Course Outline

NIST Cybersecurity Framework (NCSF) Foundation

Course Summary

Description

The one-day LRS NIST Cybersecurity Foundation course is designed for anyone in an organization who needs to understand the basics of cybersecurity, the components of the NIST CSF, and how the NIST CSF aligns to risk management. Security, IT, risk management, policy makers, and other business professionals who have responsibility for aspects of business or technical security can benefit from this course.

Topics

- Course Introduction
- The Basics of Cybersecurity
- A Holistic Study of The NIST Cybersecurity Framework
- Cybersecurity Activities: The Framework Core
- Risk Management Considerations: Framework Implementation Tiers
- Current and Desired Outcomes: Framework Profiles
- Primer on The Seven Step Framework Implementation Process

Audience

This course is designed for anyone in an organization who needs to understand the basics of cybersecurity, the components of the NIST CSF, and how the NIST CSF aligns to risk management. Security, IT, risk management, policy makers, and other business professionals who have responsibility for aspects of business or technical security can benefit from this course.

Prerequisites

There are no prerequisites for this course. Basic computing skills and security knowledge will be helpful.

Duration

One day

Course Outline

NIST Cybersecurity Framework (NCSF) Foundation

Course Outline

I. *Course Introduction*
   A. Provides the student with information relative to the course and the conduct of the course in the classroom, virtual classroom, and course materials.

II. *The Basics of Cybersecurity*
   A. What is cybersecurity?
   B. Types of attackers
   C. Vulnerabilities
   D. Exploits
   E. Threats
   F. Controls
   G. Frameworks
   H. Risk-Based Cybersecurity

III. *A Holistic Study of The NIST Cybersecurity Framework*
   A. History
   B. EO 13636
   C. Cybersecurity Enhancement Act of 2014
   D. EO 13800
   E. Uses and Benefits of the Framework
   F. Attributes of the Framework
   G. Framework Component Introduction
   H. Framework Core
   I. Framework Profiles
   J. Framework Implementation Tiers

IV. *Cybersecurity Activities: The Framework Core*
   A. Purpose of the Core
   B. Core Functions, Categories, and Subcategories
   C. Informative References

V. *Risk Management Considerations: Framework Implementation Tiers*
   A. Purpose of the Tiers
   B. The Four Tiers
   C. Components of the Tiers
   D. Compare and contrast the NIST Cybersecurity Framework with the NIST Risk Management Framework

VI. *Current and Desired Outcomes: Framework Profiles*
   A. Purpose of the Profiles
   B. The Two Profiles
   C. Interrelationships between the Framework Components

VII. *A Primer on The Seven Step Framework Implementation Process*
   A. Prioritize and Scope
   B. Orient
   C. Create a Current Profile
   D. Conduct a Risk Assessment
   E. Create a Target Profile
   F. Determine, Analyze, and Prioritize Gaps
   G. Implement Action Plan