Test - CCYB 002 Cybersecurity for Program Managers Exam

TO3.EO3 Identify key cybersecurity T&E policy used during the acquisition lifecycle.

Question 1 of 15.

According to DoDI 5000.02T PMs should coordinate with which agency to prepare their systems for cooperative vulnerability and adversarial assessments by conducting cybersecurity testing during system development?

- (•) The cognizant Developmental Test Agency (DTA)
- ( ) An appropriate Operational Test Agency (OTA)
- ( ) National Security Agency (NSA)
- ( ) Defense Information Systems Agency (DISA)

[ ] Mark for follow up

Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO2.EO1 Describe key aspects of Cyber Survivability as part of the System Survivability (SS) Key Per

Question 4 of 15.

Choose the definition for threat vector below: (Choose the one correct answer)

- The route that a threat actor may take to get past your defenses and infect your network
- An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security.
- The DoD process for identifying, implementing, assessing, and managing cybersecurity capabilities and services
- Weakness that could be exploited by a threat source

Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO6.EO4 Analyze cybersecurity RFP statements to determine their suitability for an acquisition contr

Question 12 of 15.

Choose the statement below that best defines a Performance Work Statement (PWS):

- A SOW for Performance-Based Acquisitions that clearly describes the performance objectives and standards that are expected of the contractor.
- A solicitation used in negotiated acquisition to communicate government requirements to prospective contractor and to solicit proposals.
- A document that enables offeror's to clearly understand the government's needs for the work to be done in developing or producing the goods or services to be delivered by a contractor.
- A Government prepared document incorporated into the RFP that states the overall solicitation objectives.

Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO7.EO5 Describe key activities in steps 4, 5, and 6 of the RMF process.

Question 2 of 15.

Step 4 of the RMF process is Assessing Security Controls. Choose the three possible statuses of security controls listed below:

- [ ] Compliant
- [ ] Not Applicable
- [ ] Non-Compliant
- [ ] Deferred

- [ ] Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO2.EO3 Develop the Cyber Survivability Attributes in support of the Cyber Survivability Endorsement

Question 5 of 15.

Which choice below best defines the Cyber Survivability Attribute of Mitigate?

- Transferring cybersecurity risks to the contractor.
- Design requirements that detect and respond to cyber-attacks; enabling weapon systems functions resiliency to complete the mission.
- Design requirements that protect weapon system's functions from most likely and greatest risk cyber threats.
- Design requirements that ensure minimum cyber capability available to recover from cyber-attack and enable weapon system quickly restore full functionality.

Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO5.EO1 Describe why robust ICT SCRM practices are needed throughout acquisition programs.

Question 13 of 15.

Supply Chain Risk mitigating practices include which two of the following?

- [ ] Establishing a software chain of custody for the system's software critical components as they move through the supply chain.
- [ ] Non-malicious code insertion.
- [ ] Buying only Commercial Off the Shelf (COTS) products since they have already gone through the full testing process.
- [ ] Controlling access and configuration changes to critical components within the system development life cycle.

- [ ] Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO6.EO3 Identify the principles of DevSecOps

Question 3 of 15.

Choose the statement below that best defines DevSecOps:

- An organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops).
- A set of hardware and software development practices that combines software development (Dev) and information technology operations (Ops) to shorten the production time of key system components.
- A process that places a high level of emphasis on security and separates it from development to provide more focus.
- A culture of development that stressed collaboration and approaches quality as a gate.

Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO3.EO1 Describe the 6 phases of the cybersecurity T&E process as they progress throughout the progr

Question 7 of 15.

What statement below best describes the first step (Phase 1) of the Cybersecurity T&E process?

- Understand cybersecurity requirements & develop an initial approach/plan to conduct T&E.
- Cooperative Vulnerability and Penetration Assessment.
- Cooperative vulnerability identification to identify known cybersecurity vulnerabilities in hardware, software, interfaces, operations, and architecture; to assess the mission risk associated with those vulnerabilities.
- Characterize attack surface to identify where an attacker would access / exploit the system.

Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO5.EO3 Define SCRM activities across the program acquisition life cycle.

Question 14 of 15.

Choose the item below that is NOT associated with the TSN Analysis Methodology:

- Software Assurance
- Criticality Analysis
- Threat Assessment
- Vulnerability Assessment

Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO6.EO1 Identify the foundational principles of the Cybersecurity Maturity Model Certification (CMMC

Question 8 of 15.

The CMMC consists of five Process Levels and five levels of Practice. Choose the answer below that lists the five CMMC Process levels in order (Level 1 -5).

- □Performed; Documented; Managed; Reviewed; Optimizing
- Initial; Managed; Defined; Quantitatively Managed; Optimizing
- Project Management; Engineering; Process Management; Support; Logistics.
- Basic Cyber Hygiene (CH); Intermediate CH; Good CH; Proactive; Advanced/ Progressive

Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO6.EO2 Describe the cybersecurity considerations for obtaining Cloud services.

Question 15 of 15.

Which of the following is NOT a DoD CIO recommended activity when acquiring cloud services?

- Apply the DFARS rule to commercial cloud services.
- Apply the DoD Cloud Computing Security Requirements Guide (SRG)
- Perform an IT Business Case Analysis
- Use only government designed and developed cloud services

Mark for follow up

« Back | Save / Return Later | Summary

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO7.EO1 Identify the Program Manager's specific RMF roles and responsibilities.

Question 9 of 15.

Choose the three items below that are specific responsibilities of the Program Manager as it relates to the Risk Management Framework:

- [ ] Represent operational and functional requirements of the user community for a particular system during the RMF process.
- [ ] Ensure POA&M development, tracking, and resolution.
- [ ] Implement and assist the ISO in the maintenance and tracking of the security plan for assigned IS and PIT systems.
- [ ] Ensure periodic reviews, testing and assessment of assigned IS and PIT systems are conducted no less than annually.

- [ ] Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO5.EO2 Identify ICT SCRM Policy, guidance and technical execution resources relevant to an acquisit

Question 10 of 15.

Choose the two statements below that are goals of Trusted Systems and Networks (TSN) policy:

- [ ] Control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources.
- [ ] Eliminate all risks in the DoD supply chain.
- [ ] Reduce vulnerabilities in the system design through system security engineering.
- [ ] TSN policy shall be primarily addressed through Risk Management Framework controls.

- [ ] Mark for follow up

« Back | Save / Return Later | Summary | Next »

Test - CCYB 002 Cybersecurity for Program Managers Exam

TO3.EO4 Detail key activities that a PM should support to sustain a robust cybersecurity T&E program

Question 11 of 15.

Select the best definition of a cybersecurity kill chain:

- Reviewing the factors of a threat's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate.
- A best practice for programs to identify, estimate, assess, and prioritize cybersecurity risks.
- A weakness that could be exploited by a threat source.
- A framework for describing a broad range of activities that a cyber attacker may undertake when conducting an offensive against a target system.

Mark for follow up

« Back | Save / Return Later | Summary | Next »