



Certified
Authorization Professional

An (ISC)² Certification

Domain Refresh

Effective Date: August 15, 2021

*Please note: **The CAP Exam Outline** is the official document outlining the domains, weights and subdomains of the certification exam. This document is intended as a supplementary resource only.*

CAP Domain Refresh

On August 15, 2021, the domains for the (ISC)² CAP[®] credential exam will be refreshed.

The content of the CAP will be refreshed to reflect the most pertinent issues that cybersecurity professionals currently face. These enhancements are the result of a rigorous, methodical process that (ISC)² follows to routinely update its credential exams. This process ensures that the examinations and subsequent continuing professional education requirements encompass the topic areas relevant to the roles and responsibilities of today's practicing cybersecurity professional.

As a result of the content refresh, the domain and subdomain names have been updated to describe the topics accurately. The weights for the domains have also changed. Please see the comparison table below.

Effective: August 15, 2021	
Domain 1: Information Security Risk Management Program	16%
Domain 2: Scope of the Information System	11%
Domain 3: Selection and Approval of Security and Privacy Controls	15%
Domain 4: Implementation of Security and Privacy Controls	16%
Domain 5: Assessment/Audit of Security and Privacy Controls	16%
Domain 6: Authorization/Approval of Information System	10%
Domain 7: Continuous Monitoring	16%
Total:	100%

Domain Comparison

October 15, 2018 – August 14, 2021	Effective August 15, 2021
Domain 1: Information Security Risk Management Program	Domain 1: Information Security Risk Management Program
<ul style="list-style-type: none"> Understand the foundation of an organization-wide information security risk management program Understand risk management program processes Understand regulatory and legal requirements 	<ul style="list-style-type: none"> Understand the foundation of an organization information security risk management program Understand risk management program processes Understand regulatory and legal requirements
Exam Weight: 15%	Exam Weight: 16%
October 15, 2018 – August 14, 2021	Effective August 15, 2021
Domain 2: Categorization of Information Systems (IS)	Domain 2: Scope of the Information System
<ul style="list-style-type: none"> Define the information system (IS) Determine categorization of the information systems (IS) 	<ul style="list-style-type: none"> Define the information system Determine categorization of the information system
Exam Weight: 13%	Exam Weight: 11%

October 15, 2018 – August 14, 2021	Effective August 15, 2021
Domain 3: Selection of Security Controls	Domain 3: Selection and Approval of Security and Privacy Controls
<ul style="list-style-type: none"> Identify and document baseline and inherited controls Select and tailor security controls Develop security control monitoring strategy Review and approve Security Plan (SP) 	<ul style="list-style-type: none"> Identify and document baseline and inherited controls Select and tailor controls to the system Develop continuous control monitoring strategy (e.g., implementation, timeline, effectiveness) Review and approve security plan/ Information Security Management System (ISMS)
Exam Weight: 13%	Exam Weight: 15%

October 15, 2018 – August 14, 2021	Effective August 15, 2021
Domain 4: Implementation of Security Controls	Domain 4: Implementation of Security and Privacy Controls
<ul style="list-style-type: none"> Implement selected security controls Document security control implementation 	<ul style="list-style-type: none"> Implement selected controls Document control implementation
Exam Weight: 15%	Exam Weight: 16%

October 15, 2018 – August 14, 2021	Effective August 15, 2021
Domain 5: Assessment of Security Controls	Domain 5: Assessment/Audit of Security and Privacy Controls
<ul style="list-style-type: none"> • Prepare for Security Control Assessment (SCA) • Conduct Security Control Assessment (SCA) • Prepare initial Security Assessment Report (SAR) • Review interim Security Assessment Report (SAR) and perform initial remediation actions • Develop final Security Assessment Report (SAR) and optional addendum 	<ul style="list-style-type: none"> • Prepare for assessment/audit • Conduct assessment/audit • Prepare the initial assessment/audit report • Review initial assessment/audit report and perform remediation actions • Develop final assessment/audit report • Develop remediation plan
Exam Weight: 14%	Exam Weight: 16%

October 15, 2018 – August 14, 2021	Effective August 15, 2021
Domain 6: Authorization of Information Systems (IS)	Domain 6: Authorization/Approval of Information System
<ul style="list-style-type: none"> • Develop Plan of Action and Milestones (POAM) • Assemble security authorization package • Determine Information Systems (IS) risk • Make security authorization decision 	<ul style="list-style-type: none"> • Compile security and privacy authorization/approval documents • Determine information system risk • Authorize/approve information system
Exam Weight: 14%	Exam Weight: 10%

October 15, 2018 – August 14, 2021	Effective August 15, 2021
Domain 7: Continuous Monitoring	Domain 7: Continuous Monitoring
<ul style="list-style-type: none"> • Determine security impact of changes to Information Systems (IS) and environment • Perform ongoing Security Control Assessments (SCA) • Conduct ongoing remediation actions (e.g., resulting from incidents, vulnerability scans, audits, vendor updates) • Update documentation • Perform periodic security status reporting • Perform ongoing Information System (IS) risk acceptance • Decommission Information System (IS) 	<ul style="list-style-type: none"> • Determine impact of changes to information system and environment • Perform ongoing assessments/audits based on organizational requirements • Review supply chain risk analysis monitoring activities (e.g., cyber threat reports, agency reports, news reports) • Actively participate in response planning and communication of a cyber event • Revise monitoring strategies based on changes to industry developments introduced through legal, regulatory, supplier, security and privacy updates • Keep designated officials updated about the risk posture for continuous authorization/approval • Decommission information system
Exam Weight: 16%	Exam Weight: 16%

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that CAP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

Any Questions?

(ISC)² Americas

Tel: +1.866.331.ISC2 (4722)

Email: membersupport@isc2.org

(ISC)² Asia-Pacific

Tel: +852.2850.6951/+852.2850.6959

Email: membersupportapac@isc2.org

(ISC)² EMEA

Tel: +44 (0)203.960.7800

Email: membersupportemea@isc2.org