Compliance checklist

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

- ☐ **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: Not applicable.

- ☑ **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: After conducting a controls assessment, it has been determined that Botium Toys must adhere to General Data Protection Regulation (GDPR).

This is necessary due to the company's global operations and the collection of personal information from individuals worldwide, including those in the European Union (EU). Ensuring GDPR compliance is vital to safeguarding data privacy and maintaining legal and ethical standards in handling personal information.

☑ **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: Based on the control assessment conducted, it is essential for Botium Toys to adhere to Payment Card Industry Data Security Standard (PCI DSS). This is imperative as the company is involved in storing, accepting, processing, and transmitting credit card information both in-person and online. Adhering to PCI DSS ensures the secure handling of sensitive payment card data and helps mitigate the risk of data breaches, protecting both the company and its customers from potential financial and reputational harm.

☐ **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: Not applicable.

☑ **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: Based on the control assessment conducted, it is crucial for Botium Toys to implement and enforce a comprehensive user access control policy. This policy should cover both internal and external personnel, including third-party vendors. By establishing appropriate user access controls, the company can effectively mitigate risks and ensure the safety of data. Proactive measures in this area help safeguard against unauthorized access, potential breaches, and data compromises, ultimately bolstering the overall security posture of Botium Toys.