INFORMATION SECURITY

3-Day Seminar + 2-Day CSF Gap Assessment Audit Lab

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 LEAD IMPLEMENTER + CYBER RESILIENCE REVIEW

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

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

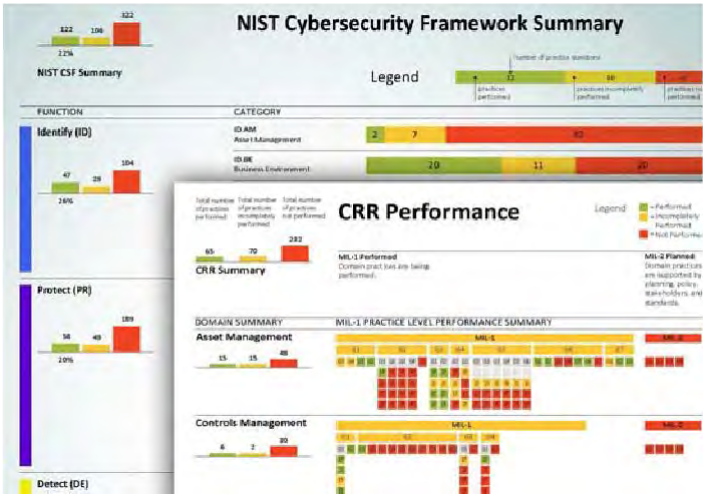
Homeland Security

CYBER RESILIENCE REVIEW

APPROACH

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's capacities and capabilities in performing, planning, managing, measuring and defining cybersecurity capabilities across 10 domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness



The CRR results can be used to assess your organization's capabilities against the Cybersecurity Framework.

PARTICIPANTS

To conduct a CRR, DHS recommends that you involve a cross-functional team representing business, operations, security, information technology, and maintenance areas, including those responsible for the functions shown in the following table:

IT Policy and Governance (e.g., Chief Information Security Officer)	Business Operations (e.g., Operations Manager)
IT Security Planning and Management (e.g., Director of Information Technology)	Business Continuity and Disaster Recovery Planning (e.g., BC/DR Manager)
IT Infrastructure (e.g., Network/System Administrator)	Risk Management (e.g., Enterprise/Operations Risk Manager)
IT Operations (e.g., Configuration/Change Managers)	Procurement and Vendor Management (e.g., Contracts and Legal Support Managers)

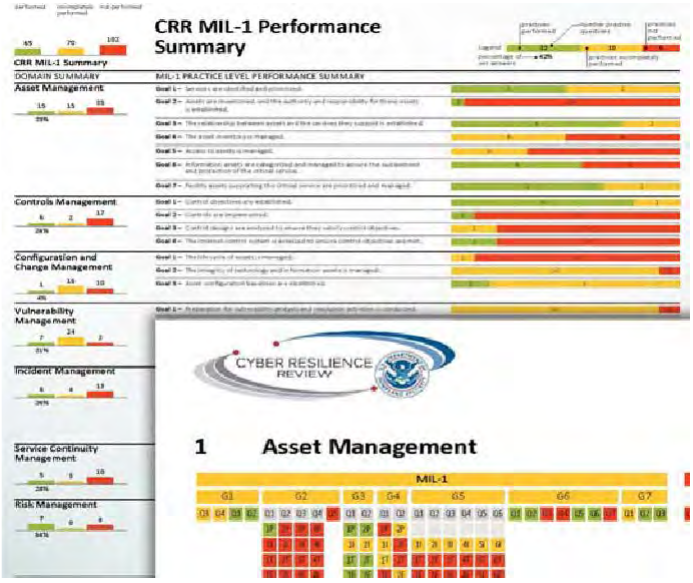
Homeland Security

BENEFITS AND OUTCOMES

The CRR provides a better understanding of an organization's cybersecurity posture. The review provides an improved organization-wide awareness of the need for effective cybersecurity management; a review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis; a verification of management success; a catalyst for dialog between participants from different functional areas within your organization; and a comprehensive final report that maps the relative maturity of the organizational resilience processes in each of the 10 domains, and that includes improvement options for consideration, using recognized standards and best practices as well as references to the CERT- RMM.

ASSOCIATION TO THE CYBERSECURITY FRAMEWORK

The principles and recommended practices within the CRR align closely with the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). After performing a CRR, your organization can compare the results to the criteria of the NIST CSF to identify gaps and, where appropriate, recommended improvement efforts. A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR self-assessment kit. An organization's assessment of CRR practices and capabilities may or may not indicate that the organization is fully aligned to the NIST CSF.



A final report will graphically map your organization's results and provides improvement options for consideration.

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

EXPERT CRR ASSESSMENT FACILITATION

Performing a CRR against the NIST CSF is an ideal way to get started with establishing or improving enterprise-wide cyber security governance and best practices based on the NIST Cybersecurity Framework. Certified Information Security's Cyber qualified security assessors have been trained by official DHS Security assessors to facilitate private CRR question-based assessments for organizations otherwise not eligible for DHS facilitation.

Learn more at [https://www.certifiedinfosec.com/services/advisory/nist-csf-cyber-resilience-review-assessment.](https://www.certifiedinfosec.com/services/advisory/nist-csf-cyber-resilience-review-assessment)