To establish a clear plan for maintaining compliance and business operations as the company grows.

Current assets

The current assets managed by the IT department at Botium Toys include:

1. Computer systems and servers
2. Software applications for online operations
3. E-commerce website and online storefront
4. Customer data and payment information
5. Network infrastructure and devices
6. Cloud services or storage providers
7. Physical security systems for the office and warehouse
8. Mobile devices used by employees
9. Email and communication systems
10. Back-up and disaster recovery solutions

Risk assessment

1. Risk Description:
There is a risk of a cybersecurity breach or data breach in the IT department at Botium Toys, which could compromise sensitive customer data, financial information, or intellectual property. This can lead to financial losses, reputational damage, and legal consequences.

2. Control Best Practices:
- Implement robust cybersecurity measures such as firewalls, anti-virus software, and intrusion detection systems to prevent unauthorized access to the network.
- Regularly update all software applications and systems with security patches to fix vulnerabilities and protect against known threats.
- Conduct regular security awareness training for employees to educate them on the importance of data security and how to identify potential threats like phishing emails.
- Encrypt sensitive data both at rest and in transit to protect it from unauthorized access.

3. Risk Score:
The risk score for this cybersecurity/data breach risk is high given the potential impact on the organization in terms of financial losses, reputational damage, and legal consequences.

4. Additional Comments:
It is crucial for the IT department at Botium Toys to continuously monitor and assess cybersecurity risks, conduct regular security audits, and develop an incident response plan in case of a security breach. Collaboration with other departments, such as legal, compliance, and risk management, is essential in addressing and mitigating cybersecurity risks effectively.
- It is important for the organization to stay updated on the latest cybersecurity threats and trends in order to proactively address potential vulnerabilities.
- Regularly testing the effectiveness of security controls through penetration testing and vulnerability assessments can help identify and address potential weaknesses in the IT infrastructure.

- Developing a business continuity and disaster recovery plan that includes protocols for responding to cybersecurity incidents can help minimize the impact of a breach and facilitate a swift recovery process.
- Compliance with relevant data protection regulations such as GDPR or CCPA is essential to avoid legal liabilities and protect customer privacy.
- Building a culture of security awareness and accountability within the organization can help create a proactive approach to mitigating cybersecurity risks.