Global Certificate in Critical Infrastructure Security Management

Regulatory and Compliance Frameworks

Regulatory and Compliance Frameworks are critical components of the Global Certificate in Critical Infrastructure Security Management. These frameworks provide a set of guidelines, policies, and procedures that organizations must follow to ensure the security and resilience of their critical infrastructure. Here are some key terms and vocabulary related to Regulatory and Compliance Frameworks:

1. Regulatory Framework: A regulatory framework is a set of laws, regulations, and guidelines that an organization must follow to operate within a specific industry or sector. These frameworks are designed to ensure that organizations comply with certain standards and practices to protect public safety, security, and health. In the context of critical infrastructure, regulatory frameworks may include laws and regulations related to transportation, energy, water, and other critical sectors.

Example: The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are a regulatory framework for the electric utility industry in North America. These standards establish requirements for cybersecurity, physical security, and recovery planning for bulk power systems.

2. Compliance Framework: A compliance framework is a set of standards, policies, and procedures that an organization must follow to comply with specific regulations, laws, or contractual obligations. Compliance frameworks may be established by regulatory bodies, industry groups, or individual organizations. These frameworks provide a systematic approach to managing compliance risk and ensuring that an organization meets its legal and contractual obligations.

Example: The National Industrial Security Program Operating Manual (NISPOM) is a compliance framework for contractors who handle classified information for the U.S. government. The framework establishes requirements for security clearances, facility security, and information handling.

3. Risk Management: Risk management is the process of identifying, assessing, and prioritizing risks to an organization's critical infrastructure. Risk management involves developing strategies to mitigate or eliminate these risks and monitoring their effectiveness. Regulatory and compliance frameworks often include risk management requirements to ensure that organizations are taking a proactive approach to security and resilience.

Example: The National Institute of Standards and Technology (NIST) Cybersecurity Framework includes a risk management function that provides guidance on identifying, protecting, detecting, responding, and recovering from cybersecurity threats.

4. Audit and Assessment: Audit and assessment are processes used to evaluate an organization's compliance with regulatory and compliance frameworks. Audits may be conducted by internal or external

parties and typically involve a review of policies, procedures, and records to ensure that the organization is following the required standards and practices. Assessments may also include testing and validation of security controls to ensure that they are effective.

Example: The Payment Card Industry Data Security Standard (PCI DSS) requires organizations to undergo annual audits to ensure compliance with the standard. These audits may be conducted by Qualified Security Assessors (QSAs) who are trained and certified to evaluate compliance with the PCI DSS.

5. Incident Response: Incident response is the process of identifying, containing, and mitigating security incidents that may impact an organization's critical infrastructure. Regulatory and compliance frameworks often include incident response requirements to ensure that organizations are prepared to respond to security threats and minimize the impact of incidents.

Example: The NIST Cybersecurity Framework includes an incident response function that provides guidance on preparing for, detecting, responding to, and recovering from cybersecurity incidents.

6. Policy and Procedure: Policies and procedures are formal documents that establish guidelines and procedures for an organization's operations. Regulatory and compliance frameworks often include policy and procedure requirements to ensure that organizations have a clear and consistent approach to security and resilience.

Example: The Health Insurance Portability and Accountability Act (HIPAA) includes policy and procedure requirements for protecting patient health information. These requirements include guidelines for access control, data backup, and incident response.

7. Training and Awareness: Training and awareness are critical components of regulatory and compliance frameworks. These activities help ensure that employees are aware of security risks and understand their roles and responsibilities in protecting critical infrastructure. Training and awareness programs may include security awareness training, incident response training, and role-based training for specific job functions.

Example: The NERC CIP standards include training and awareness requirements for employees who are responsible for operating and maintaining bulk power systems. These requirements include training on cybersecurity threats, physical security, and emergency response.

8. Continuous Monitoring: Continuous monitoring is the process of continuously evaluating and assessing an organization's security posture. Regulatory and compliance frameworks often include continuous monitoring requirements to ensure that organizations are proactively identifying and addressing security threats.

Example: The Federal Risk and Authorization Management Program (FedRAMP) includes continuous monitoring requirements for cloud service providers who serve the U.S. government. These requirements include ongoing security assessments, vulnerability scans, and security controls testing.

9. Third-Party Risk Management: Third-party risk management is the process of evaluating and managing the security risks associated with third-party vendors and contractors. Regulatory and compliance frameworks often include third-party risk management requirements to ensure that organizations are taking a proactive approach to managing security risks associated with third-party relationships.

Example: The NIST Cybersecurity Framework includes a third-party risk management function that provides guidance on identifying, assessing, and mitigating security risks associated with third-party relationships.

10. Supply Chain Risk Management: Supply chain risk management is the process of evaluating and managing the security risks associated with an organization's supply chain. Regulatory and compliance frameworks often include supply chain risk management requirements to ensure that organizations are taking a proactive approach to managing security risks associated with their supply chain.

Example: The National Industrial Security Program Operating Manual (NISPOM) includes supply chain risk management requirements for contractors who handle classified information for the U.S. government. These requirements include evaluating the security practices of subcontractors and suppliers.

In summary, Regulatory and Compliance Frameworks are essential components of the Global Certificate in Critical Infrastructure Security Management. These frameworks provide a set of guidelines, policies, and procedures that organizations must follow to ensure the security and resilience of their critical infrastructure. Understanding key terms and vocabulary related to these frameworks is critical for ensuring that organizations are following best practices and meeting their legal and contractual obligations. By implementing effective regulatory and compliance frameworks, organizations can proactively identify and address security threats, minimize the impact of incidents, and ensure the continued operation of their critical infrastructure.