**Sprint Four**

**Theme: Legal, Regulatory, and Compliance Implementation on Security Controls**

"Legal, regulatory, and compliance implementation on security controls" refers to the process of ensuring that an organization's security measures align with relevant laws, regulations, and industry standards. It involves implementing security controls and practices that comply with legal requirements and regulations in order to protect sensitive data and maintain the organization's integrity.

**What are the differences between a law, a regulation and compliance?**

**What are the differences between a cybersecurity secure program being legal, it being in and of regulations and the same program being in compliance?**

**Laws:** A law, also known as legislation or statute, is a formal rule or set of rules enacted by a legislative body, such as a national or state government. Laws are generally broader in scope and can cover a wide range of issues, including cybersecurity. They establish legal obligations and consequences for non-compliance. Laws are binding and enforceable, and violations can lead to legal penalties. When a cybersecurity secure program is legal, it means that it adheres to the laws and regulations applicable to cybersecurity and data protection. ***It ensures that the program meets the minimum legal requirements set by governing bodies.*** Compliance with legal requirements helps avoid legal consequences and penalties.

*Example*: The California Consumer Privacy Act (CCPA) is a state law that grants consumers certain rights regarding their personal information and imposes obligations on businesses regarding data protection and privacy. It sets requirements for cybersecurity practices, breach notification, and consumer rights related to data privacy.

**Regulations**: Regulations are specific rules and guidelines established by regulatory authorities or industry bodies. ***Being "in regulations" means that the cybersecurity secure program aligns with the specific regulations relevant to the organization's industry or operations.*** This entails meeting the additional requirements beyond the basic legal obligations. Regulations are typically more specific and detailed than laws, and they often focus on a particular industry, sector, or specific aspect of a broader law. In the cybersecurity realm, regulations outline specific requirements and standards that organizations must follow to ensure the security and privacy of data. These regulations may be issued by governmental bodies or industry-specific regulatory agencies.

*Example*: The General Data Protection Regulation (GDPR) in the European Union is a regulation that governs the privacy and protection of personal data for individuals residing in EU member states. It sets specific requirements for organizations to handle personal data, including cybersecurity measures, breach notification obligations, and data subject rights.

**Compliance**: Compliance refers to the act of adhering to all applicable legal requirements, regulations, and standards. ***A cybersecurity secure program is considered "in compliance" when it fulfills all the necessary obligations, both legal and regulatory.*** Compliance demonstrates that the program meets the required standards and best practices. Compliance programs are designed to mitigate risks, promote good governance, and ensure adherence to legal and regulatory obligations.

*Example*: An organization being in compliance with the Payment Card Industry Data Security Standard (PCI DSS) means that it has implemented the necessary technical and operational security measures to protect cardholder data as required by the standard. Compliance with PCI DSS is essential for organizations that handle payment card information.

**Real Quick:**

* ***regulations*** are specific rules and guidelines established by governing bodies;,
* ***laws*** are broader rules enacted by legislative bodies;
* ***compliance*** refers to adhering to legal, regulatory, and industry-specific requirements.

**Legal: Depending on which laws you as a group member decided to work on, your research and writing should answer the following questions (with APA Cited References):**

* **What federal laws does a cybersecurity secure program for a non-profit have to adhere to? (What are the federal legal requirements a cybersecurity security program must comply with?)**
* **What New York State laws does a cybersecurity secure program for a non-profit have to adhere to? (What are the federal legal requirements a cybersecurity security program must comply with?)**
* **Why does the cybersecurity program have to adhere to this specific federal or state law? (For example, it’s because they take online payments.)**
* **What does the cybersecurity secure program have to contain or offer to satisfy or adhere to (federal or state law being discussed)?**
* **Are there any California, Georgia or New Jersey state laws applicable to a cybersecurity secure program for an NPO (as TKH operates in CA, GA and NJ)?**
* **What are the penalties for violating federal law to the non-profit in this instance?**
* **What are the penalties for violating state law to the non-profit organization?**
* **Relate it back to regulatory compliance:** 
  + **What cybersecurity frameworks are being followed when a cybersecurity secure program is following [insert law here]?**
  + **What regulations are being followed when a cybersecurity secure program is following [insert law here]?**

**Regulation: Depending on what regulation and/or cybersecurity framework you’re working on, the research and writing should answer most the following questions (with APA Cited References):**

* **What federal regulations does a cybersecurity secure program for a non-profit organization have to adhere to?**
* **What state regulations does a cybersecurity secure program for a non-profit have to adhere to?**
* **Why does the cybersecurity program have to adhere to this specific federal or state regulation? (For example, it’s because they take online payments.)**
* **What industry-specific regulations are applicable to the non-profit organization?**
* **What does the cybersecurity secure program have to contain or offer to satisfy or adhere to (regulation being discussed)?**
* **Are there any California, Georgia or New Jersey state regulations applicable to a cybersecurity secure program for an NPO (as TKH operates in CA, GA and NJ)?**
* **Which cybersecurity frameworks would keep a secure program in regulatory compliance? How?**
* **What is CIS and how is it used as a security control tool? How does CIS satisfy compliance?**
* **What are the data breach notification requirements? (What are the legal obligations and timelines for reporting data breaches or security incidents to affected individuals, regulatory authorities, or other relevant parties?)**
* **Relate it back to legal compliance:** 
  + **What federal laws are being followed when a cybersecurity secure program is following [insert federal regulation here]?**
  + **What federal laws are being followed when a cybersecurity secure program is following [insert state regulation here]?**
    - For example, breach notification for personal information breaches is in alliance with the New York SHIELD Act
  + **How do CIS controls factor into regulatory compliance?**

**Duties and Responsibilities:**

**Focus:**

**Federal Laws**

* Gramm-Leach-Bliley Act (GLBA)
* The Family Educational Rights and Privacy Act (FERPA)
* The Children's Online Privacy Protection Act (COPPA)
* The Health Insurance Portability and Accountability Act (HIPAA)??

**State Laws**

* New York General Business Law (GBL) § 899-aa
* New York Education Law § 2-d
* New York Nonprofit Revitalization Act
* New York General Business Law (GBL) Article 39-F

**Federal Regulations**

* Federal Acquisition Regulation (FAR) Clause 52.204-21
* Section 5 of the Federal Trade Commission Act
* Safeguards Rule (part of the Gramm-Leach-Bliley Act)
* General Data Protection Regulation (GDPR)
* Payment Card Industry Data Security Standard (PCI DSS)
* Red Flags Rule?
* Health Breach Notification Rule?

**New York State Regulations**

* NYSED Data Privacy and Security Policy
* New York SHIELD Act: The SHIELD Act (Stop Hacks and Improve Electronic Data Security)

**Presentation**

**Sprint Summary**

**Law/Regulation Outline (brief):**

1. What is the law or regulation? (in simple terms)
2. Why is it applicable to TKH?

(For example, PCI DSS is applicable to TKH because the organization.)

1. Does TKH’s current secure program satisfy this legal or regulatory requirement? Yes or No and Why?
2. What are the fines for violating this law or regulation?

| **Group Member** | **Regulation** |
| --- | --- |
| **Everyone** | Payment Card Industry Data Security Standard (PCI DSS) |
| **Tianna G.** | **State Law:** New York SHIELD Act  **Federal Law:** COPPA |
| **Aaron Kaah** | **State Law:** GA/ SS-08-016 Computer Operations Center Security. Reference: NIST SP 800-12 Information Security Handbook (Ch 15)  **Center for Internet Security (CIS) Controls** |
| **Frederick Asante** | **Regulation:** General Data Protection Regulation (GDPR) |
| **Jane Pierre** | **State Law:** New York General Business Law (GBL) §899-aa  **Summary** |
| **Mishelly Sandoval** | **State Law:** New York Nonprofit Revitalization Act  **Presentation** |
| **Lucas Higgs** | **Federal Law:** Gramm-Leach-Bliley Act (GLBA)  **Regulation:** Safeguards Rule (part of the Gramm-Leach-Bliley Act)  **Presentation** |
| **Shamar Brown** | **Federal Law:** The Family Educational Rights and Privacy Act (FERPA) |
| **Elizabeth Bond** | **State Law:** New York Education Law § 2-d  **Summary** |

**Payment Card Industry Data Security Standard (PCI DSS) - (Remember to Put the Website you got your info from) (Add: Use web resources and put them in short and long APA citation format.)**

1. **What is the PCI DSS?**
2. **What parts are applicable to TKH? Why?**
3. **How can a secure program satisfy the regulatory requirements of the PCI DSS?**
4. **What ways can a medium non-profit violate the PCI DSS? (Examples)**
5. **What are the fines/consequences associated with violating the PCI DSS?**
6. **Case Examples of companies similar to TKH that had violated the PCI DSS (in terms of cybersecurity) and what happened as a result.**

**Deliverables due Friday, May 19, 2023 at 11:59pm**

**1 Google Doc - with a brief outline of the law you choose AND your research on PCI DSS (with APA citation)**