NIST Cybersecurity Framework (CSF) Implementation Workshop Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

NIST Cybersecurity Framework (CSF) Implementation Workshop Training Course provides an essential roadmap for organizations seeking to master the NIST Cybersecurity Framework (CSF) and build a robust, adaptive cyber resilience strategy. The training is specifically designed to transition from theoretical concepts to practical implementation, guiding participants through the latest CSF 2.0 structure, including the new Govern function. In today?ÇÖs complex digital landscape, characterized by escalating supply chain risks, pervasive cloud security challenges, and stringent cybersecurity compliance mandates, adopting a standardized, risk-based approach is non-negotiable. This workshop is your essential toolkit for assessing your current cybersecurity posture, developing a strategic Target Profile, and implementing the necessary security controls across the five core functions: Identify, Protect, Detect, Respond, and Recover, ensuring effective risk management and proactive threat mitigation.

The program emphasizes a Zero Trust architecture mindset and operationalizing the CSF across all business units, moving beyond IT-centric security to holistic enterprise risk management. Participants will gain the skills to leverage the CSF as a powerful communication tool to align executive leadership and technical teams on cyber risk appetite and security investment priorities. Through real-world case studies and hands-on exercises, attendees will learn to practically apply the Framework's Implementation Tiers to measure and continuously improve their security maturity, ultimately strengthening their critical infrastructure protection and overall digital trust in the face of sophisticated, evolving threats.

Programme Curriculum

NIST Cybersecurity Framework (CSF) Implementation Workshop Training Course

Introduction

NIST Cybersecurity Framework (CSF) Implementation Workshop Training Course provides an essential roadmap for organizations seeking to master the NIST Cybersecurity Framework (CSF) and build a robust, adaptive cyber resilience strategy. The training is specifically designed to transition from theoretical concepts to practical implementation, guiding participants through the latest CSF 2.0 structure, including the new Govern function. In today?ÇÖs complex digital landscape, characterized by escalating supply chain risks, pervasive cloud security challenges, and stringent cybersecurity compliance mandates, adopting a standardized, risk-based approach is non-negotiable. This workshop is your essential toolkit for assessing your current cybersecurity posture, developing a strategic Target Profile, and implementing the necessary security controls across the five core functions: Identify, Protect, Detect, Respond, and Recover, ensuring effective risk management and proactive threat mitigation.

The program emphasizes a Zero Trust architecture mindset and operationalizing the CSF across all business units, moving beyond IT-centric security to holistic enterprise risk management. Participants will gain the skills to leverage the CSF as a powerful communication tool to align executive leadership and technical teams on cyber risk appetite and security investment priorities. Through real-world case studies and hands-on exercises, attendees will learn to practically apply the Framework's Implementation Tiers to measure and continuously improve their security maturity, ultimately strengthening their critical infrastructure protection and overall digital trust in the face of sophisticated, evolving threats.

Course Duration

10 days

Course Objectives

Upon completion of this workshop, participants will be able to:

1. Establish and align cybersecurity risk management with organizational mission and enterprise risk strategies.
2. Conduct a gap analysis between a Current Profile and a desired Target Profile using the CSF Core.
3. Integrate SCRM principles across all CSF Functions to mitigate third-party vulnerabilities.
4. Utilize the CSF's Implementation Tiers to mature and prioritize security investments.
5. Develop and maintain comprehensive asset management and vulnerability assessment programs.
6. Deploy protective controls for data-at-rest and data-in-transit, addressing data governance requirements.
7. Map Zero Trust principles to the Protect function, focusing on micro-segmentation and robust access control.
8. Implement continuous monitoring and establish Security Operations Center (SOC) processes aligned with the Detect function.
9. Formulate and practice a structured, scalable response to cyber events using the Respond function.
10. Implement strategies for data backup and system restoration to ensure rapid disaster recovery.
11. Effectively convey risk levels and security requirements to executive leadership and non-technical stakeholders.
12. Map CSF controls to major compliance standards like ISO 27001, HIPAA, or CMMC
13. Define metrics and key performance indicators (KPIs) for ongoing program optimization and maintaining an Adaptive security state.

Target Audience

1. Chief Information Security Officers / Chief Information Officers
2. Information Security Managers & Analysts
3. IT Risk Management and Compliance Professionals

4. Business Continuity and Disaster Recovery Specialists
5. Internal and External IT Auditors
6. Program/Project Managers leading cybersecurity initiatives
7. Non-technical Executive Leadership responsible for risk decisions
8. Critical Infrastructure Personnel

Course Modules

1. Introduction to the NIST CSF 2.0 & Governance

- Overview of the CSF Structure.
- Understanding the Govern Function.
- Mapping Legal, Regulatory, and Contractual Requirements to the CSF.
- The role of the Implementation Tiers in maturity assessment.
- Case Study: Governing Risk at a Financial Institution.

2. Identifying Organizational Assets & Risks

- Developing a complete Asset Inventory
- Conducting a structured Risk Assessment methodology using CSF criteria.
- Establishing a Cybersecurity Policy framework and communication strategy.
- Categorizing and classifying information systems and data based on business criticality.
- Case Study: Critical Asset Identification in a Manufacturing Plant.

3. Protect: Access Control and Authentication

- Implementing foundational Identity and Access Management controls.
- Strategies for deploying Multi-Factor Authentication and password hygiene.
- Least Privilege principle and network segmentation techniques.
- Managing user access reviews and privileged access management
- Case Study: Implementing Zero Trust in a Remote Workforce.

4. Protect: Data Security and Information Protection

- Data classification, labeling, and handling procedures.
- Implementing encryption methods for data-at-rest and data-in-transit.
- Securing data backup and data loss prevention strategies.
- Secure configuration and patch management for all system components.
- Case Study: Securing Healthcare Data.

5. Protect: Awareness, Training, and Protective Technology

- Developing a **Role-Based Security Awareness Program**.
- Implementing **phishing simulation** and social engineering training.
- Selecting and deploying protective technologies
- Personnel security and supply chain risk communication.
- **Case Study:** Mitigating Insider Threat via Awareness.

6. Detect: Continuous Monitoring and Anomaly Detection

- Establishing Continuous Monitoring programs for network and endpoints.
- Defining and collecting security logs and event data.

- Implementing threat intelligence feeds and vulnerability scanning.
- Identifying and analyzing anomalies to uncover potential cyber incidents.
- Case Study: Optimizing a SOC for Proactive Detection.

7. Respond: Incident Response Planning

- Developing a formal Incident Response Plan and playbook creation.
- Defining roles, responsibilities, and communication protocols
- Techniques for incident analysis, containment, and eradication.
- The importance of tabletop exercises and post-incident review.
- Case Study: Ransomware Incident Response Drill.

8. Respond: Communication and Analysis

- Crisis communication strategies with stakeholders, regulators, and customers.
- Conducting forensic analysis and data preservation for legal requirements.
- Learning from incidents and implementing corrective actions.
- Coordinating response activities with external partners and law enforcement.
- Case Study: Managing Public Relations Post-Breach.

9. Recover: Recovery Planning and Resilience

- Establishing a Disaster Recovery and business continuity strategy.
- Restoring systems and data consistent with the recovery plan.
- Prioritizing recovery efforts based on business impact analysis.
- Documenting and communicating recovery activities to stakeholders.
- Case Study: Post-Disaster System Restoration.

10. Creating the CSF Profile: Gap Analysis

- Steps for building a Current Profile
- Defining the Target Profile
- Performing a Gap Analysis to identify deficiencies in the security program.
- Prioritizing gap remediation based on risk and business need.
- Case Study: Gap Analysis for a Mid-Sized Tech Firm.

11. CSF Implementation Roadmapping and Action Planning

- Developing a prioritized, multi-year cybersecurity roadmap.
- Integrating CSF implementation with existing risk management frameworks.
- Estimating resources, budget, and staffing requirements.
- Establishing a program management structure for CSF adoption.
- Case Study: Building a Phased Implementation Plan.

12. Integrating CSF with Other Standards

- Understanding the relationship between the CSF and ISO/IEC 27001
- Mapping CSF controls to specific CMMC practices and maturity levels.
- Leveraging the CSF for compliance with GDPR, CCPA, and other privacy laws.
- Utilizing NIST SP 800-53 as an informative reference for control implementation.
- Case Study: Dual Compliance Strategy for Defense Contractor.

13. Cybersecurity Risk Metrics and Reporting

- Defining effective Key Performance Indicators and Key Risk Indicators.
- Developing a clear, concise reporting structure for executive leadership.
- Measuring the effectiveness of implemented security controls.
- Using metrics to drive continuous improvement and security funding decisions.
- Case Study: Executive Dashboard Design.

14. Supply Chain Risk Management with CSF

- Identifying and assessing cybersecurity risks posed by third-party vendors.
- Integrating SCRM activities across the Identify and Protect Functions.
- Developing vendor security questionnaires and contractual requirements.
- Ongoing monitoring and oversight of supply chain partners.
- Case Study: Mitigating the Third-Party Vendor Risk.

15. The Future of CSF: Emerging Trends and Technology

- Addressing Cloud Security challenges within the CSF framework.
- Integrating AI/ML for enhanced threat detection and response.
- The role of the CSF in securing Operational Technology environments.
- Preparing for future updates and the evolution of the cybersecurity threat landscape.
- Case Study: Securing an Industrial IoT Deployment.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com