Cybersecurity Assessment Training (non-DOD)

5 Days – 40 Hours

Training Description

The NIST Cybersecurity Framework (CSF) is a risk-based approach to managing cybersecurity that can be used by organizations of all sizes. The CSF provides a common language and set of processes for organizations to use to improve their cybersecurity posture. This training will provide an overview of the NIST CSF and it's five core functions: Identify, Protect, Detect, Respond, Recover.

In this training participants will learn how to conduct a light gap assessment of their organization's cybersecurity framework and how to identify risks. Participants will learn how to summarize their assessment based on each control family. Participants will then have a path moving forward to address concerns and issues within their own company. The training will identify real world examples of current cyber incidents to illustrate the importance of cybersecurity.

This training is appropriate for Organizational staff and leadership focused on IT, Quality, Risk Compliance and/or Governance. It will be delivered virtually.

Training Objective

Overall, the training aims to equip participants with an understanding of the NIST CSF, conduct a gap assessment, evaluate associated risks, and develop an actionable plan to enhance the organization's cybersecurity posture.

Skill Attainment

Upon completing this training, participants will acquire firsthand knowledge of identifying risks using the NIST Cybersecurity Framework. They will gain a comprehensive understanding of creating and maintaining action plans to address identified risks, along with recognizing the significance of IT governance.

Agenda

Day 1

- Introduction to the NIST CSF
  - What is the NIST CSF
  - The five core functions of the NIST CSF
  - Gather information about the organization's cybersecurity posture.
  - Identify gaps between the organization's current posture and the NIST CSF

Day 2-4

- Assess the risks associated with the gaps by participants.
- Develop a plan to address the risks identified in the risk assessment.
- Create assessment deliverables identifying areas for improving their cybersecurity posture with a Project plan.

Day 5

- Summary of the assessment
- Review assessment deliverables
- Questions and answers