Hewlett Packard
Enterprise

Course data sheet

# NCSP Boot Camp Certification, Rev.20.21 H0DV9AAE

| | |
|---|---|
| **HPE course number** | H0DV9AAE |
| **Course length** | 16 Hours |
| **Delivery mode** | WBT |
| **View schedule, local pricing, and register** | **View now** |
| **View related courses** | **View now** |

**Why HPE Education Services?**

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

The NCSP Certification Training Programs are the industry's first accredited cybersecurity certification training programs based on the NIST Cybersecurity Framework (NIST-CSF).

The Boot Camp program combines the NCSP Foundation and Practitioner programs into one course, supported by one certification exam.

The NCSP Certification Training Programs teach organizations how to:
• Assess an organization's cybersecurity capabilities in order to understand its current cybersecurity state
• Design a cybersecurity program using NIST-CSF informative reference controls to realize its future cybersecurity state
• Implement and operationalize a Continual Implementation and Improvement Management System (CIIS) to automate, sustain and continually improve its future cybersecurity state

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

## Audience

- Cybersecurity engineers
- Cybersecurity specialists, examples include:
  - Pen testers
  - Ethical hackers
- IT operations
- Software and application developers
- Digital transformation
- Business risk professionals
- ITauditors
- Business professionals—lawyers, accountants
- Candidates wishing to pursue a career in cybersecurity

## Prerequisites

There are no prerequisites for either course or exam, however, as the exam is a combination of the Foundation and Practitioner exams, this should indicate the suggested level of experience you need before attempting either the course or the exam. For more information, consult the datasheets for the Foundation and Practitioner, or call for some advice.

## Course objectives

At the conclusion of this course, the student will be able to:

- Use the Framework as a key part of a systematic process for identifying, assessing, and managing cybersecurity risk
- Overlay the Framework onto current processes to determine gaps in current cybersecurity risk approach and develop a roadmap
- Use the Framework as a cybersecurity risk management tool
- Determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment

## .Credits Earned

40 PDU and 40 CEU Credits

## Body of knowledge

This course is based on the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1.

## Detailed course outline

| | | |
|---|---|---|
| **NCSP Foundation Training** | | |
| **Chapter 01 - Course Introduction** | | |
| **Lesson: Course Organization** | • Welcome to the course<br>• Why are you here?<br>• Using Bloom's Taxonomy | • What do you expect?<br>• Housekeeping<br>• Getting started in the classroom |
| **Lesson: Course Resources** | • Course materials<br>• Syllabus<br>• Student manual<br>• Your day and quizzes | • My ITSM Mentoring Community<br>• NCSP Foundation Certification Exam<br>• Agenda—NCSP Foundation |
| **Lesson: NIST-CSF "Setting the Stage"** | • The context<br>• NIST Cybersecurity Framework<br>• The story | • Let's get started<br>• Checkpoint |
| **Chapter 02 - Digital Transformation: Becoming Digital** | • Digital transformation<br>• Introduction | • Learning outcomes |
| **Lesson: Basics of Digital Transformation** | • What is digital transformation?<br>• Transformation—industrial to digital era | • Digital transformation and critical infrastructure<br>• Digital transformation: Attributes of the digital enterprise |
| **Lesson: Becoming Digital** | • Digital transformation from the corner office<br>• Becoming "digital"<br>• Optimized rate of change | • Outside-in, putting customers first<br>• Transforming the enterprise |
| **Lesson: Cybersecurity and Digital Transformation** | • Role of cybersecurity in digital transformation<br>• Cybersecurity and critical infrastructure<br>• Digital transformation: Basic principles (THRIVE) | • Digital transformation impacts many areas<br>• Cybersecurity: Key DX challenge |
| **Lesson: DX and the Framework** | • Digital transformation and NIST Cybersecurity Framework (CSF)<br>• Basic review of cybersecurity practices<br>• Establish or improve the cybersecurity program<br>• Communicate CS requirements with stakeholders | • Buying decisions<br>• Identify opportunities for new or revised Informative References<br>• Methodology to protect privacy and civil liberties |
| **Summary: Digital Transformation** | • Knowledge check—things you should know | • Checkpoint |
| **Chapter 03 - Understanding Cyber Risks** | • Understanding cyber risks<br>• Introduction | • Learning outcomes |
| **Lesson: Cyber Risk Equation** | • The problem<br>• Profile of an attack<br>• Phases of the kill chain<br>• MITRE Attack Framework | • MITRE Enterprise ATT&CK Framework<br>• The cyber risk equation<br>• Evaluating the results—what does it all mean? |

| | | |
|---|---|---|
| **Lesson: Cyber Risk Components** | • Cyber risk components: Threats<br>• Threats<br>• Cyber risk components: Business and technical vulnerabilities<br>• Vulnerabilities<br>• Cyber risk components: Assets and information | • Asset value<br>• Cyber risk components: Controls<br>• Controls<br>• Cyber risk: Fighting back<br>• Risk |
| **Lesson: Basics of Cyber Risk Assessment** | • Risk assessments<br>• Risk management process<br>• Frame the risk<br>• Assess the risk<br>• Respond to the risk | • Monitor the risk<br>• Key risk concepts<br>• Risk framing components and relationships<br>• Organizational risk frame |
| **Summary: Understanding Cyber Risks** | • Knowledge check—things you should know | • Checkpoint |
| **Chapter 4 - NIST Cybersecurity Framework Fundamentals** | • NIST Cybersecurity Framework fundamentals<br>• Introduction | • Learning outcomes |
| **Lesson: NIST-CSF Overview** | • Cybersecurity Framework: Origins<br>• Key attributes of NIST-CSF<br>• The Framework is for organizations …<br>• The Framework components<br>• NIST Cybersecurity Framework components | • NIST Cybersecurity Framework as a guide<br>• The key areas of focus<br>• Why adopt the NIST CSF?<br>• Benefits of adopting NIST-CSF<br>• Evolution of NIST-CSF |
| **Lesson: Framework Core, Tiers and Profiles** | • NIST-CSF Core functions<br>• Core function: Goals and objectives<br>• Framework Core approach<br>• NIST-CSF Tier<br>• NIST-CSF Implementation Tiers<br>• Key properties of cyber risk management<br>• Implementation Tiers approach | • Implementation Tiers example<br>• NIST CSF Framework Profiles<br>• Thinking about a Profile<br>• Profile information input<br>• Seven-step process<br>• Core, Tiers, Profiles example |
| **Summary: NCSF Fundamentals** | • Knowledge check—things you should know | • Checkpoint |
| **Chapter 5 - Core Functions, Categories and Subcategories: Organizational Cybersecurity Capabilities** | • Core Functions, Categories and Subcategories<br>• Introduction<br>• Learning outcomes | • The Five Core Functions<br>• Framework Core structure<br>• Framework Categories, Subcategories, References |
| **Lesson: Identify** | • Core Function Identify—purpose, goals and objectives<br>• Identify: Framework Categories<br>• Core Function Identify: Subcategories (AM and BE) | • Core Function Identify: Subcategories (GV and RA)<br>• Core Function Identify: Subcategories (RM and SC) |
| **Lesson: Protect** | • Core Function Protect—purpose, goals and objectives<br>• Protect: Framework Categories<br>• Core Function Protect: Subcategories (AC and AT) | • Core Function Protect: Subcategories (DS)<br>• Core Function Protect: Subcategories (IP)<br>• Core Function Protect: Subcategories (MA and PT) |
| **Lesson: Detect** | • Core Function Detect—purpose, goals and objectives<br>• Detect: Framework Categories | • Core Function Detect: Subcategories (AE and CM)<br>• Core Function Detect: Subcategories (DP) |

| | | |
|---|---|---|
| **Lesson: Respond** | • Core Function Respond—purpose, goals and objectives<br>• Respond: Framework Categories | • Core Function Respond: Subcategories (RP and CO)<br>• Core Function Respond: Subcategories (AN, MI and IM) |
| **Lesson: Recover** | • Core Function Recover—purpose, goals and objectives<br>• Recover: Framework Categories | • Core Function Recover: Subcategories (RP, IM and CO) |
| **Lesson: Informative References** | • Informative References<br>• Tailor to suit<br>• Exploring CIS 20 Critical Controls<br>• Critical Security Controls overview<br>• CIS Controls—key principles for v7.1<br>• CIS Controls-v7<br>• Basic—CIS Controls 1 to 6 | • CIS-01 to 06 mapped to NIST Core Functions<br>• Foundational—CIS Controls 7 to 11<br>• Foundational—CIS Controls 12 to 16<br>• CIS-07 to 16 mapped to NIST Core Functions<br>• Organizational—CIS Controls 17 to 20<br>• CIS-17 to 20 mapped to NIST Core Functions |
| **Summary: Core Functions, Categories & Subcategories** | • Knowledge Check—things you should know | • Checkpoint |
| **Chapter 6 - Implementation Tiers and Profiles: Understanding Current and Future Capabilities** | • Implementation Tiers and Profiles<br>• Introduction | • Learning outcomes |
| **Lesson: Understanding Tiers** | • NIST Cybersecurity Framework—Tiers<br>• Implementation Tiers<br>• Implementation Tier objectives<br>• Tier 1: Partial<br>• Tier 2: Risk Informed | • Tier 3: Repeatable<br>• Tier 4: Adaptive<br>• Risk management practices<br>• Example—Implementation Tiers and their use |
| **Lesson: Understanding Profiles** | • Developing Framework Profiles<br>• Profiles | • Framework Profiles<br>• Profile—an example |
| **Lesson: Creating Profiles** | • Using the risk assessment to create the Profile<br>• Identify Function: Asset Management Profile<br>• Protect Function: Data Security | • Detect Function: Detection Process<br>• Respond Function: Analysis<br>• Recover Function: Recovery Planning |
| **Summary: Developing Framework Profiles** | • Knowledge check—things you should know | • Checkpoint |
| **Chapter 7 - Cybersecurity Improvement: Getting "There" From "Here"** | • Cybersecurity improvement<br>• Introduction | • Learning outcomes |
| **Lesson: Adopt and Adapt** | • Adopt—the decision to move forward with NIST-CSF<br>• Adapt—tailor NIST to your context<br>• Principles of adaptation<br>• Customer drives value<br>• Start where you are | • Simplify everything<br>• Adopt and apply systems thinking<br>• Change is an organizational capability<br>• Technology is a means, not an end<br>• Create to overcome entropy |
| **Lesson: Implement and Improve** | • Fast Track concepts<br>• NCSF-Fast Track controls (NCSF-FT) | • Fast Track—implement/improve cycles<br>• Adaptive approach reduces waste, delivers value |

| | | |
|---|---|---|
| **Lesson: Continual Implementation and Improvement System (CIIS) as a Practice** | • CIIS approach<br>• Seven Step approach<br>• Step 1: Prioritize and Scope<br>• Step 2: Orient<br>• Step 3: Create a Current Profile | • Step 4: Conduct a Risk Assessment<br>• Step 5: Create a Target Profile<br>• Step 6: Determine, Analyze, and Prioritize Gaps<br>• Step 7: Implement Action Plan |
| **Summary: Cybersecurity Improvement** | • Knowledge check—things you should know | • Checkpoint |
| **NCSP Practitioner Training Outline** | | |
| **Chapter 1 - Course Introduction** | • Course Introduction | |
| **Lesson: Course Organization** | • Learning outcomes<br>• Welcome to the course<br>• Why are you here?<br>• Using Bloom's Taxonomy<br>• What do you expect?<br>• Housekeeping online | • Daily routine, quizzes and exercises<br>• NCSP Practitioner Exam<br>• NCSP Bootcamp Exam<br>• Getting started in the classroom<br>• Agenda |
| **Lesson: Setting the Stage** | • Constantly evolving threat landscape<br>• Adopt the NIST-CSF and adapt an informative reference<br>• Cybersecurity adopt and adapt—governance and management | • Use an adaptive way of working<br>• Rapid Adoption and Rapid Adaptation FastTrack<br>• Continual improvement and implementation of cybersecurity |
| **Chapter 02 - Digital Transformation and Cybersecurity** | • Digital transformation and cybersecurity | • Learning outcomes |
| **Lesson: DX as a Practitioner** | • The industrial era and the digital era<br>• Entering the digital era<br>• Unique strategic challenges of the digital era<br>• Digital strategy concepts<br>• Organizational culture defined<br>• The need for a digital culture<br>• Get your culture ready to transform<br>• Digital transformation readiness framework<br>• Framework structure | • Operational sustainability—principle themes<br>• Attributes of operational sustainability<br>• Organizational agility—principle themes<br>• Attributes of organizational agility<br>• Strategic agility—principle themes<br>• Attributes of strategic agility<br>• Disruptive culture—principle themes<br>• Disruptors are not loose cannons<br>• Digital readiness framework |
| **Lesson: DX in the Context of Cybersecurity** | • More about culture than technology<br>• Adopt and adapt—DX and cybersecurity<br>• Agility demands | • Shared aspects<br>• Different sides of the same coin |
| **Lesson: Cybersecurity as a DX Catalyst** | • Start with operational sustainability<br>• Becoming agile | • Establish a strategic approach |

| | | |
|---|---|---|
| **Summary: Digital Transformation and Cybersecurity** | • Becoming digital ready<br>• Interdependencies—DX/Cybersecurity | • Checkpoint |
| **Chapter 03 - Threat Landscape** | • Threat landscape<br>• Learning outcomes | • Introduction |
| **Lesson: Threat Actors: Agile and Creative** | • Take advantage of everything: all information has value<br>• Threat actor creativity | • Threat actors—agile and adaptive<br>• Threat actors exploit vulnerabilities |
| **Lesson: Attacks** | • Generic attack types<br>• Typical attack profile<br>• Lockheed-Martin Cyber Kill Chain<br>• Typical mitigation controls | • External attacks<br>• Insider attacks<br>• Verizon 2019 Data Breach Investigation Report (DBIR)<br>• Verizon 2019 DBIR Summary |
| **Lesson: Challenges** | • Vulnerability contributors<br>• Indicators for cybersecurity issues<br>• Most prevalent deficiencies<br>• IT and cybersecurity<br>• Organizational challenges | • Lack of cybersecurity budget/funding<br>• Cybersecurity funding impacts all organizations<br>• Increased threat sophistication<br>• CISO actions |
| **Lesson: Organizational Response to Threat Landscape** | • New approach to Information Security Management (ISM)<br>• Understand cyber risk<br>• Understand importance of controls<br>• Breaches—lessons learned<br>• Analysis of Target breach—background<br>• Analysis of Target breach—threat actor reconnaissance phase<br>• Analysis of Target breach—threat actor infection and infiltration phases<br>• Analysis of Target breach—threat actor data collection and exfiltration phases | • General lessons from Target breach<br>• Lessons from Target breach for each attack phase (1)<br>• Lessons from Target breach for each attack phase (2)<br>• Analysis of Home Depot breach—background<br>• Lessons from Home Depot breach<br>• Analysis of Sony breach—background<br>• General lessons from the Sony breach<br>• Lessons from the Sony breach—infection and infiltration<br>• Lessons from the Sony breach—data collection and exfiltration |
| **Lesson: Absolute Prevention Not Possible** | • Ongoing improvement is critical<br>• Cybersecurity isn't implemented and done<br>• Make strategic commitment to inculcate cybersecurity into culture<br>• Trust and verify<br>• Not just awareness and training—deterrence | • What is cybersecurity deterrence<br>• Start with program to raise awareness<br>• Make CS training and awareness critical part of organizational DNA<br>• Training alone insufficient |
| **Summary: Threat Landscape** | • Threat actors<br>• Attacks<br>• Challenges | • Organizational response to threat landscape<br>• Absolute prevention not possible<br>• Checkpoint |

| | | |
|---|---|---|
| **Chapter 04 - The Controls** | • The controls<br>• Learning outcomes<br>• Overall approach and control selection | • Control selection rationale<br>• Introduction to cybersecurity controls |
| **Lesson: Initiation and Basic Controls** | • Controls phased adoption<br>• Controls—order of precedence (initiation and basic [startup])<br>• CIS Control 17—Implement a Security Awareness and Training Program<br>• CIS Control 17—Implement a Security Awareness and Training Program Sub Controls<br>• CIS Control 19—Incident Response and Management<br>• CIS Control 19—Incident Response and Management Sub Controls<br>• CIS Control 1—Inventory and Control of Hardware Assets | • CIS Control 1—Inventory and Control of Hardware Assets Sub Controls<br>• CIS Control 2—Inventory and Control of Software Assets<br>• CIS Control 2—Inventory and Control of Software Assets Sub Controls<br>• CIS Control 3—Continuous Vulnerability Management<br>• CIS Control 4—Controlled Use of Administrative Privileges<br>• CIS Control 5—Secure Configurations<br>• CIS Control 6—Maintenance, Monitor and Analysis of Audit Logs |
| **Lesson: Foundation Controls** | • CIS Control 7—Email and Web Browser Protections<br>• CIS Control 8—Malware Defenses<br>• CIS Control 9—Limitations and Control of Network Ports, Protocols and Services<br>• CIS Control 10—Data Recovery Capabilities<br>• CIS Control 11—Secure Configurations for Network Devices | • CIS Control 12—Boundary Defenses<br>• CIS Control 13—Data Protection<br>• CIS Control 14—Control Access Based on the Need to Know<br>• CIS Control 15—Wireless Access Control<br>• CIS Control 16—Account Monitoring and Control |
| **Lesson: Organizational and Recovery Controls** | • CIS Control 18—Application Software Security<br>• CIS Control 20—Penetration Tests and Red Team Exercises | • Recovery NIST-CSF—NIST 800-53 |
| **Summary: Controls** | • Controls—order of precedence (initiation and basic [startup]) | • Checkpoint |
| **Chapter 05 - Adopt and Adapt** | • Adopt and adapt | • Learning outcomes |
| **Lesson: The Context of Adopt and Adapt** | • Introduction to adopt and adapt<br>• Adopt: What's included in governance for cybersecurity?<br>• Adapt: What's included in management for cybersecurity? | • Lean thinking applied<br>• Cybersecurity adopt and adapt—governance and management<br>• Management: Operationalization of cybersecurity |
| **Lesson: Cybersecurity and Culture** | • Culture defined and thoughts about culture<br>• Cultural patterns<br>• Characteristics of culture types: How they process information | • How to change your culture<br>• Culture and cybersecurity<br>• Final thoughts on culture |
| **Lesson: Where We Are** | • Determine current state<br>• Determinative model<br>• Flow of improvement<br>• Flow of communication | • Flow of work<br>• 3D knowledge flow model<br>• Consultant's view of the flows |

| | | |
|---|---|---|
| **Summary: Adopt and Adapt** | • The context of adopt and adapt<br>• Cybersecurity and culture | • Where we are<br>• Checkpoint |
| **Chapter 06 - Adaptive Way of Working** | • Adaptive way of working | • Learning outcomes |
| **Lesson: Introduction to Adaptive Way to Work** | • Adaptive approach reduces waste, delivers value<br>• Little gap and big gap<br>• Quick review<br>• Approach<br>• Leverage cross-functional teams<br>• Lots of small projects<br>• Work structure | • Facilitate learning<br>• Everything is subject to improvement<br>• Try something new in “the small”<br>• Be proactive<br>• Organizational change<br>• Change requires engagement<br>• Focus on small steps toward a goal, not the whole |
| **Lesson: How to Get Started** | • Adaptive approach<br>• Work in phases<br>• Ask questions: Method (how), not capability (binary choice)<br>• Develop small requirements | • Prioritize based on most valuable thing to do “next”<br>• Focus on value, outcomes, costs and risks<br>• Develop different flow patterns |
| **Summary: Adaptive Way of Working** | • Introduction to adaptive way of working<br>• How to get started | • Checkpoint |
| **Chapter 07 - Rapid Adoption and Rapid Adaptation FastTrack** | • Rapid Adoption and Rapid Adaptation FastTrack<br>• Learning outcomes | • Rapid adoption and adaptation using FastTrack |
| **Lesson: Rapid Adoption** | • Determine risk appetite<br>• Establish cybersecurity governance<br>• Assess cybersecurity capabilities | • Balance resources and risks<br>• Balance resource optimization model<br>• Optimized resources |
| **Lesson: Rapid Adaptation** | • Cybersecurity assessment<br>• Impact on people, practice and technology<br>• Impact flows<br>• Implementation groups<br>• Review Center for Internet Security Controls<br>• Take a phased approach | • Phase 0: Initiation<br>• Phase 1: Establish cybersecurity beachhead<br>• Phase 2: Expand defensible perimeter<br>• Phase 3: Refine and tailor<br>• FastTrack—implement/improve cycles |
| **Summary: Rapid Adoption and Rapid Adaptation FastTrack** | • Rapid Adoption and Adaptation using FastTrack<br>• Rapid adoption<br>• Rapid adaptation | • FastTrack—implement/improve cycles<br>• Checkpoint |

| | | |
|---|---|---|
| **Chapter 08 - CIIS Practice** | • CIIS Practice<br>• Chapter: CIIS practice | • Learning outcomes |
| **Lesson: Ongoing Practice of Cybersecurity** | • Set the stage for continual improvement<br>• Build a learning organization<br>• How to scope ongoing improvement<br>• Identify business systems most at risk<br>• Verify or create inventory of hardware and software assets | • Think like a threat actor<br>• Mitigate and protect<br>• Learn and improve<br>• Embed<br>• Overall flow |
| **Lesson: NIST 7-Step Improvement** | • NIST 7-step<br>• Step 1: Prioritize and Scope<br>• Step 2: Orient<br>• Step 3: Create Current Profile | • Step 4: Conduct Risk Assessment<br>• Step 5: Create Target Profile<br>• Step 6: Determine, Analyze and Prioritize Gaps<br>• Step 7: Implement Action Plan |
| **Lesson: Cybersecurity Maturity Model Certification CMMC** | • Origins of CMMC<br>• CMMC Model Framework<br>• CMMC Model Level Descriptions—1 and 2<br>• CMMC Model Level Descriptions—3 and 4 | • CMMC Model Level Descriptions—5<br>• Examples of Level 1 to 3 practices<br>• Examples of Level 4 and 5 practices |
| **Lesson: Integrate Cybersecurity** | • Balancing loop<br>• Escalation (archetype)<br>• People, practice and technology: Improvement cycle | • Assess cybersecurity posture: Implementation cycle<br>• FastTrack—combined implement/improve cycles |
| **Summary: CIIS Practice** | • Set the stage for continual improvement<br>• Overall flow<br>• NIST 7-step | • Origins of CMMC<br>• FastTrack—combined implement/improve cycles<br>• Checkpoint |
| **Chapter 09 - Course Summary** | • Course summary wrap up | |

Learn more at

hpe.com/ww/learnsecurity

**Follow us:**

Hewlett Packard
Enterprise

H0DV9AAE, May 2020