8 Days

NIST CSF Course

The NIST Cybersecurity Professional (NCSP) is an accredited training program that teaches organizations how to rapidly design, operationalize and automate the NIST Cybersecurity Framework informative reference controls and management systems required to deliver the business outcomes expected by executive management, government regulators, and industry auditors.

Course Details

Course Outline

Domain 1: Digital Transformation Becoming Digital

Lesson: Basics of Digital Transformation What is Digital Transformation?

- Transformation – Industrial to Digital Era Digital Transformation & Critical Infrastructure
- Digital Transformation: Attributes of the Digital Enterprise

Lesson: Becoming Digital

- Digital Transformation from the Corner Office Becoming “Digital”
- Optimized Rate of Change
- Outside-in, Putting Customers First Transforming the Enterprise

Lesson: Cybersecurity & Digital Transformation Role of Cybersecurity in Digital Transformation Cybersecurity & Critical Infrastructure

- Digital Transformation: Basic Principles (THRIVE) Digital Transformation Impacts Many Areas Cybersecurity: Key DX Challenges

Lesson: DX & Using the Framework

- Digital Transformation & NIST Cybersecurity Framework (CSF) Basic Review of CS Practices
- Establish or Improve CS program
- Communicate CS Requirements with Stakeholders Buying Decisions
- Identify for New or Revised Informative References Methodology to Protect Privacy & Civil Liberties

Domain 2 : Understanding Cyber Risks

Lesson: Cyber Risk Equation The Problem

- Profile of an Attack Phases of the Kill Chain
- MITRE ATT&CK™ Framework
- MITRE Enterprise ATT&CK™ Framework The Cyber Risk Equation
- Evaluating the Results – What does it all mean?

Lesson: Cyber Risk Components Cyber Risk Components: Threats Threats

- Cyber Risk Components: Business & Technical Vulnerabilities Vulnerabilities
- Cyber Risk Components: Assets & Information Asset Value
- Cyber Risk Components: Controls Controls

- Cyber Risk: Fighting Back Risk

Lesson: Basics of Cyber Risk Assessment Risk Assessments

- Risk Management Process Frame the Risk
- Assess the Risk Respond to the Risk Monitor the Risk Key Risk Concepts
- Risk Framing Components & Relationships Organizational Risk Frame

Domain 3 : NIST Cybersecurity Framework Fundamentals

Lesson: NIST-CSF Overview Cybersecurity Framework: Origins Key Attributes of NIST- CSF

- The Framework is for Organizations The Framework Components
- NIST Cybersecurity Framework Components NIST Cybersecurity Framework as a Guide The Key Areas of Focus
- Why Adopt the NIST CSF? Benefits of Adopting NIST-CSF Evolution of NIST-CSF

Lesson: Framework Core, Tiers & Profiles NIST-CSF Core Functions

- Core Function: Goals and Objectives Framework Core Approach
- NIST-CSF Tier
- NIST-CSF Implementation Tiers
- Key Properties of Cyber Risk Management Implementation Tiers Approach Implementation Tiers Example
- NIST CSF Framework Profiles Thinking about a Profile Profile Information Input Seven-Step Process
- Core, Tiers, Profiles Example

Domain 4 : Core Functions, Categories & Subcategories Organizational Cybersecurity Capabilities

Lesson: Identify

- Core Function Identify - Purpose, Goals & Objectives Identify: Framework Categories
- Core Function Identify: Subcategories (AM & BE) Core Function Identify: Subcategories (GV & RA) Core Function Identify: Subcategories (RM & SC)

Lesson: Protect

- Core Function Protect - Purpose, Goals & Objectives Protect: Framework Categories
- Core Function Protect: Subcategories (AC & AT) Core Function Protect: Subcategories (DS)
- Core Function Protect: Subcategories (IP)
- Core Function Protect: Subcategories (MA & PT)

Lesson: Detect

- Core Function Detect - Purpose, Goals & Objectives Detect: Framework Categories
- Core Function Detect: Subcategories (AE & CM) Core Function Detect: Subcategories (DP)
- Lesson: Respond
- Core Function Respond - Purpose, Goals & Objectives Respond: Framework Categories
- Core Function Respond: Subcategories (RP & CO) Core Function Respond: Subcategories (AN, MI & IM))

Lesson: Recover

- Core Function Recover - Purpose, Goals & Objectives Recover: Framework Categories
- Core Function Recover: Subcategories (RP, IM & CO)

Lesson: Informative References Informative References

- Tailor to Suit
- Exploring CIS 20 Controls CIS Controls Overview
- CIS Controls – Key Principles for v7.1 CIS Controls-v7
- Basic - CIS Controls 1 to 6
- CIS-01 to 06 Mapped to NIST Core Functions Foundational - CIS Controls 7 to 11 Foundational - CIS Controls 12 to 16
- CIS-07 to 16 Mapped to NIST Core Functions Organizational – CIS Controls 17 to 20
- CIS-17 to 20 Mapped to NIST Core Functions

Domain 5 : Implementation Tiers & Profiles Understanding Current & Future Capabilities

Lesson: Understanding Tiers

- NIST Cybersecurity Framework – Tiers Implementation Tiers Implementation Tier Objectives
- Tier 1: Partial
- Tier 2: Risk Informed Tier 3: Repeatable
- Tier 4: Adaptive
- Risk Management Practices

Lesson: Understanding Profiles Developing Framework Profiles Profiles

- Framework Profiles Profile – An Example

Lesson: Creating Profiles

- Using the Risk Assessment to Create the Profile Identify Function: Asset Management Profile Protect Function: Data Security
- Detect Function: Detection Process Respond Function: Analysis
- Recover Function: Recovery Planning

Domain 6 : Cybersecurity Improvisation

Lesson: Adopt & Adapt

- Adopt – the Decision to Move Forward with NIST-CSF Adapt – Tailor NIST to Your Context
- Principles of Adaptation Customer Drives Value Start Where You Are Simplify Everything
- Adopt & Apply Systems Thinking Change is an Organizational Capability Technology is a Means, Not an End Create to Overcome Entropy

Lesson: Implement & Improve Fast Track™ Concepts

- NCSF-Fast Track TM Controls (NCSF-FT) Fast Track TM – Implement/Improve Cycles
- Adaptive Approach Reduces Waste, Delivers Value

Lesson: Continual Implementation & Improvement System (CIIS) as a Practice CIIS Approach

- Seven Step Approach Step 1: Prioritize & Scope Step 2: Orient
- Step 3: Create a Current Profile Step 4: Conduct a Risk Assessment Step 5: Create a Target Profile
- Step 6: Determine, Analyze, & Prioritize Gaps Step 7: Implement Action Plan

464, Udyog Vihar Phase
V,Gurgaon (Delhi
NCR)-122016,India

+91 8882 233 777

training@mercury.co.in

www.mercurysolutions.co

Date - May 20, 2025