Compliance checklist

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

☐ **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: N/A

☑ **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: Botium Toys, although a U.S. based company, sells toys to customers in the U.S. and abroad, which includes the European Union. The GDPR applies to any organization that processes the personal data of EU citizens, regardless of where the organization is located. Since Botium Toys has customers from the EU, they must comply with GDPR to protect these customers' data privacy rights. This regulation ensures that:

- **EU citizens' personal data is processed lawfully, fairly, and transparently.**

- **Data subjects have the right to be informed, access, rectify, erase, restrict processing, data portability, object to processing, and rights related to automated decision making and profiling.**
- **In the event of a data breach where EU citizens' data might be compromised, Botium Toys is required to notify the affected individuals within 72 hours. This is crucial for maintaining trust and ensuring legal compliance.**

☑ **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: Botium Toys accepts online payments, which involves handling credit card information. The PCI DSS is essential for Botium Toys because:

- **It mandates a secure environment for storing, processing, and transmitting credit card data, which is crucial for preventing data breaches and fraud.**
- **Compliance with PCI DSS helps in building customer trust by ensuring that their payment information is handled with the highest standards of security.**
- **Non-compliance could lead to fines, loss of ability to process credit card payments, and damage to the company's reputation, which would be particularly detrimental as the company grows and aims to expand its online presence.**

By adhering to these regulations, Botium Toys not only complies with legal requirements but also enhances its security posture, protecting both its business operations and its customers' sensitive information. This compliance is part of the broader strategy to ensure business continuity, customer trust, and to mitigate risks associated with data handling in a digital marketplace.

☐ **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: N/A

☑ **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.

System and Organizations Controls (SOC) Type 1

Explanation: SOC 1 reports are specifically focused on financial reporting controls. For Botium Toys, as they grow and their online presence expands, ensuring the integrity of financial reporting becomes increasingly important. Here's how SOC 1 applies:

- **Financial Compliance**: As Botium Toys deals with transactions through online payments, maintaining accurate financial records is crucial. SOC 1 Type 1 provides

an assessment of the design and implementation of controls at a specific point in time, which helps in:

    - Ensuring that financial data is processed accurately, which is vital for compliance with financial regulations and for maintaining investor or stakeholder confidence.
    - Identifying any potential control weaknesses that could lead to financial misstatements or fraud, particularly as they handle customer payments.
- **Risk Assessment**: By undergoing a SOC 1 Type 1 audit, Botium Toys can demonstrate to partners, investors, or regulatory bodies that they have implemented controls designed to safeguard financial information, reducing the risk of financial discrepancies or fraud.

System and Organizations Controls (SOC) Type 2

Explanation: SOC 2 reports go beyond financial reporting to include criteria for security, availability, processing integrity, confidentiality, and privacy. This is particularly relevant for Botium Toys due to:

Security: With the increase in online sales, securing customer data against unauthorized access is paramount. SOC 2 Type 2 assesses the effectiveness of these controls over a period, ensuring:

    - **That customer data, including payment information, is secure against breaches, which is vital for trust in an e-commerce environment.**

Availability: Ensuring that their online platform is available when customers need it, which is critical for maintaining sales and customer satisfaction.

Processing Integrity: Guaranteeing that transactions are processed accurately, completely, and in a timely manner, which directly impacts customer trust and satisfaction.

- **Confidentiality and Privacy: Handling customer information with the utmost confidentiality and respecting privacy laws like GDPR, as they have EU customers. This includes:**

    - **Protecting personal data from unauthorized disclosure and ensuring that customer privacy is maintained, which is crucial for compliance with privacy laws and for maintaining a good reputation.**
- **Risk Mitigation: A SOC 2 Type 2 report provides evidence that not only are controls designed well (as in SOC 1 Type 1), but they are also operating effectively over time. This ongoing evaluation helps Botium Toys in:**

    - **Identifying and addressing operational risks before they lead to significant issues or breaches.**
    - **Demonstrating to customers, partners, and regulatory bodies that they are committed to high standards of data safety and operational integrity.**

By adhering to SOC 1 and SOC 2 standards, Botium Toys can assure stakeholders of their commitment to robust financial and operational controls, reducing the risk of fraud, enhancing customer trust, and supporting business growth through compliance and transparency.