1. NIST Cybersecurity Framework 2.0 Foundation

Duration: 1 Day

Course Overview:

This course provides a foundational understanding of the NIST Cybersecurity Framework (CSF) 2.0. Participants will gain knowledge about the framework's core components, principles, and how it can be applied to enhance cybersecurity practices in organizations.

Course Objectives:

- Understand the purpose and structure of the NIST CSF 2.0.
- Learn the key components: Functions, Categories, and Subcategories.
- Explore the Tiers and Profiles and how they guide cybersecurity maturity.
- Gain insights into integrating the framework within an organization's existing cybersecurity practices.

Course Outline:

1. **Introduction to NIST Cybersecurity Framework 2.0**
   - Overview of NIST and the evolution of the CSF
   - Key changes and updates in version 2.0
   - Importance and benefits of adopting the NIST CSF
2. **Understanding the Core Functions**
   - **Identify:** Understanding organizational context, assets, and risks
   - **Protect:** Safeguards to ensure critical services
   - **Detect:** Identifying cybersecurity events promptly
   - **Respond:** Steps to take in response to detected cybersecurity events
   - **Recover:** Plans for resilience and restoring capabilities
3. **Deep Dive into Categories and Subcategories**
   - Explanation of the Categories within each Function
   - Understanding Subcategories and how they relate to organizational activities
4. **Implementation Tiers and Profiles**
   - Explanation of Tiers (Partial, Risk Informed, Repeatable, Adaptive)
   - Developing and using Profiles for aligning cybersecurity activities with business requirements
5. **Integrating NIST CSF 2.0 in Organizational Practices**
   - Practical steps to start using the framework
   - Case studies and examples of NIST CSF implementation
   - Challenges and best practices
6. **Interactive Session: Case Study & Group Discussion**
   - Real-world scenarios and group discussion
   - Applying the framework to various organizational contexts
7. **Conclusion and Q&A**
   - Recap of key learnings
   - Open forum for questions and discussion

2. NIST Cybersecurity Framework 2.0 Lead Implementer

Duration: 2 Days

Course Overview:

This course is designed for professionals who will be responsible for leading the implementation of the NIST Cybersecurity Framework 2.0 in their organizations. Participants will learn how to tailor the framework to their organization's needs, develop implementation plans, and integrate the framework into existing processes.

Course Objectives:

- Develop a comprehensive understanding of NIST CSF 2.0.
- Learn to customize and implement the framework in different organizational contexts.
- Understand how to create effective implementation plans and integrate with existing cybersecurity strategies.
- Gain practical experience through case studies and role-playing exercises.

Course Outline:

1. **Introduction and Review of NIST CSF 2.0**
   - Quick review of NIST CSF 2.0 components and principles
   - Role of a Lead Implementer
2. **Planning the Implementation**
   - Assessing organizational readiness
   - Defining scope and objectives for the NIST CSF implementation
   - Building a cross-functional implementation team
3. **Tailoring the Framework to Organizational Needs**
   - Customizing the Core Functions, Categories, and Subcategories
   - Setting appropriate Implementation Tiers
   - Developing and aligning Profiles with organizational risk management
4. **Developing an Implementation Plan**
   - Roadmap and timeline creation
   - Resource allocation and budgeting
   - Communication strategy and stakeholder engagement
5. **Integrating NIST CSF with Existing Practices**
   - Mapping the framework to existing cybersecurity policies and procedures
   - Coordinating with risk management, compliance, and IT governance
6. **Change Management and Continuous Improvement**
   - Managing organizational change during implementation
   - Establishing metrics and KPIs for continuous improvement
7. **Interactive Workshops**
   - Case study analysis: Developing a custom implementation plan
   - Role-playing exercises: Handling implementation challenges
8. **Finalizing the Implementation**
   - Testing and validating the implementation
   - Transitioning from implementation to operationalization
   - Documenting and reporting the implementation process
9. **Conclusion and Q&A**
   - Recap of key learnings
   - Open forum for questions and discussion

3. NIST Cybersecurity Framework 2.0 Lead Auditor

Duration: 2 Days

Course Overview:

This course is intended for professionals who will lead audits of the NIST Cybersecurity Framework 2.0 within their organizations or as external auditors. Participants will learn how to assess and evaluate the implementation and effectiveness of the NIST CSF 2.0.

Course Objectives:

- Gain a deep understanding of the NIST CSF 2.0.
- Learn how to conduct comprehensive audits of the NIST CSF implementation.
- Develop skills to evaluate the effectiveness of cybersecurity practices against the framework.
- Learn how to report findings and provide actionable recommendations.

Course Outline:

1. **Introduction and Overview**
    - Introduction to auditing principles
    - Overview of NIST CSF 2.0 and its importance in cybersecurity audits
    - Role of a Lead Auditor
2. **Understanding the Audit Process**
    - Planning the audit: Scope, objectives, and criteria
    - Developing an audit plan and checklist
    - Preparing audit documentation
3. **Conducting the Audit**
    - Gathering and analyzing evidence
    - Techniques for interviewing and inspecting documents
    - Assessing compliance with NIST CSF functions, categories, and subcategories
4. **Evaluating Effectiveness**
    - Measuring the maturity of cybersecurity practices
    - Identifying gaps and areas of improvement
    - Risk-based approach to auditing
5. **Interactive Audit Simulation**
    - Conducting a simulated audit
    - Hands-on practice with audit tools and techniques
6. **Reporting the Audit Findings**
    - Documenting audit results
    - Creating actionable audit reports
    - Communicating findings to stakeholders
7. **Follow-up and Continuous Monitoring**
    - Post-audit activities: Corrective actions and follow-up audits
    - Establishing a continuous monitoring process
    - Integrating audit findings into the continuous improvement cycle
8. **Challenges and Best Practices**
    - Common challenges in NIST CSF audits
    - Best practices for effective auditing
9. **Conclusion and Q&A**
    - Recap of key learnings
    - Open forum for questions and discussion