

CERTIFIED NIST CYBERSECURITY FRAMEWORK 2.0 LEAD AUDITOR

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.

The NIST CSF 2.0 Lead Auditor certification is a stacking credential **that requires current CIS Certified NIST CSF 2.0 Lead Implementer certification as a prerequisite for Lead Auditor certification eligibility**. The Lead Auditor program extends this knowledge with an advanced understanding of how to assess and audit the 103 goals and objectives of NIST CSF 2.0 and its 367 corresponding recommended implementation tasks.

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

- Be equipped with knowledge and skills required to audit NIST Cybersecurity Framework policy and program in line with the NIST CSF 2.0 and related standards of best practice;
- Expand your cybersecurity competency

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

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

For more information, please contact Certified Information Security

Toll Free: (888) 547-3481 • Tel: +1 (904) 406 4311 • Fax: +1 (786) 522-9063 • info@certifiedinfosec.com

Certification Application



The NIST Cybersecurity Framework 2.0 provides a policy framework of computer security guidance for how public and private sector organizations in the United States and around the world can assess and improve their ability to prevent, detect, and respond to cyberattacks. The framework has been translated to many languages, and is used by the governments of Japan and Israel, among others. It is now 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.

The NIST CSF 2.0 Lead Auditor certification is available to qualified candidates who:

1. **Are a member of CIS in good standing.** If you are not already an Associate member of the CIS certification student body, you must first become a member to pursue the NIST CSF 2.0 LI credential. Please see www.certifiedinfosec.com/estore/cis-membership/cis-body-of-certified-professionals-detail for further details.
2. **Have achieved and maintain professional accreditation as a CIS Certified NIST CSF 2.0 Lead Implementer.** The NIST CSF 2.0 Lead Auditor certification is a stacking credential that requires current CIS Certified NIST CSF 2.0 Lead Implementer certification as a prerequisite for Lead Auditor certification eligibility.
3. **Attend the required CIS approved curriculum course, NIST CSF 2.0 Lead Auditor Training.** Seminars may be attended at [live instructor-led sessions](#), OR [online](#).
4. **Pass the NIST CSF 2.0 Lead Auditor Exam.** For NIST CSF LA Professional certification, candidates must pass CIS online exam #CSF102. CIS exams are administered online and can be taken at your convenience at your home or work through the CIS Learning Center, where your progress and score are monitored and recorded centrally. Your exam results are provided to you automatically upon completion of your exam.
5. **Submit this application kit to the Certification Department at certification@certifiedinfosec.com**

