

NCSP® 800-53 Practitioner Certification Training HODV8S

HPE course number	HODV8S
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?

- Comprehensive worldwide [HPE technical, IT industry and personal development training](#)
- [Training and certification preparation](#) for ITIL®, Security, VMware®, Linux, Microsoft and more
- Innovative [training options](#) that match individual learning styles
- Anytime, anywhere remote learning via [HPE Digital Learner](#) subscriptions
- Verifiable [digital badges](#) for proof of training, skill recognition and career development
- Simplified purchase options with [HPE Training Credits](#)

The NCSP® 800-53 Practitioner Training course is accredited (APMG International), certified (NCSC/GCHQ-UK), and recognized (DHS-CISA-USA). In this course, digital business, operational stakeholders, auditors, and risk practitioners learn a fast-track approach to adopting and adapting the NIST Cybersecurity Framework and its 800-53 controls across the enterprise and its supply chain.

The course also teaches how to build a Digital Value Management System (DVMS) CPD overlay model capable of enabling the quick adoption and adaptation of new frameworks and models (NIST-CSF, NIST Privacy Framework, CMMC, etc.) that may be required to address changes to internal, external (regulatory) and cyber threat landscapes.

Finally, the course teaches candidates how to ensure the organization's DVMS is designed for use within the organization, and supports auditing by government regulators looking to verify regulatory outcomes.

Audience

This course is for digital business, operational stakeholders, auditors, and risk practitioners. It delivers the knowledge they need to implement, operationalize and continually innovate an NIST Cybersecurity Framework program underpinned by a DVMS.

Prerequisites

Candidates must have attended and completed the NCSP Foundation course and exam to participate in this course.

Course objectives

- Create a business culture of creating, protecting, and delivering digital business value
- Enable the business to adopt and adapt quickly to regulatory updates
- Provide the board and senior leadership team with evidence to show the organization did everything possible to defend itself from a breach
- Leverage this new business capability as a competitive advantage

Examination

The NCSP© Practitioner Exam

- 65 multiple-choice questions per exam
- 150-minute exam
- Pass mark – 50% (33 marks)
- Open book
- Blooms Level 3,4, & 5
- Paper-based and online availability (including ProctorU)

Detailed course outline

Be the Menace—a Proactive Approach	<ul style="list-style-type: none"> Establish an understanding of the threat landscape to facilitate a proactive approach to cyber resilience within the context of strategy-risk
Systems Thinking	<ul style="list-style-type: none"> Establish an understanding of systems thinking and how to use it to affect change and build a cyber-resilient organization
Cybersecurity and the DVMS	<ul style="list-style-type: none"> Establish an understanding of the Digital Value Management System™ (DVMS) as part of an approach to manage digital business risk and achieve the desired cybersecurity posture
Adapting the Way We Work	<ul style="list-style-type: none"> Understand the role of adoption and adaptation in achieving the desired cybersecurity posture
Cybersecurity Within a System	<ul style="list-style-type: none"> Establish an understanding of the relationship between systems thinking, and the Z-X Model™ capabilities practice areas, cybersecurity controls, and the DVMS FastTrack™ approach
Digital Business Risk Management	<ul style="list-style-type: none"> Establish an understanding of how mental models and the DVMS practice areas fit to support establishing digital business risk management
The DVMS as a Scalable Overlay	<ul style="list-style-type: none"> Establish an understanding of the three layers of the DVMS model and how they form a scalable overlay adaptable to organizations of any size

Learn more at
hpe.com/ww/learnsecurity

Follow us:

