Hewlett Packard Enterprise

NCSP Practitioner Training, Rev.20.21 H0DV8AAE

HPE course number	H0DV8AAE
Course length	12 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 APMG/GCHQ accredited NIST Cybersecurity Professional (NCSP) Practitioner course teaches the candidate 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 also prepares the candidate to sit for the NCSP Practitioner certification exam.

The NCSP Practitioner course builds upon the NCSP Foundation course (H0DV8AAE or H0DV8S) and targets IT, cybersecurity and auditing professionals looking to learn the knowledge, skills and abilities to assess, design, implement, operationalize and continually improve the controls and management systems associated with an NIST Cybersecurity program.

This course is supplemented by a student book to enhance the learning experience. The desired or expected outcome is an advanced understanding of the NIST-CSF in preparation to sit the NCSP Practitioner exam.

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

Audience

- Candidates pursuing a career in cybersecurity
- IT, cybersecurity and digital transformation design and implementation engineers
- IT, cybersecurity and digital transformation technical operations and business analysts
- IT, cybersecurity and digital transformation specialists including pen testers, ethical hackers, software and application developers, auditors, and investigators.

Prerequisites

- Candidates must have completed the NCSP Foundation course (H0DV7AAE or H0DV7S) and passed the NCSP Foundation exam

Course objectives

At the conclusion of this class, students will know a practical approach to build and maintain a comprehensive cybersecurity and cyber-risk management program.

.Credits Earned

- 24 PDU and CEU Credit

Body of knowledge

This course is based on the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1. It was published by the National Institute of Standards & Technology on February 12, 2014.

Detailed course outline

Chapter 01 - Course Introduction	• Course Introduction	
Lesson: Course Organization	• Learning outcomes • Welcome to the course • Why are you here? • Using Bloom's Taxonomy • What do you expect?	• Housekeeping online • Daily routine, quizzes and exercises • NCSP Practitioner Exam • NCSP Bootcamp Exam • Getting started in the classroom • Agenda
Lesson: Setting the Stage	• Constantly evolving threat landscape • Adopt the NIST-CSF and adapt an informative reference • Cybersecurity adopt and adapt—governance and management	• Use an adaptive way of working • Rapid Adoption and Rapid Adaptation FastTrack • 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 • Entering the digital era • Unique strategic challenges of the digital era • Digital strategy concepts • Organizational culture defined • The need for a digital culture • Get your culture ready to transform • Digital transformation readiness framework • Framework structure	• Operational sustainability—principle themes • Attributes of operational sustainability • Organizational agility—principle themes • Attributes of organizational agility • Strategic agility—principle themes • Attributes of strategic agility • Disruptive culture—principle themes • Disruptors are not loose cannons • Digital readiness framework
Lesson: DX in the Context of Cybersecurity	• More about culture than technology • Adopt and adapt—DX and cybersecurity • Agility demands	• Shared aspects • Different sides of the same coin
Lesson: Cybersecurity as a DX Catalyst	• Start with operational sustainability • Becoming agile	• Establish a strategic approach
Summary: Digital Transformation and Cybersecurity	• Becoming digital ready • Interdependencies—DX/cybersecurity	• Checkpoint
Chapter 03 - Threat Landscape	• Threat landscape • Learning outcomes	• Introduction
Lesson: Threat Actors: Agile and Creative	• Take advantage of everything: all information has value • Threat actor creativity	• Threat actors—agile and adaptive • Threat actors exploit vulnerabilities
Lesson: Attacks	• Generic attack types • Typical attack profile • Lockheed-Martin Cyber Kill Chain • Typical mitigation controls	• External attacks • Insider attacks • Verizon 2019 Data Breach Investigation Report (DBIR) • Verizon 2019 DBIR Summary

Lesson: Challenges	• Vulnerability contributors • Indicators for cybersecurity issues • Most prevalent deficiencies • IT and cybersecurity • Organizational challenges	• Lack of cybersecurity budget/funding • Cybersecurity funding impacts all organizations • Increased threat sophistication • CISO actions
Lesson: Organizational Response to Threat Landscape	• New approach to Information Security Management (ISM) • Understand cyber risk • Understand importance of controls • Breaches—lessons learned • Analysis of Target breach—background • Analysis of Target breach—threat actor reconnaissance phase • Analysis of Target breach—threat actor infection and infiltration phases • Analysis of Target breach—threat actor data collection and exfiltration phases	• AGeneral lessons from Target breach • Lessons from Target breach for each attack phase (1) • Lessons from Target breach for each attack phase (2) • Analysis of Home Depot breach—background • Lessons from Home Depot breach • Analysis of Sony breach—background • General lessons from the Sony breach • Lessons from the Sony breach—infection and infiltration • Lessons from the Sony breach—data collection and exfiltration
Lesson: Absolute Prevention Not Possible	• Ongoing improvement is critical • Cybersecurity isn't implemented and done • Make strategic commitment to inculcate cybersecurity into culture • Trust and verify • Not just awareness and training—deterrence	• What is cybersecurity deterrence • Start with program to raise awareness • Make CS training and awareness critical part of organizational DNA • Training alone insufficient
Summary: Threat Landscape	• Threat actors • Attacks • Challenges	• Organizational response to threat landscape • Absolute prevention not possible • Checkpoint
Chapter 04 - The Controls	• The controls • Learning outcomes • Overall approach and control selection	• Control selection rationale • Introduction to cybersecurity controls
Lesson: Initiation and Basic Controls	• Controls phased adoption • Controls—order of precedence (initiation and basic [startup]) • CIS Control 17—Implement a Security Awareness and Training Program • CIS Control 17—Implement a Security Awareness and Training Program Sub Controls • CIS Control 19—Incident Response and Management • CIS Control 19—Incident Response and Management Sub Controls • CIS Control 1—Inventory and Control of Hardware Assets	• CIS Control 1—Inventory and Control of Hardware Assets Sub Controls • CIS Control 2—Inventory and Control of Software Assets • CIS Control 2—Inventory and Control of Software Assets Sub Controls • CIS Control 3—Continuous Vulnerability Management • CIS Control 4—Controlled Use of Administrative Privileges • CIS Control 5—Secure Configurations • CIS Control 6—Maintenance, Monitor and Analysis of Audit Logs

Lesson: Foundation Controls	• CIS Control 7-Email and Web Browser Protections • CIS Control 8-Malware Defenses • CIS Control 9-Limitations and Control of Network Ports, Protocols and Services • CIS Control 10-Data Recovery Capabilities • CIS Control 11-Secure Configurations for Network Devices	• CIS Control 12-Boundary Defenses • CIS Control 13-Data Protection • CIS Control 14-Control Access Based on the Need to Know • CIS Control 15-Wireless Access Control • CIS Control 16-Account Monitoring and Control
Lesson: Organizational and Recovery Controls	• CIS Control 18—Application Software Security • 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 • Adopt: What's included in governance for cybersecurity? • Adapt: What's included in management for cybersecurity?	• Lean thinking applied • Cybersecurity adopt and adapt—governance and management • Management: Operationalization of cybersecurity
Lesson: Cybersecurity and Culture	• Culture defined and thoughts about culture • Cultural patterns • Characteristics of culture types: How they process information	• How to change your culture • Culture and cybersecurity • Final thoughts on culture
Lesson: Where We Are	• Determine current state • Determinative model • Flow of improvement • Flow of communication	• Flow of work • 3D knowledge flow model • Consultant's view of the flows
Summary: Adopt and Adapt	• The context of adopt and adapt • Cybersecurity and culture	• Where we are • 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 • Little gap and big gap • Quick review • Approach • Leverage cross-functional teams • Lots of small projects • Work structure • Facilitate learning	• Everything is subject to improvement • Try something new in "the small" • Be proactive • Organizational change • Change requires engagement • Focus on small steps toward a goal, not the whole
Lesson: How to Get Started	• Adaptive approach • Work in phases • Ask questions: Method (how), not capability (binary choice) • Develop small requirements	• Prioritize based on most valuable thing to do "next" • Focus on value, outcomes, costs and risks • Develop different flow patterns
Summary: Adaptive Way of Working	• Introduction to adaptive way of working • How to get started	• Checkpoint
Chapter 07 - Rapid Adoption and Rapid Adaptation FastTrack	• Rapid Adoption and Rapid Adaptation FastTrack • Learning outcomes	• Rapid adoption and adaptation using FastTrack
Lesson: Rapid Adoption	• Determine risk appetite • Establish cybersecurity governance • Assess cybersecurity capabilities	• Balance resources and risks • Balance resource optimization model • Optimized resources
Lesson: Rapid Adaptation	• Cybersecurity assessment • Impact on people, practice and technology • Impact flows • Implementation groups • Review Center for Internet Security Controls	• Take a phased approach • Phase 0: Initiation • Phase 1: Establish cybersecurity beachhead • Phase 2: Expand defensible perimeter • Phase 3: Refine and tailor • FastTrack—implement/improve cycles
Summary: Rapid Adoption and Rapid Adaptation FastTrack	• Rapid Adoption and Adaptation using FastTrack • Rapid adoption	• Rapid adaptation • FastTrack—implement/improve cycles • Checkpoint
Chapter 08 - CIIS Practice	• CIIS Practice • Chapter: CIIS practice	• Learning outcomes

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

Learn more at
hpe.com/ww/learnsecurity

Follow us:

H0DV8AAE, May 2020

Hewlett Packard
Enterprise