NISTCSF Practitioner Training
Course Description & Outline

The NIST CSF Practitioners Course explains in detail current security challenges, and how organizations design, build, maintain and test a comprehensive Cybersecurity Program and Risk Management Program based on the NIST Cybersecurity Framework. The NIST CSF Practitioners Course includes detailed capabilities organizations can use to build a comprehensive program.

IS THIS COURSE RIGHT FOR YOU OR YOUR STAFF?

Do you want to:

- Understand the innovation economy and key threats and challenges
- Understand the risk equation including threats, vulnerabilities, assets / identities, and controls
- Learn the difference between managed and unmanaged assets
- Build your knowledge of the NIST Cybersecurity Framework
- Understand the Controls Factory Model and key components including the Engineering Office, Technology Center, and Business Office
- Learn how implementing security technologies and establishing operational and management practices reduce cybersecurity risk.

WHAT'S IN IT FOR YOU?

What is covered:

The NIST CSF Practitioners training course outlines challenges surrounding critical infrastructure sector security and explains how implementing a security program based on the NIST Cybersecurity Framework can help organizations mitigate these issues.

Key areas of discussion include:

- Control costs and gain real-world insights on security best practices
- Understand the NIST CSF and related technical and business controls.
- Drive security controls and best practices across your business

COURSE DELIVERY

Course content is delivered as:

- Self-paced eLearning course
- Hosted three-day, on-site instructor-led training

You will earn fifteen (24) Continuing Professional Education (CPE) hours for the eLearning course or instructor-led option. There is an exam qualification associated with this course.

WHO SHOULD ATTEND?

Geared to practitioners including IT Operations Managers and Staff, IT Audit Managers and Staff, IT Risk managers and Staff, IT Compliance Managers and Staff, IT Applications and Business Management, etc. This course is for those individuals that are responsible for designing, building and operating an organizations Cybersecurity or Risk Management Program.

Perquisites – CISSP, Security+, CISA or CISP certification

Typical job titles include:

- IT Audit Manager or Specialist
- IT Business Analyst
- IT Compliance Officer
- Human Resource Manager
- Finance Manager
- IS Manager
- IT Specialist
- Project/Program Manager
- Risk Manager
- Risk Analyst
- Security Manager
- Security Analyst
- Senior Developer
- Software Engineer
- System Administrator
- Application Administrator

WHAT'S COVERED IN THE COURSE?

This course helps improve security, reduce the risk of data loss / compromise, and improve security controls for an organization:

- Detailed understanding of the NIST Cybersecurity Framework and the key deliverables including core functions, implementation tiers, and security profiles
- Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.
- Framework Core Functions include cybersecurity activities, desired outcomes, categories, subcategories, and applicable references common across critical infrastructure sectors.
- Framework Profile represents outcomes based on business needs the organization selects from Framework Categories and Subcategories.
- The Profile is characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.
- Understand the Controls Factory Model that organizations can use to better understand how the NIST Cybersecurity framework can be used to implement technical and business controls.
- Understand the key components of the Controls factory including the Engineering Office, Technology Center and Business Office.

Upon completion of the course, you will be able to:

- Understand the key elements of risk including threats, vulnerabilities, controls and assets / identities
- Understand differences between managed and unmanaged assets
- Understand the NIST Cybersecurity Framework capabilities
- Understand the Controls Factory Model and deliverables
- Have tools and insight to build a Cybersecurity Program
- Have tools and insight to build a Risk Management Program