Compliance checklist

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

This 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 Federal Energy Regulatory Commission (FERC).

Explanation: NA - Botium Toys does not work directly with the power grid or electricity generation, making FERC-NERC regulations not applicable to their operations.

___X__ 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 engages in online sales and collects personal information from customers globally, including those in the E.U. Adhering to GDPR is essential to protect the privacy of E.U. citizens and avoid substantial fines.

___X__ 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: As Botium Toys accepts and processes credit card payments from customers, compliance with PCI DSS is mandatory to secure payment transactions and protect against data breaches.

____ 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: NA - Botium Toys does not deal with health information, so HIPAA does not apply to their business operations.

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

___X__ 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: Implementing SOC1 and SOC2 controls may be beneficial for Botium Toys to ensure the integrity and security of their financial and customer data. This is particularly important as the company grows and scales its operations internationally, requiring robust data safety measures.