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: Botium Toys would typically not be directly subject to regulations specific to the energy industry, such as the FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation) regulations. These regulatory bodies primarily oversee and regulate the electric utility industry to ensure the reliability, security, and safety of the power grid.

☑ **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 operates globally, offers its products and services to individuals within the EU, The GDPR provides a framework for data protection, including guidelines for data security, data breach notification, and individual rights regarding their personal information. By incorporating GDPR principles into its data management processes, Botium Toys can enhance its overall data security practices and align with internationally recognised best practices. This would help ensure that the company respects the privacy rights of its EU customers and avoids potential legal and reputational risks associated with mishandling their personal data.

☐ **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: Adhering to the Payment Card Industry Data Security Standard (PCI DSS) is essential for Botium Toys, an online toy retailer. It protects customer payment card data, builds trust, meets legal requirements, satisfies partner agreements, and mitigates data breach risks. Compliance ensures secure transactions, safeguards reputation, and demonstrates commitment to data security.

☐ **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: Botium Toys is not subject to the Health Insurance Portability and Accountability Act (HIPAA) laws. HIPAA regulations primarily apply to healthcare providers, health plans, and entities that handle protected health information (PHI). Since Botium Toys' operations revolve around selling toys online and not healthcare services or handling medical data, HIPAA compliance is not necessary in their case.

☑ **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: Botium Toys, as an online toy retailer, should consider utilizing System and Organization Controls (SOC) Type 1 and SOC Type 2 reports to enhance its operational transparency and build trust with customers. A SOC Type 1 report provides an assessment of the effectiveness of Botium Toys’ internal controls at a specific point in time, offering insights into the design and implementation of its systems. This can assure customers that Botium Toys has adequate controls in place to protect their data and maintain the integrity of its operations. On the other hand, a SOC Type 2 report evaluates the operational effectiveness of these controls over a period of time, demonstrating Botium Toys’ commitment to continuous monitoring and improvement. By obtaining and sharing SOC reports, Botium Toys can provide customers with independent validation of its security measures, fostering confidence in the company's ability to handle customer data securely and reliably.