Hewlett Packard Enterprise

CAP—Certified Authorization Professional H0DU4S

This Official (ISC)² course is designed for the information security practitioner who champions system security commensurate with an organization's mission and risk tolerance, while meeting legal and regulatory requirements. It conceptually mirrors the NIST system authorization process in compliance with the Office of Management and Budget (OMB) Circular A-130, appendix III.

HPE course number	H0DU4S
Course length	5 Days
Delivery mode	ILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

Why HPE Education Services?

- IDC MarketScape leader 4 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 (ISC)²
- 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

Audience

The course is intended for students who have at least one full year of experience using the federal Risk Management Framework (RMF) or comparable experience gained from the ongoing management of information system authorizations, such as ISO 27001. The CAP certification is an objective measure of the knowledge, skills, and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation.

Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk and damage to assets or individuals. CAP is appropriate for commercial markets, civilian and local governments, and the U.S. Federal government, including the State Department and the Department of Defense (DoD). See CAP and DoD 8570. Job functions such as authorization officials, system owners, information owners, information system security officers, certifiers, and senior system managers are great fits as CAPs.

The ideal candidate should have the following experience, skills, or knowledge in:

- IT security
- Information assurance
- Information risk management
- Certification
- Systems administration
- One to two years of general technical experience
- Two years of general systems experience
- One to two years of database/systems development/network experience
- Information security policy
- Technical or auditing experience within government, the U.S. Department of Defense, the financial or health care industries, and/or auditing firms
- Strong familiarity with NIST documentation

Course description

In this course you will find that several types of activities are used to reinforce topics and increase knowledge retention. These activities include open-ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, January 2016

Course objectives

After completing this course, the participant will be able to:

- Describe the historical legal and business considerations that required the development of the RMF, including related mandates
- Identify key terminology and associated definitions
- Describe the Risk Management Framework components, including the starting point inputs (architectural description and organization inputs)
- Describe the core roles defined by the RMF, including primary responsibilities and supporting roles for each RMF step
- Describe the core federal statutes, OMB directives, Federal Information Processing Standards (FIPS) and Special Publications (SP), and Department of Defense and Intelligence Community instructions that form the legal mandates and supporting guidance required to implement the RMF
- Identify and understand the related processes integrated with the RMF
- Identify key references related to RMF Step 1—Categorize
- Identify the roles, requirements, and processes to register an information system
- Identify key references related to RMF Step 2—Select
- Identify requisites for establishing information system security controls
- Identify key references related to RMF Step 3—Implement
- Identify key references related to RMF Step 4—Assess
- Identify key references related to RMF Step 5—Authorize
- Identify the roles, requirements, and processes associated with conducting remediation and completing the final security assessment report
- Identify key references related to RMF Step 6—Authorize
- Identify the roles, requirements, and processes associated with preparing the Plan of Action and Milestones (POA&M) for an information system
- Identify key references related to RMF Step 7—Monitor
- Identify the roles, requirements, and processes to formally dispose of an information system

Detailed course outline

Domain 1: Risk Management Framework (RMF)	• Describe the Risk Management Framework (RMF) • Describe and distinguish between the RMF steps • Identify roles and define responsibilities • Understand and describe how the RMF process relates to • Understand the relationship between the RMF and System Development Life Cycle (SDLC) • Understand legal, regulatory, and other security requirements
Domain 2: Categorization of information systems	• Categorize the system • Describe the information system (including the security authorization boundaries) • Register the system
Domain 3: Selection of security controls	• Identify and document common (inheritable) controls • Select, tailor, and document security controls • Develop security control monitoring strategy • Review and approve SP
Domain 4: Security control implementation	• Implement selected security controls • Document security control implementation
Domain 5: Security control assessment	• Prepare for security control assessment • Develop security control assessment plan • Assess security control effectiveness • Develop initial Security Assessment Report (SAR) • Review interim SAR and perform initial remediation actions • Develop final SAR and optional addendum
Domain 6: Information system authorization	• Develop Plan of Action and Milestones (POA&M) (e.g., resources, schedule, requirements) • Assemble security authorization package • Determine risk • Determine the acceptability of risk • Obtain security authorization decision
Domain 7: Monitoring of security controls	• Determine security impact of changes to system and environment • Perform ongoing security control assessments (e.g., continuous monitoring, internal and external assessments) • Conduct ongoing remediation actions (resulting from incidents, vulnerability scans, audits, vendor updates, etc.) • Update key documentation (e.g., SP, SAR, POA&M) • Perform ongoing risk determination and acceptance • Decommission and remove system

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04755686, September 2016, Rev. 3

Hewlett Packard
Enterprise