NIST Practitioner Bootcamp

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 NCSF Practitioner program teaches the knowledge to prepare for the NCSF Practitioner exam plus the skills and abilities to design, build, test, manage and improve a cybersecurity program based on the NCSF.

What You Will Accomplish

- Learn how the NCSF helps you identify, assess, and manage cybersecurity risk
- Learn to develop a roadmap and scorecard for assessing and improving your cybersecurity risk management approach
- Develop engineering, technology, and business centers to implement the Controls Factory Model
- Prioritize investments to maximize positive impact
- Build cybersecurity and cyber risk scorecards and roadmaps
- Be able to answer the question – are we secure?

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 APMG and NCSC/GCHQ accredited five (5) day in-depth course teaches students how to apply a best practice approach to designing an enterprise risk management cybersecurity program based on the NIST Cybersecurity Framework Informative references and management systems.

The course is based on the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 and qualifies for PMI, CompTIA and ISACA Professional Development Credits

Following the course introduction, the course provides an introduction to the intersection between digital transformation and cybersecurity, which is followed by an overview of the threat landscape.

With this in place, the course uses the Center for Internet Security Controls as an example of a cybersecurity "informative reference" (mentioned in the NIST Cybersecurity Framework. Each organization that sends candidates to the course should select one or more informative references that match the need of the organization (e.g., HIPAA, PCI-DSS, or NIST 800-171).

Following an approach to the implementation of cybersecurity controls, the course delves into an organizational approach to cybersecurity that starts governance, management, and a supportive culture, including an understanding of how things occur within the organization concerning three specific areas: work, communication, and improvement.

Finally, the course provides additional guidance for the cybersecurity practitioner to determine the current state, the desired state, and a plan to close the gap – and to do this over and over again to inculcate it into organizational DNA.

Course Introduction

This course looks at cybersecurity risks and instructs students on the best approach to design and build a comprehensive technology focused cybersecurity program and business focused cyber-risk management program that will minimize risks, and at the same time, protect our critical assets. Executives are keenly aware of the risks, but have limited knowledge on the best way to mitigate these risks. We will want to enable our executives to answer the key question – Are we secure?

The class will include lectures, informative supplemental reference materials, quizzes, exercises and tests. Outcomes and benefits from this class is a practical approach that students can use to build and maintain comprehensive cybersecurity and cyber-risk management programs.

Course Outline…

Chapter 1: Course Overview

Reviews at a high level each chapter of the course.

Chapter 2: Framing the Problem

Reviews the main business and technical issues that we will address through the course.

Chapter 3: The Controls Factory Model

Introduces the concept of a Controls Factory Model and the three areas of focus:

1. the Engineering Center,
2. the Technology Center, and
3. the Business Center.

Chapter 4: The Threats and Vulnerabilities

Provides an overview of cyber –attacks (using the Cyber Attack Chain Model),

1. discusses the top 15 attacks,
2. the most common technical vulnerabilities and,
3. the most common business vulnerabilities.

Chapter 5: The Assets and Identities

Provides a detailed discussion of

1. asset families,
2. key architecture diagrams,

3. an analysis of business and technical roles, and
4. a discussion of governance and risk assessment.

Chapter 6: The Controls Framework
Provides a detailed analysis of the controls framework based on the NIST Cybersecurity Framework. Includes the five core functions (Identify, Protect, Detect, Respond and Recover).

Chapter 7: The Technology Controls
Provides a detailed analysis of the technical controls based on the Center for Internet Security 20 Critical Security Controls©. This section includes:

1. the controls objective,
2. controls design,
3. controls details, and
4. a diagram for each control.

Chapter 8: The Security Operations Center (SOC)
Provides a detailed analysis of Information Security Continuous Monitoring (ISCM) purpose and capabilities. This section includes an analysis of:

1. people,
2. process,
3. technology, and
4. services provided by a Security Operations Center.

Chapter 9: Technical Program Testing and Assurance
Provides a high-level analysis of technology testing capabilities based on the PCI Data Security Standard (DSS). The testing capabilities include all 12 Requirements of the standard.

Chapter 10: The Business Controls
Provides a high-level analysis of the business controls based on the ISO 27002:2013 Code of Practice. Includes:

1. the controls clauses,
2. objective, and
3. implementation overview.

The business controls are in support of ISO 27001 Information Security Management System (ISMS).

Chapter 11: Workforce Development
Provides a review of cybersecurity workforce demands and workforce standards based on the NICE Cybersecurity Workforce Framework (NCWF).

Chapter 12: The Cyber Risk Program
Provides a review of the AICPA Proposed Description Criteria for Cybersecurity Risk Management. Covers the 9 Description Criteria Categories and the 31 Description Criteria.

Chapter 13: Cybersecurity Program Assessment
Provides a detailed review of the key steps organizations can use for conducting a Cybersecurity Program Assessment. Assessment results include:

1. a technical scorecard (based on the 20 critical controls),
2. an executive report,
3. a gap analysis and
4. an implementation roadmap.

Chapter 14: Cyber-risk Program Assessment
Provides a review of the Cyber Risk Management Program based on the five Core Functions of the NIST Cybersecurity Framework. This chapter includes a resource guide by the Conference of State Bank Supervisors (CSBS), “Cybersecurity 101 – A Resource Guide for Bank Executives”. Results include:

1. a sample business scorecard,
2. executive report,
3. gap analysis and
4. an implementation roadmap.

Prerequisites
NIST Foundations certification preferred.

Exam
Optional Exam required for certification. The exam will be comprised of 100 multiple choice questions. Approximately 60% will be Blooms Level 1 & 2 and the remaining 40% will be Blooms Level 3 & 4.

Certification is through APMG. Student must pass a 180-minute, 100 question closed book multiple choice, examination with a passing score of 70% in order to receive

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