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.

# CERTIFIED NIST CYBERSECURITY FRAMEWORK 2.0 LEAD IMPLEMENTER

## Get trained as an expert in planning, deploying and managing cybersecurity according to the NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework 2.0 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 2.0 is the go-to playbook for countless organizations for building a robust data protection strategy. It's structured along six core functions — Govern, 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 2.0 deliver for an organization?

The CSF 2.0 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.

## Become a NIST CSF 2.0 Lead Implementer


The Certified NIST CSF 2.0 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.

## 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 2.0 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**
   - Govern
   - Identify
   - Protect
   - Detect
   - Respond
   - Recover
2. **Framework Profiles**
3. **Risk Communication and Integration**
4. **Framework Tiers (Cyber Security Risk Management)**
5. **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

# CERTIFIED NIST CYBERSECURITY FRAMEWORK 2.0 LEAD AUDITOR

2-Day Seminar

Recommended Pre-Requisite Training: ***None***

CPE Credit Hours: ***16***

Available as a private on-site engagement for groups of 10 or more participants.

www.certifiedinfosec.com
+1 (888) 547-3481 (USA)
+1 (904) 406-4311

## Get trained as an expert in assessing and auditing cybersecurity according to the NIST Cybersecurity Framework 2.0

Assessing the organization's cybersecurity program against the key capabilities and objectives is the cornerstone of cybersecurity improvement and optimization. Internal and external stakeholders have a vested interest in managing cyber risk, and measuring the organization's cybersecurity processes, procedures, and controls against desired cybersecurity objectives provides the basis for identifying critical risk exposures and opportunities for improvement.

NIST CSF 2.0 now provides 103 desired cybersecurity outcomes/objectives along with 367 implementation recommendations. In two short days, our certified NIST CSF 2.0 expert will lead you and your team through a hands-on assessment of these very implementation tasks.

## NIST CSF 2.0 Core desired outcomes can also be assessed for maturity of Execution

Trying to assess a cybersecurity objective or desired outcome as simply "Incomplete", "Partially Complete", or "Complete" does not fully capture how mature the recommended tasks are implemented. Were a given cybersecurity objective and its corresponding implementation tasks well-planned? Were the tasks driven by documented policy? Were the implementation policy and procedures standardized throughout the organization, or do they differ from one department to another? Are metrics used and monitored to identify opportunities for improvement? These are some of the questions we should also consider as we assess every desired outcome and control objective's level of maturity of execution. Determining Maturity Indicator Levels (MIL) is a critical part of a cybersecurity review, and your instructor will provide the seasoned guidance you and your fellow assessors/auditors need to perform the assessment properly.

## Become a NIST CSF 2.0 Lead Auditor


The Certified NIST CSF 2.0 LA credential certifies your ability to assess and audit a robust cybersecurity framework following internationally recognized and respected NIST best practices and standards.

## 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 2.0 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).

## Who should attend

Participation is recommended for:

- 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