



Hewlett Packard Enterprise

NIST Cybersecurity Professional 800-53 Practitioner Certification Training

H0DV8AAE

Course ID	H0DV8AAE
Duration	16 hours
Subscription length	12 months
Format	eLearning
View schedule, local pricing, and register	View now
Browse related courses	View now

5 reasons to choose HPE as your training partner

1. Learn HPE and in-demand IT industry technologies from expert instructors.
2. Build career-advancing power skills.
3. Enjoy personalized learning journeys aligned to your company's needs.
4. Choose how you learn: [in-person](#), [virtually](#), or [on-demand](#)—anytime, anywhere.
5. Sharpen your skills with access to real environments in [virtual labs](#).

Explore our simplified purchase options, including [HPE Education Learning Credits](#).

This course provides a fast-track approach to assessing, engineering, implementing, and operationalizing the NIST Cybersecurity Framework (NIST-CSF) 800-53 controls across an enterprise and its supply chain. It demonstrates how to build an overlay model capable of operationalizing the NIST-CSF and its NIST 800-53 controls to facilitate the secure, resilient, and auditable digital outcomes expected by government regulators and operational stakeholders.

In addition, this training offers a deep dive into the DVMS Institute Create, Protect, and Deliver (CPD) overlay model. As cloud services revolutionized the creation and management of digital infrastructure, the DVMS CPD overlay model, underpinned by well-known frameworks from NIST and standards from ISO, revolutionizes how organizations manage their digital risk, resiliency, and privacy.

The NIST Cybersecurity Framework (NIST-CSF) provides a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks. It provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

NIST Cybersecurity Professional certification training programs are accredited by APMG International.

Audience

This course is ideal for IT, business and cybersecurity professionals who play an active or passive role in engineering, operationalizing, and continually improving an organization's NIST-CSF program and those looking for a baseline knowledge of the NIST-CSF who are considering a career in cybersecurity.

Certifications and related exams

This course prepares you for the NIST Cybersecurity Professional Foundation certification exam.

Course objectives

After completing this course, you should be able to:

- Describe today's digital economy
- Understand cyber risks
- Outline NIST Cybersecurity Framework fundamentals
- Identify core functions, categories, and subcategories
- Classify Implementation tiers
- Develop framework profiles
- Detect cybersecurity improvement

Detailed course outline

Module 1: 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
Module 2: 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.
Module 3: 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
Module 4: Adapting the Way We Work	<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
Module 5: 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
Module 6 : 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
Module 7: 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/learn/cybersecurity

Follow us:

