NIST CyberSecurity Foundation

Certificate:	NIST CyberSecurity Foundation	**Course ID:**	NIST-CS-F
Duration:	2 days	**Language:**	English
Course Delivery:	Classroom / Virtual Classroom, Exam, eBook	**PMI® PDUs:**	16
Accreditor:	Kepner-Tregoe	**CPEs:**	16.5

The CyberSecurity Foundation course is developed to teach the basic information security concepts and techniques. The knowledge captured and communicated in this course can be immediately applied by organizations around the globe to ramp up to meet their legal obligations defined by newly introduced statutory and regulatory acts. The course consists of five primary modules that address NIST Critical Security Factors which are Identify, Protect, Detect, Respond, and Recover. In addition, the course introduces GAP Assessment and four tiers of capability and maturity created to help organizations plan their CyberSecurity roadmap.

Audience:
The CyberSecurity Foundation course is developed to help business leaders and IT professionals design and plan the adoption of NIST CyberSecurity Framework. For example:

- Risk, security or cyber security managers
- Business process owners
- Business risk managers
- Regulatory compliance managers
- Project managers
- Individuals responsible for cyber security within an organization

Learning Objectives:
Individuals certified at this level will have demonstrated their understanding to:

- Define business environment and plan for governance, risk, and compliance
- Establish access control, raise awareness, and choose protective technologies
- Monitor actively for anomalies and events
- Implement a response plan and apply continuous improvement
- Implement a recovery plan with communications and continuous improvement

Benefits of Taking This Course:
Participants in this course will obtain the following benefits:

- Reduce risks and threats to the Confidentiality, Integrity, and Availability of the Enterprise's CyberSecurity Assets and System Resources by providing policies, practices and standards designed to mitigate or eliminate all known risks and threats.
- Improve the effectiveness and efficiency of CyberSecurity Management by implementing a world class best practice and framework for consistent, concise security administration.
- Improve effectiveness and efficiencies of the existing CyberSecurity mechanisms by formalizing new practices to monitor compliance and maintain sensitive data awareness.
- Improve reassurance testing and validation outcomes by Internal Audit and External Auditors to further assure the Enterprise's Investors, Board of Directors, and Executive Management Team that the Enterprise's CyberSecurity Assets and System Resources are secure.
- Reduce the likelihood of accidental incidents caused by Enterprise's staff that can adversely affect the Enterprise's reputation or liabilities by providing an ongoing CyberSecurity education and awareness program.

Prerequisites:
None

Course Materials:
You will receive the participant handbook (printed or as an eBook).

Examination:
None

Technical Requirements:
For eBooks:

- Internet connection to download the eBook
- Laptop, tablet, Smartphone, eReader (no Kindle)
- Adobe DRM supported software, such as Digital Editions and Bluefire Reader
- eBook download and activation instructions

Agenda:

Day 1	Day 2
1. Course Introduction	1. Preliminary CyberSecurity Framework–Detect
2. Preliminary CyberSecurity Framework–Identify	2. Preliminary CyberSecurity Framework–Respond
3. Preliminary CyberSecurity Framework–Project	3. Preliminary CyberSecurity Framework–Recover

Course Outline:

Preliminary CyberSecurity Framework–Identify: Develop the organization's knowledge of CyberSecurity to enable and empower management to address risk to organizational assets, people, information, software, hardware, telecommunications, and facilities. Key processes include:

- Business Environment
- Risk Management Strategy
- Governance
- Risk Assessment
- Asset Management

Preliminary CyberSecurity Framework–Protect: Design, test, and deploy appropriate safeguards that mitigate CyberSecurity threats to the organizations' operations and services. Key processes include:

- Data Security
- Protective Technology
- Information Protection Processes and Procedures
- Access Control
- Awareness Training
- Maintenance

Preliminary CyberSecurity Framework–Detect: Design and implement effective tools that will actively monitor the organizations' operations and services to identify events before they develop into a security incident. Key processes include:

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Preliminary CyberSecurity Framework–Respond: Plan, test, and operationalize CyberSecurity event and incident management processes. Train security teams to effectively engage CyberSecurity threats and test the organization's response to events and incidents. Key processes include:

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Preliminary CyberSecurity Framework–Recover: Plan, test, and deploy recovery processes that will quickly return the organization to full operational capacity. Train employees designated to participate in the recovery team ensuring a smooth seamless transition from Cyber Security incidents to full operational capacity. Key processes include:

- Recovery Planning
- Improvements
- Communications

Follow-on Courses:

- CISM, CGEIT, CRISC, CISA
- ISO /IEC 27001 Lead Auditor
- Security Architecture
- Service Management ITIL
- Certified Information Systems Security Professional (CISSP)
- Preparation Certified Ethical Hacker (CEH)
- CompTIA Security+ Service Oriented Architecture (SOA) for Security Professionals
- Certified Wireless Network Administrator (CWNA)
- Certified Wireless Security Professional (CWSP) Certified Wireless Technical Specialist (CWTS)
- Wireless Analysis & Exploitation (WAX)
- Computer Hacking Forensic Investigator (CHFI)
- Operational CyberSecurity EC-Council Certified Security Analyst (ECSA) Network & Packet Analysis EC-Council Network Security Administrator (ENSA) Network Defense
- CISSP® - ISSEP® - Information Systems Security Engineering Professional CompTIA Linux+ Certification Prep System Security Certified Practitioner (SSCP)
- Malware Analysis (Triage)
- Metasploit Framework Penetration Testing Methodology Java Development for Secure Systems Securing Java Web Applications Securing Java Web Services CYBR 691
- Applied Network Security Certified Information Systems Security Professional (CISSP)
- Preparation Online Cyber Insider Threat Metasploit® Framework, Penetration Testing Methodology & Malware Analysis (Triage)