Hewlett Packard Enterprise

NCSP Boot Camp Certification H0DV9S

HPE course number	H0DV9S
Course length	5 Days
Delivery mode	ILT, VILT
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

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

This APMG accredited training program is targeted at IT and cybersecurity professionals who wish to become certified on how to operationalize the NIST-CFS across an enterprise and its supply chain. The NCSP Bootcamp program teaches the knowledge to prepare for the NSCP Boot Camp exam (Foundation + Practitioner) plus the skills and abilities to design, build, test, manage and improve a cybersecurity program based on the NCSF.

This course essentially combines the NCSP Foundation and Practitioner, but with only one exam instead of two (if the foundation and Practitioner are taken separately).

Audience

- Candidates looking to pursue 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 a reasonable amount of cyber security awareness and/or experience.

Course objectives

Upon completion of this course, students will have:

- The skills and abilities to design, build, test, manage and improve a cybersecurity program based on the NCSF
- The knowledge to prepare for the NSCP Boot Camp exam (Foundation + Practitioner)

Credits Earned

- 24 PDU & 24 CEU Credits

Delivery

The course will be delivered using ILT (traditional classroom with a live instructor) or vILT (a real instructor delivering the course over the internet). Draining Materials provided to each registration will include the following: Student book in PDF format - Enables note taking during the course. Video Library - Access to the self-study / self-paced videos will be provided (a 12 month license (renewable)) for future reference purposes.

Detailed course outline

H0DV7S: NCSP Foundation Training		
Digital Transformation	• Explain what it means to "become digital" • Discuss the difference between industrial and digital era enterprises	• Explain how cybersecurity supports an organization's digital transformation
Understanding Cyber Risks	• Explain the cyber risk equation • Identify and explain each component of the cyber risk equation	• Describe the basics of a risk assessment
NIST Cybersecurity Framework Fundamentals	• Explain the genesis of the NIST-CSF • List and describe the components of the NIST-CSF	• Describe each of the NIST-CSF's objectives
Core Functions, Categories and Subcategories	• Understand and explain – Core functions	– Framework categories – Informative references
Implementation Tiers and Profiles	• Understand and explain Implementation Tier terms and their use • Understand and explain each Implementation Tier • Understand and describe the three risk categories • Understand and explain Profiles and their use	• Understand and describe the use of Profiles when – Determining gaps – Identifying and prioritizing focus areas
Cybersecurity Improvement	• Understand and explain how an organization can approach the adoption and adaptation of the NIST-CSF • Understand and describe how to implement cybersecurity controls using an incremental improvement approach	• Understand and describe CIIS as a practice within an organization
H0DV8S: NCSP Practitioner Training		
Chapter 1: Course Introduction	• Course organization	• Setting the stage
Chapter 2: Digital Transformation	• DX as a practitioner • DX in the context of cybersecurity	• Cybersecurity as a DX catalyst
Chapter 3: Threat Landscape	• Threat actors: Agile and Creative • Attacks • Challenges	• Organizational response to threat landscape • Absolute prevention not possible
Chapter 4: The Controls	• Initiation and basic • Foundation	• Organizational and recovery
Chapter 5: Adopt and Adapt	• The context of adopt and adapt • Cybersecurity and culture	• Where we are
Chapter 6: Adaptive Way of Working	• Introduction to adaptive way to work	• How to get started
Chapter 7: Rapid Adoption and Rapid Adaptation FastTrack™	• Rapid adoption	• Rapid adaptation
Chapter 8: CIIS as a Practice	• Ongoing practice of cybersecurity • NIST 7-step improvement	• Cybersecurity Maturity Model Certification (CMMC) • Integrate cybersecurity

Learn more at
hpe.com/ww/learnsecurity

Follow us:

H0DV9S A.00, March 2020

Hewlett Packard
Enterprise