Supply Chain Risk Management (SCRM) Plan

Objective: To enhance Mentornity's ability to manage cybersecurity risks across its supply chain and ensure information security and privacy in its relationships with suppliers.

1. Establishing a Supply Chain Risk Management Strategy (GV.SC-01)

- **Step 1: Define Policies and Procedures**
  - Mentornity should develop a supply chain risk management policy to manage risks associated with suppliers and third-party service providers.
  - This policy should outline the security practices, data handling procedures, and incident response protocols of suppliers.
- **Step 2: Assign Roles and Responsibilities**
  - Specific roles should be assigned within Mentornity to manage supply chain risk management tasks and responsibilities. For example, the security team could be responsible for managing supplier risk assessments and security audits.
- **Step 3: Define Security Contract Clauses**
  - Mentornity should include cybersecurity requirements and compliance commitments in agreements with suppliers. These requirements should cover data encryption standards, access control policies, and the reporting of security incidents.

2. Supplier Security Risk Assessment (GV.SC-05)

- **Step 1: Create a Supplier Evaluation Process**
  - A process should be developed to evaluate the cybersecurity risk profiles of suppliers. This process should involve identifying the existing security measures and potential vulnerabilities of each supplier.
  - For example, an annual cybersecurity assessment and risk analysis can be conducted for each supplier.
- **Step 2: Implement Supplier Security Audits**
  - Mentornity should regularly audit the security controls and practices of critical suppliers. These audits provide an opportunity for suppliers to address vulnerabilities and make improvements.
- **Step 3: Continuous Monitoring and Reporting**
  - A continuous monitoring and reporting system should be established to track supplier performance and security compliance. This system ensures that any security breaches or poor security practices are promptly reported.

3. Supply Chain Collaboration and Communication (GV.SC-02)

- **Step 1: Establish Communication and Training Programs**

    - Effective communication channels should be established with suppliers and partners, and awareness training programs on cybersecurity risks should be developed.
- **Step 2: Define Breach Notification Procedures**
    - Under agreements with suppliers, a breach notification procedure should be established that specifies the timeframe and method for reporting any potential security breach.

4. Supply Chain Risk Management Improvement Process (GV.SC-06)

- **Step 1: Review and Improve Evaluation Outcomes**
    - The results from supplier assessments and audits should be regularly reviewed, and existing supply chain security policies should be continuously improved.
- **Step 2: Prepare for Future Risk Scenarios**
    - To proactively address potential security risks across the supply chain, potential risk scenarios should be developed, and preventive measures should be established.