NISTv2.0: Integrating NIST Frameworks (ERM/CSF/RMF)

Days: 3

Description: This three-day Integrating NIST Frameworks (ERM/CSF/RMF) course helps students to understand the background and integration of several key frameworks from the National Institute of Standards and Technology (NIST). The course explains the background and application of NIST's Cybersecurity Framework (CSF) version 2.0, Enterprise Risk Approach, and Risk Management Framework (RMF), and their relationship to other NIST models such as those for Cybersecurity Workforce, Privacy Risk Management, and Cybersecurity Supply Chain Risk Management (C-SCRM). Discussion also addresses NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, that many private organizations must apply within their own operations.

Using CSF's proven components (updated in 2024) as a way to organize risk expectations, outcomes and communication, the course explains the interaction among mission objectives and priorities, risk management through the language of business, and application of those objectives for managing risk for business systems and services.

The course helps security teams understand how to manage risk in light of executives' priorities, and it helps leaders apply the necessary privacy & security enablers to be prepared for an ever-evolving cybersecurity risk landscape.

OUTLINE

SECTION 1 - COURSE INTRODUCTION

- This section will provide an overview of the course including the relevant learning objectives, course organization, and approach. It will introduce the role of the U.S. National Institute of Standards and Technology (NIST) in setting international standards, providing broad risk management guidance, and promoting interoperability.

SECTION 2 - THE BASICS OF CYBERSECURITY RISK MANAGEMENT

- Internationally-recognized standards and models for describing risk itself and the management of that risk to support enterprise mission and objectives;
- Defining the scope of a risk management program and establishing relevant internal and external context for achieving objectives;
- Purpose and process for risk identification;
- Methodologies and tradeoffs for effective risk analysis;
- Risk evaluation to consider the results of analysis, in light of stakeholder expectations and enterprise context, to determine appropriate risk response;
- Risk treatment through accountable implementation of the risk response selected;
- Monitoring and review of ongoing risk conditions at each organizational level; and,
- Tools, templates, and processes for continuous communications for risk management strategy, direction, achievement, and adjustment.

SECTION 3 - INTRODUCTION TO THE NIST CYBERSECURITY FRAMEWORK V2.0

- Events leading to the creation and updates to the Cybersecurity Framework;
- Uses and Benefits of the Framework;
- The CSF process for organizational communications and coordination;
- Framework Components (Core, Profiles, Implementation Tiers); and,
- NIST Supplemental Materials for applying the CSF.

SECTION 4 - DETAILED REVIEW OF THE FRAMEWORK CORE

- The Framework's 6 Functions

NISTv2.0: Integrating NIST Frameworks (ERM/CSF/RMF)

- Govern - Determine and maintain the organization's cyber risk strategy, expectations, and policy;
- Identify – Determine and document what resources are vital to enterprise mission, and a high-level understanding of threats and vulnerabilities;
- Protect – Define and document how best to protect those resources;
- Detect – Effectively detect and analyze emerging risks;
- Respond – Efficiently implement risk response in accordance with plans, training, and strategies; and
- Recover – Plan, execute, and document steps to recover from cyber incidents, including necessary notifications, communications, and improvements.
- Explore each of the 22 Categories in detail, including review of CSF's Subcategories;
- Discuss the value of (and cautions regarding) changes to the CSF Core; and,
- Provide a demonstration of NIST's Online Informative Reference (OLIR) Program.

SECTION 5 - ORGANIZATIONAL ASSESSMENT THROUGH THE FRAMEWORK IMPLEMENTATION TIERS

- Background and purpose of the Implementation Tiers;
- The components of the Implementation Tiers (Risk Management, Risk Process Integration, External Participation);
- The four Implementation Tier levels (Partial, Risk Informed, Repeatable, Adaptive); and,
- Parallel industry models for measuring process achievement.

SECTION 6 - PLANNING AND RECORDING ORGANIZATIONAL OUTCOMES THROUGH FRAMEWORK PROFILES

- The purpose of the Profile CSF component;
- Examples of manual and automated profiles, including pointers to various templates;
- Discussion about how to measure plans and results;
- Methods for documenting current state ("as-is"), desired, or target, state ("to-be"), and interim milestones between those states; and,
- Considerations for measuring progress and recording that in profiles.

SECTION 7 - THE CYBERSECURITY FRAMEWORK FIVE-STEP PROCESS

- Review of Step 1 - Scope the Organizational Profile.
- Review of Step 2 - Gather the information needed to prepare the Organizational Profile
- Review of Step 3 - Create the Organizational Profile and apply Community Profiles, where applicable.
- Review of Step 4 - Plan actions based on gaps among Current and Target Profiles.
- Review of Step 5 - Implement the action plan and update the Organizational Profile.

SECTION 8 - INTRODUCTION TO THE NIST RISK MANAGEMENT FRAMEWORK

- A brief history of the NIST FISMA Implementation Project;
- NIST's role in various cybersecurity initiatives;
- Introduction to NIST publications and standards;
- The Risk Management Framework seven step process (Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor); and,
- Connections among Cybersecurity Framework steps, RMF steps, and other models.

NISTv2.0: Integrating NIST Frameworks (ERM/CSF/RMF)

SECTION 9 - INTEGRATION OF CSF AND RMF WITH OTHER KEY FRAMEWORKS

- Integrating CSF, RMF, and the NIST Privacy Framework;
- Understanding the relationship to NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, which many private organizations must apply in daily operations;
- Defining risk management activities through the work roles, tasks, knowledge statements, and skills statements of the NICE Workforce Framework;
- Leveraging other NIST Frameworks (e.g., Baldrige, Supply Chain, Software Development, Cyber Physical) to ensure a comprehensive risk management approach; and,
- Integrating NIST risk management with those from other worldwide organizations.

SECTION 10 - APPLYING NIST FRAMEWORKS TO REAL-WORLD CYBERSECURITY

- Integrating cybersecurity risk management (CSRM) in support of enterprise risk management (ERM), including review of NIST's recent guidance on that topic (NIST Interagency Report 8286);
- Organizational assessments through integrated CSF/RMF templates
- Processes for security planning through selecting and tailoring security and privacy controls
- Integration of MITRE ATT&CK™ and Pre-ATT&CK into training, assessment, reporting, and monitoring
- Reviewing Roles and Responsibilities from the CSF, RMF, NICE, and other models
- Continuous monitoring and ongoing authorization / ongoing assessment; and,
- Applying the integrated approach to ensure holistic enterprise risk communications, coordination, and comprehension.