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:

  BOTIUM toys are not directly involved with the North American Power grid. And Botium is working towards adding more safety for physical/ On site incidents such as fires and natural disasters.

- ☑ **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:

  Currently not in compliance with GDPR as nist CSF is implemented and as per European laws. For BOTIUM toys to be able to expand and continue to

do business in the European Union. ECSF(European CyberSecurity Framework) needs to be implemented.

☑ **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:

Botioum Toys does not comply with Payment Card Industry Data Security as only NIST CSF has been implemented and it only deals with general risk assessment and management and ways to mitigate it to be able to ensure safety of payments Botium toys needs to adhere to PCI DSS. PCI DSS is important because it has 12 set of requirements which include

1. **Firewalls**
2. **Antivirus**
3. **Network Monitoring**
4. **Access controls**
5. **Tracking and monitoring usage**
6. **Developing safe to use Applications.**
7. **Maintaining network access**
8. **Restrict Physical Access to card holder's data**
9. **Maintaining a strict policy that ensures data security**
10. **Assigning unique ID to everybody who access the card holder's data**
11. **Regularly Update Firewalls and Antiviruses**
12. **Regularly Testing Firewalls and safetyfeatures**

☐ **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 in tow business and does not deal directly with the employees medical record. So Botium Toys does not have to comply with the HIPAA policies. What Botium Toys can do is make sure that their insurance company which offers insurance to the employees follow the HIPAA guidelines. The company needs to adhere to HIPAA because protecting Employee SPII is the responsibility of the company such as medical records that they have on themselves or they receive through the insurance companies.

☑ **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:

While NIST CSF(currently implemented) Does offer some type of access control it does require discrete information about the organization. Currently Botium Toys does not comply with SOC1 and SOC2 but it does protect the CIA triad in some way. One risk that NIST CSF has is it does not give clear implications of financial risks and fines that would be implied on

Botium technologies to assess those financials one would need to go imply these frameworks.