2017 CAP Detailed Content Outline (DCO) with Weights
Effective Date: October 15, 2018

CAP 2017 Detailed Content Outline With Weights (For Public Release)		
Classification	Domain/Task/Subtask Statements	Weight
1	Information Security Risk Management Program	15%
1.1	Understand the Foundation of an Organization-Wide Information Security Risk Management Program	
1.1.1	Principles of information security	
1.1.2	National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)	
1.1.3	RMF and System Development Life Cycle (SDLC) integration	
1.1.4	Information System (IS) boundary requirements	
1.1.5	Approaches to security control allocation	
1.1.6	Roles and responsibilities in the authorization process	
1.2	Understand Risk Management Program Processes	
1.2.1	Enterprise program management controls	
1.2.2	Privacy requirements	
1.2.3	Third-party hosted Information Systems (IS)	
1.3	Understand Regulatory and Legal Requirements	
1.3.1	Federal information security requirements	
1.3.2	Relevant privacy legislation	
1.3.3	Other applicable security-related mandates	
2	Categorization of Information Systems (IS)	13%
2.1	Define the Information System (IS)	
2.1.1	Identify the boundary of the Information System (IS)	
2.1.2	Describe the architecture	
2.1.3	Describe Information System (IS) purpose and functionality	
2.2	Determine Categorization of the Information System (IS)	
2.2.1	Identify the information types processed, stored, or transmitted by the Information System (IS)	
2.2.2	Determine the impact level on confidentiality, integrity, and availability for each information type	
2.2.3	Determine Information System (IS) categorization and document results	
3	Selection of Security Controls	13%
3.1	Identify and Document Baseline and Inherited Controls	
3.2	Select and Tailor Security Controls	
3.2.1	Determine applicability of recommended baseline	
3.2.2	Determine appropriate use of overlays	
3.2.3	Document applicability of security controls	
3.3	Develop Security Control Monitoring Strategy	
3.4	Review and Approve Security Plan (SP)	
4	Implementation of Security Controls	15%
4.1	Implement Selected Security Controls	
4.1.1	Confirm that security controls are consistent with enterprise architecture	
4.1.2	Coordinate inherited controls implementation with common control providers	
4.1.3	Determine mandatory configuration settings and verify implementation (e.g., United States Government Configuration Baseline (USGCB), National Institute of Standards and Technology (NIST) checklists, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) benchmarks)	
4.1.4	Determine compensating security controls	
4.2	Document Security Control Implementation	
4.2.1	Capture planned inputs, expected behavior, and expected outputs of security controls	
4.2.2	Verify documented details are in line with the purpose, scope, and impact of the Information System (IS)	
4.2.3	Obtain implementation information from appropriate organization entities (e.g., physical security, personnel security)	
5	Assessment of Security Controls	14%
5.1	Prepare for Security Control Assessment (SCA)	
5.1.1	Determine Security Control Assessor (SCA) requirements	
5.1.2	Establish objectives and scope	
5.1.3	Determine methods and level of effort	

5.1.4	Determine necessary resources and logistics	
5.1.5	Collect and review artifacts (e.g., previous assessments, system documentation, policies)	
5.1.6	Finalize Security Control Assessment (SCA) plan	
5.2	Conduct Security Control Assessment (SCA)	
5.2.1	Assess security control using standard assessment methods	
5.2.2	Collect and inventory assessment evidence	
5.3	Prepare Initial Security Assessment Report (SAR)	
5.3.1	Analyze assessment results and identify weaknesses	
5.3.2	Propose remediation actions	
5.4	Review Interim Security Assessment Report (SAR) and Perform Initial Remediation Actions	
5.4.1	Determine initial risk responses	
5.4.2	Apply initial remediations	
5.4.3	Reassess and validate the remediated controls	
5.5	Develop Final Security Assessment Report (SAR) and Optional Addendum	
6	Authorization of Information Systems (IS)	14%
6.1	Develop Plan of Action and Milestones (POAM)	
6.1.1	Analyze identified weaknesses or deficiencies	
6.1.2	Prioritize responses based on risk level	
6.1.3	Formulate remediation plans	
6.1.4	Identify resources required to remediate deficiencies	
6.1.5	Develop schedule for remediation activities	
6.2	Assemble Security Authorization Package	
6.2.1	Compile required security documentation for Authorizing Official (AO)	
6.3	Determine Information System (IS) Risk	
6.3.1	Evaluate Information System (IS) risk	
6.3.2	Determine risk response options (i.e., accept, avoid, transfer, mitigate, share)	
6.4	Make Security Authorization Decision	
6.4.1	Determine terms of authorization	
7	Continuous Monitoring	16%
7.1	Determine Security Impact of Changes to Information System (IS) and Environment	
7.1.1	Understand configuration management processes	
7.1.2	Analyze risk due to proposed changes	
7.1.3	Validate that changes have been correctly implemented	
7.2	Perform Ongoing Security Control Assessments (SCA)	
7.2.1	Determine specific monitoring tasks and frequency based on the agency's strategy	
7.2.2	Perform security control assessments based on monitoring strategy	
7.2.3	Evaluate security status of common and hybrid controls and interconnections	
7.3	Conduct Ongoing Remediation Actions (e.g., resulting from incidents, vulnerability scans, audits, vendor updates)	
7.3.1	Assess risk(s)	
7.3.2	Formulate remediation plan(s)	
7.3.3	Conduct remediation tasks	
7.4	Update Documentation	
7.4.1	Determine which documents require updates based on results of the continuous monitoring process	
7.5	Perform Periodic Security Status Reporting	
7.5.1	Determine reporting requirements	
7.6	Perform Ongoing Information System (IS) Risk Acceptance	
7.6.1	Determine ongoing Information System (IS)	
7.7	Decommission Information System (IS)	
7.7.1	Determine Information System (IS) decommissioning requirements	
7.7.2	Communicate decommissioning of Information System (IS)	