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: Does not meet this standard as Botium toys currently does not have a business continuity plan or any system in place to mitigate incidents. Was placed on high priority in the controls assessment

☐ **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 does not meet this standard as they do not have security measures in place to protect sensitive data such as financial records, and personal information. Related controls were set as a Medium priority in the controls assessment.

☐ **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 does not meet this standard as they do not have a strong enough security to store, accept, process, and transmit financial data. Related controls were set to Medium priority in the controls assessment.

☐ **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 does not meet this standard as they lack the security to fully protect employee health data from breaches. Related controls were set to Medium priority in the controls assessment.

☐ **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 does not meet this standard as there is an overall high amount of risk that could affect the business, its employees, and its customers. The overall risk score is 8/10 High. Botium Toys was given a

controls assessment to provide insight on what they should focus their priority on and the reasons why.