

NIST Professional Foundation Certification Training

H0DV7S

Course ID	H0DV7S
Duration	2 days
Format	ILT, VILT
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 teaches business leaders and operational stakeholders the fundamentals of communicating with executive leadership on what investments must be made to operationalize the NIST Cybersecurity Framework and its informative references to facilitate secure, resilient, and auditable digital outcomes. It introduces you to 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

Detailed course outline

Module 1: Digital Evolution	<ul style="list-style-type: none"> The evolving threat landscape Digital evolution 	<ul style="list-style-type: none"> NIST-CSF and digital evolution Digital evolution and the framework
Module 2: Understanding Cyber Risk	<ul style="list-style-type: none"> Introducing cyber risk Cyber risk components 	<ul style="list-style-type: none"> Basics of cyber risk assessment
Module 3: NIST Cybersecurity Framework	<ul style="list-style-type: none"> NIST-CSF overview 	<ul style="list-style-type: none"> Framework, Core, Tiers, and Profiles
Module 4: Core Functions, Categories, and Subcategories	<ul style="list-style-type: none"> Identity Protect Detect 	<ul style="list-style-type: none"> Respond Recover Informative references
Module 5: Implementing Tiers and Profiles	<ul style="list-style-type: none"> Understanding tiers Understanding profiles 	<ul style="list-style-type: none"> Creating profiles
Module 6: Beyond the Framework	<ul style="list-style-type: none"> Adopt and adapt 	<ul style="list-style-type: none"> Establish and improve

Learn more at

hpe.com/ww/learncybersecurity

Follow us:



© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

All third-party marks are property of their respective owners.

H0DV7S B.00, April 2024