Compliance checklist

☐ **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: Unless Botium Toys is directly involved in the generation, distribution, or management of electric power, or has a significant role in the power grid's infrastructure, FERC-NERC regulations are likely not applicable. Botium Toys, being a toy company, is unlikely to fall under this standard unless there are specific operations related to power distribution that have not been mentioned.

☐ **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: GDPR is relevant for any organization that processes, stores, or manages data of E.U. citizens, irrespective of the organization's physical location. If Botium Toys has customers from the E.U. or operates within its

boundaries, it's essential to ensure GDPR compliance. This includes clear data handling and privacy policies and prompt breach notifications.

☐ **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 likely accepts card payments (given the mention of e-commerce systems in their assets), they must adhere to PCI DSS standards. This ensures that customers' payment data is handled securely and minimizes the risk of financial 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: HIPAA is specific to the healthcare sector, focusing on protecting patients' health information. Unless Botium Toys has some involvement in healthcare or manages health-related data, this regulation isn't directly applicable. However, it's always good to be aware of strict data protection standards like HIPAA.

☐ **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: SOC reports help organizations demonstrate the robustness of their financial reporting and internal controls. For Botium Toys, undergoing SOC audits can assure stakeholders, especially if they manage third-party data or provide services requiring a high level of trust in their data management and security practices. While not always a legal requirement, SOC compliance can be crucial for business partnerships and trustworthiness. For Botium Toys, it appears that GDPR and PCI DSS are the most immediately relevant compliance standards. Still, the applicability of other standards will depend on specific business operations not outlined in the provided information.