# NIST Foundation

Powered By APMG Accredited NIST Cybersecurity Professional (NCSP) Curriculum.

In response to the accelerating set of security risks and threats to critical infrastructure sectors, the US Government's National Institute for Standards and Technology (NIST) was directed to create a cybersecurity framework (CSF) for public and private organizations to use to assess their security practices and controls and to support continual improvement. The NIST cybersecurity framework (NCSF) was published in 2014 and critical infrastructure sectors are expected to adopt these practices no later than 2022.

This APMG accredited training program is targeted at IT and Cybersecurity professionals looking to become certified on how to adopt the NIST Cybersecurity Framework (NCSF) across an enterprise and its supply chain. The NIST CSF Foundation training course outlines current cybersecurity challenges and explains how organizations who implement a NCSF program can mitigate these challenges.

**What You Will Accomplish**

- Learn how the NCSF helps you identify, assess, and manage cybersecurity risk
- Learn to develop a roadmap for improving your cybersecurity risk management approach
- Prioritize investments to maximize positive impact
- Learn how to use the Controls Factory Model (CFM) to implement your cybersecurity risk program

**What You Will Accomplish**

- Learn how the NCSF helps you identify, assess, and manage cybersecurity risk
- Learn to develop a roadmap for improving your cybersecurity risk management approach
- Prioritize investments to maximize positive impact
- Learn how to use the Controls Factory Model (CFM) to implement your cybersecurity risk program

**Who Should Attend**

Risk Managers, Security Managers, CISOs, all IT staff with security management responsibilities, business relationship managers, business leadership with responsibility for security practices and assurance.

**Body of Knowledge**

This course is based on the Framework for Improving Critical Infrastructure Cybersecurity, version 1.0. It was published by the National Institute of Standards & Technology on February 12, 2014.

The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It "provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes."

**Course Introduction**

This course introduces the NIST Cybersecurity Framework (NCSF). The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

This course discusses how an organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement.

In addition this course will introduce the cybersecurity Controls Factory™ Model (CFM) developed by Larry Wilson, CISO, UMass President's Office. The CFM provides an organization with an approach to the operationalization of the NIST Cybersecurity Framework based on a modular engineering-based approach. The NIST CSF also provides a 7-step approach for the implementation and improvement of their cybersecurity posture utilizing the NIST CSF.

The class will include lectures, informative supplemental reference materials, quizzes, and tests.

## Course Outline…

1. Course Introduction
2. Doing Business
3. Risk-based Approach
4. The NIST Cybersecurity Framework Fundamentals
5. Core Functions, Categories & Subcategories
6. Implementation Tiers
7. Developing Framework Profiles
8. Cybersecurity Controls Factory™ Model

9. Cybersecurity Improvement – The NIST CSF also provides a 7-step approach for the implementation and improvement of their cybersecurity posture utilizing the NIST CSF.

Exam: The optional certification exam will be comprised of 100 Blooms level 1 & 2 multiple choice questions.

Certification is through APMG. Students must pass a 90-minute, 100 question closed book multiple choice, examination with a passing score of 70% in order to receive this certification.

Onsite program offerings can include a second day NCSF simulation program to help your organization assess your readiness and identify continual improvement areas of focus.