CERTIFIED NIST CYBERSECURITY FRAMEWORK LEAD IMPLEMENTER

3-Day Seminar

Prior attendance of ISO 31000 or ISO 27005 risk management training is encouraged, but not required.

CPE Credit Hours: ***24***

For currently scheduled seminars please see
www.certifiedinfosec.com
+1 (888) 547-3481 (USA)
+1 (904) 406-4311

This course can be arranged as a private on-site training session at up to a 40% discount from public session fees.

Get trained as an expert in planning, deploying and managing cybersecurity according to the NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States and around the world can assess and improve their ability to prevent, detect, and respond to cyber attacks. It has been translated to many languages, and is used by the governments of Japan and Israel, among others.

The NIST CSF is now the go-to playbook for countless organizations for building a robust data protection strategy. It's structured along five core functions — Identify, Protect, Detect, Respond and Recover — each of which captures and curates the essential goals and actions that should be prioritized across the cybersecurity lifecycle.

What does NIST CSF deliver for an organization?

The CSF helps make sense of what to do before, during, and after an incident: from shedding light on your data ecosystem and where the vulnerabilities lie; to locking down sensitive data and remediating known risks; to detecting malicious activity and meeting the threat with consistent and repeatable processes; to finally recovering through the quarantine of corrupted data, monitoring of ongoing threat activity, protocol adjustment and related steps.

The beauty is that all this guidance and wisdom comes in the form of a few strategic guidelines that are intuitive and accessible to a wide range of practitioners. Of course, not everything about NIST is voluntary for all organizations (U.S. government contractors, for example, must demonstrate security compliance under NIST 800-171 or risk losing their contracts), and regulations are always changing. That's why the CSF is still the roadmap to drive your organization toward the most secure data and architectures possible.

Become a NIST CSF Lead Implementer

The Certified NIST CSF LI certification certifies your ability to implement the formal structure, governance, and policy of a robust cybersecurity framework following internationally recognized and respected NIST best practices and standards. Get trained and certified as an expertin developing, implementing, and managing a robust cybersecurity program according to internationally adopted NIST CSF governance and management best practices.

Upon completion of this training and certificate program, participants will:

- Be equipped with knowledge and skills required to manage, monitor, and improve NIST Cybersecurity Framework policy and program in line with the NIST CSF 1.1 and related standards of best practice;
- Expand your cybersecurity competency; and
- Be prepared to integrate a robust NIST Cybersecurity program into an ISO 27001 Information Security Management System (ISMS).

Course Content Details

1. Framework Core Functions

- Identify
- Protect
- Detect
- Respond
- Recover

2. Framework Implementation Tiers (Cyber Security Risk Management)

3. Framework Profiles

4. Converging the CSF Framework into an ISO 27001 Information Security Management System

Who should attend

- Policy Approvers / Strategy Decision Makers
- Chief Information Officer (CIO / CISO)
- Information security / cybersecurity professionals
- IT Managers
- Risk managers
- Business continuity managers
- Facilities managers
- Operations department heads (business unit managers)
- Auditors