Uniform CPA Examination Information Systems and Controls (ISC)

Blueprint

AICPA®

Table of Contents

Uniform CPA Examination Blueprints

The CPA licensure model requires all candidates to pass three Core exam sections and one Discipline exam section of a candidate's choosing. The Uniform CPA Examination (the Exam) has been designed accordingly as reflected in the Exam Blueprints. The Core exam sections assess the knowledge and skills that all newly licensed CPAs (nlCPAs) need in their role to protect the public interest. The Discipline exam sections assess the knowledge and skills in the respective Discipline domain applicable to nlCPAs in their role to protect the public interest.

The three Core exam sections, each four hours long, are: Auditing and Attestation (AUD), Financial Accounting and Reporting (FAR) and Taxation and Regulation (REG). The three Discipline exam sections, each four hours long, are: Business Analysis and Reporting (BAR), Information Systems and Controls (ISC) and Tax Compliance and Planning (TCP).

The table below presents the design of the Exam by Core and Discipline section, section time and question type.

Section	Section Time	Multiple-Choice Questions (MCQs)	Tasked-Based Simulations (TBSs)
AUD – Core	4 hours	78	7
FAR – Core	4 hours	50	7
REG – Core	4 hours	72	8
BAR – Discipline	4 hours	50	7
ISC – Discipline	4 hours	82	6
TCP – Discipline	4 hours	68	7

The table below presents the scoring weight of MCQs and TBSs for each Core and Discipline Exam section.

	Score Weighting	
Section	Multiple-Choice Questions (MCQs)	Tasked-Based Simulations (TBSs)
AUD – Core	50%	50%
FAR – Core	50%	50%
REG – Core	50%	50%
BAR – Discipline	50%	50%
ISC – Discipline	60%	40%
TCP – Discipline	50%	50%

The AICPA adopted a skill framework for the Exam based on the revised Bloom's Taxonomy of Educational Objectives[1]. Bloom's Taxonomy classifies a continuum of skills that students can be expected to learn and demonstrate.

[1] Revised taxonomy see Anderson, L.W. (Ed.), Krathwohl, D.R. (Ed.), Airasian, P.W., Cruikshank, K.A., Mayer, R.E., Pintrich, P.R., Raths, J., & Wittrock, M.C. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's Taxonomy of Educational Objectives (Complete Edition). New York: Longman. For original taxonomy see Bloom, B.S. (Ed.), Engelhart, M.D., Furst, E.J., Hill, W.H., & Krathwohl, D.R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook 1: Cognitive domain. New York: David McKay.

Uniform CPA Examination Blueprints (continued)

Representative tasks that are critical to an nlCPA's role in protecting the public interest have been identified. The representative tasks combine both the applicable content knowledge and skills required in the context of the work of an nlCPA. Based on the nature of a task, one of four skill levels, derived from the revised Bloom's Taxonomy, is assigned to each of the tasks, as follows:

Skill Levels	
Evaluation	The examination or assessment of problems, and use of judgment to draw conclusions.
Analysis	The examination and study of the interrelationships of separate areas in order to identify causes and find evidence to support inferences.
Application	The use or demonstration of knowledge, concepts or techniques.
Remembering and Understanding	The perception and comprehension of the significance of an area utilizing knowledge gained.

The skill levels to be assessed on each Core and Discipline section of the Exam are included in the table below.

Section	Remembering and Understanding	Application	Analysis	Evaluation
AUD – Core	30–40%	30–40%	15–25%	5–15%
FAR – Core	5–15%	45–55%	35–45%	–
REG – Core	25–35%	35–45%	25–35%	–
BAR – Discipline	10–20%	45–55%	30–40%	–
ISC – Discipline	55–65%	20–30%	10–20%	–
TCP – Discipline	5–15%	55–65%	25–35%	–

Each section of the Exam has a section introduction and a corresponding section blueprint.

- The **section introduction** outlines the scope of the section, the content organization and tasks, the content allocation, the overview of content areas, section assumptions, the skill allocation and a listing of the section's applicable reference literature.
- The **section blueprint** outlines the content to be tested, the associated skill level to be tested and representative tasks an nlCPA would likely encounter. The blueprints are organized by content AREA, content GROUP and content TOPIC. Each topic includes one or more representative TASKS that an nlCPA may be expected to complete.

The purpose of the blueprint is to:

- Document the minimum level of knowledge and skills necessary for initial licensure.
- Assist candidates in preparing for the Exam by outlining the knowledge and skills that may be tested.
- Apprise educators about the knowledge and skills candidates will need to function as nlCPAs.
- Guide the development of Exam questions.

The tasks in the blueprints are representative and are not intended to be (nor should they be viewed as) an all-inclusive list of tasks that may be tested on the Exam. The number of tasks associated with a particular content group or topic is not indicative of the extent such content group, topic or related skill level will be assessed on the Exam.

Information Systems and Controls

The Information System and Controls (ISC) section of the Uniform CPA Examination (the Exam) tests the knowledge and skills that nICPAs must demonstrate with respect to information systems, including processing integrity, availability, security, confidentiality and privacy. Inherent in the analysis of controls in each of these subjects is awareness of the risks that the entity is intending to mitigate through the use of those controls.

The ISC section also tests the knowledge and skills that nICPAs must demonstrate with respect to data management, including data collection, storage and usage throughout the data life cycle.

The ISC section of the exam focuses on information technology (IT) audit and advisory, including System and Organization Controls (SOC) engagements. With respect to SOC engagements, the ISC section primarily focuses on:

- The use of the Description Criteria for a Description of a Service Organization's System and Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy in planning, performing and reporting in a SOC 2® engagement.
- Planning, certain procedures (excluding the testing of internal controls over financial reporting) and reporting on a SOC 1® engagement.

The assessment will also incorporate applied research with a focus on reviewing and using excerpts of source materials (e.g., standards, regulations, frameworks) to complete a range of tasks including identifying issues, analyzing facts and determining appropriate responses.

A list of reference materials relevant to the ISC section of the Exam is included under References at the conclusion of this introduction.

Content organization and tasks

The ISC section blueprint is organized by content AREA, content GROUP and content TOPIC. Each topic includes one or more representative TASKS that an nICPA may be expected to complete when performing assurance or advisory services relative to an entity's business processes, information systems, data management and security.

The tasks in the blueprint are representative. They are not intended to be (nor should they be viewed as) an all-inclusive list of tasks that may be tested in the ISC section of the Exam. Lists or examples included within the text of a representative task beginning with the word "including" are not intended to be exhaustive. Within some representative tasks are parenthetical lists. If a parenthetical list begins with "e.g.", this is not intended to be an exhaustive list but rather examples of the types of content that could be assessed. Parenthetical lists that do not include "e.g." are intended to be an exhaustive list of the content to be assessed with respect to that representative task.

Content allocation

The following table summarizes the content areas and the allocation of content tested in the ISC section of the Exam:

Content area		Allocation
Area I	Information Systems and Data Management	35–45%
Area II	Security, Confidentiality and Privacy	35–45%
Area III	Considerations for System and Organization Controls (SOC) Engagements	15–25%

Information Systems and Controls (continued)

Overview of content areas

Area I of the ISC section blueprint is focused on information systems and data management in a modern context, recognizing that much of it is cloud-based and undergoing rapid innovation. The Area includes the following:

- IT architecture components and the use of cloud-based models for IT infrastructure, platforms and services.
- Enterprise and accounting information systems, the business processes they enable and controls over processing integrity.
- System availability and IT change management.
- Data collection, storage, structured query language (SQL) queries and integration of data from different data sources.
- Business process models.

While certain representative tasks in Area I relate to testing controls in a SOC 2® engagement context, they are representative of similar procedures that may be performed in other IT audit and advisory contexts.

Area II of the ISC section blueprint covers security, confidentiality and privacy. The Area includes the following:

- Select portions of specified regulations, standards and frameworks related to information security and privacy that are considered by management in designing and implementing information systems and related controls.
- Types of threats and attacks (including cyber) to which an entity may be subject.
- Controls the entity uses to prevent, detect and respond to those threats and attacks.
- Controls the entity uses to maintain the confidentiality and privacy of information.
- Testing an entity's controls over security, confidentiality and privacy.
- An entity's incident response plan.

Group A covers foundational knowledge of certain regulations, standards and frameworks related to security, confidentiality and privacy at a Remembering and Understanding level. Those regulations, standards and frameworks underpin the higher-order skill testing in Group B – Security, Group C – Confidentiality and Privacy and Group D – Incident Response.

While certain representative tasks in Area II relate to testing controls in a SOC 2® engagement context, they are representative of similar procedures that may be performed in other IT audit and advisory contexts.

Area III of the ISC section blueprint covers considerations for SOC engagements. This area focuses on aspects that are unique considerations in SOC engagements distinct from other types of attestation engagements. The Area includes the following:

- Form, content and management assertions in SOC 1®, SOC 2® and SOC 3® reports and the intended users of those reports.
- Aspects of engagement planning and reporting for SOC 1® and SOC 2® engagements.
- Procedures related to complementary user entity controls and complementary subservice organization controls.
- Procedures related to the system description criteria for SOC 1® and SOC 2® engagements.
- Trust services criteria for SOC 2® engagements.

Section assumptions

The ISC section of the Exam includes multiple-choice questions and task-based simulations. Candidates should assume that the information provided in each question is material and should apply all stated assumptions.

Information Systems and Controls (continued)

Skill allocation

The Exam applies a skill framework based on the revised Bloom's Taxonomy of Educational Objectives[6]. Bloom's Taxonomy classifies a continuum of skills depicted in the table below:

Skill Levels	
Evaluation	The examination or assessment of problems, and use of judgment to draw conclusions.
Analysis	The examination and study of the interrelationships of separate areas in order to identify causes and find evidence to support inferences.
Application	The use or demonstration of knowledge, concepts or techniques.
Remembering and Understanding	The perception and comprehension of the significance of an area utilizing knowledge gained.

The ISC section of the Exam assesses content at the first three skill levels of Bloom's Taxonomy as described below:

- Remembering and Understanding skills are tested across all areas. These areas contain foundational knowledge that nlCPAs are expected to possess related to standards, regulations, frameworks and procedures.
- Application skills are tested across all areas. These areas contain tasks that nlCPAs are expected to perform related to examining information systems, data management and SOC engagements.
- Analysis skills are tested in Area I and Area II. These areas contain tasks that nlCPAs are expected to perform related to detecting deficiencies in the suitability or design and deviations in the operation of controls related to information systems.

The representative tasks combine both the applicable content knowledge and the skills required in the context of the work that an nlCPA would reasonably be expected to perform.

References — Information Systems and Controls

The subject matter covered in the ISC section is subject to rapid change. The References detailed below are the sources of the subject matter eligible for assessment in the ISC section, to the extent that the subject matter is included in the blueprint's content areas, groups and topics. Further, the assessment of the subject matter described in a representative task that identifies an organization, publication, law, regulation, standard or framework is limited to the specific sections of the References detailed below. For example, a representative task that refers to a Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework is limited to the COSO guides listed below.

- AICPA
  - 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus 2022) (Trust Services Criteria)
  - 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® (with Revised Implementation Guidance 2022)
  - Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program
  - Frequently asked questions – SOC 2® and SOC 3® examinations
  - Materiality considerations for attestation engagements involving aspects of subject matters that cannot be quantitatively measured
  - Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®) – Guide

[6] Revised taxonomy see Anderson, L.W. (Ed.), Krathwohl, D.R. (Ed.), Airasian, P.W., Cruikshank, K.A., Mayer, R.E., Pintrich, P.R., Raths, J., & Wittrock, M.C. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's Taxonomy of Educational Objectives (Complete Edition). New York: Longman. For original taxonomy see Bloom, B.S. (Ed.), Engelhart, M.D., Furst, E.J., Hill, W.H., & Krathwohl, D.R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook 1: Cognitive domain. New York: David McKay.

Information Systems and Controls (continued)

  - SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy
  - Statements on Standards for Attestation Engagements and Interpretations
- Center for Internet Security (CIS), CIS Controls; Version 8
  - "Overview" and "Why is this Control critical?" sections of each control (Control 01 to Control 18)
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Blockchain and Internal Control: The COSO Perspective
  - Enterprise Risk Management for Cloud Computing
  - Managing Cyber Risk in a Digital Age
- Cybersecurity & Infrastructure Security Agency (CISA)
  - Security Tips published by the National Cyber Awareness System (NCAS), released or revised subsequent to November 1, 2019 that are relevant to the Groups and Topics in Area I and Area II, limited to the information in the tip itself, and not extending to the underlying referenced material
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR Part 164 Security and Privacy
  - Section 164.103 through Section 164.530 excluding Implementation Specifications and Compliance Dates
- ISACA
  - COBIT 2019 Framework: Introduction and Methodology, Chapters 1 through 5
  - White papers available to the public free of charge that address subject matters covered in the groups and topics of ISC Area I and Area II
- National Institute of Standards and Technology (NIST)
  - Framework for Improving Critical Infrastructure Cybersecurity (CSF) Version 1.1, Sections 1 and 2, including the glossary definitions of terms used in those sections
  - NIST Privacy Framework: A Tool For Improving Privacy through Enterprise Risk Management; Version 1.0, Sections 1 and 2, including the glossary definitions of terms used in those sections
  - Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53 (SP 800-53) Revision 5, Chapters 1 and 2, including the glossary definitions of terms used in those sections
- PCI Security Standards Council Payment Card Industry Data Security Standard (PCI DSS)
  - PCI DSS v4.0 Quick Reference Guide, Importance of Protecting Payment Account Data with the PCI Data Security Standard and Overview of PCI SSC Standards
- Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)
  - Articles 4 through 34
- Textbooks
  - Accounting Information Systems
  - Data Confidentiality and Privacy
  - Data Literacy
  - Data Management
  - Incident Response and Disaster Recovery
  - Information Security / Cyber Security
  - Information Systems
  - Information Technology (IT)
  - IT Audit and Assurance

Summary Blueprint

Content area allocation	Weight
I. Information Systems and Data Management	35–45%
II. Security, Confidentiality and Privacy	35–45%
III. Considerations for System and Organization Controls (SOC) Engagements	15–25%

Skill allocation	Weight
Evaluation	–
Analysis	10–20%
Application	20–30%
Remembering and Understanding	55–65%

The following pages include the detailed blueprints that define the areas, groups, topics and representative tasks for the ISC section. It is important to note that the number of representative tasks associated with a particular content group or topic is not indicative of the extent to which such content group, topic or related skill level will be assessed on the Exam (i.e., more numerous tasks in a particular group, topic or skill compared to another should not infer more content weight assigned to that group, topic or skill).

Area I – Information Systems and Data Management (35–45%)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
A. Information systems					
1. IT infrastructure	✓				Explain the purpose and recognize examples of key components of IT architecture (e.g., operating systems, servers, network infrastructure, end-user devices).
	✓				Explain cloud computing, including cloud computing models (infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS)) and deployment models (e.g., public, private, hybrid).
	✓				Summarize the role and responsibilities of cloud service providers.
	✓				Explain how the COSO frameworks address cloud computing governance.
2. Enterprise and accounting information systems	✓				Summarize enterprise resource planning (ERP) and accounting information systems, what they encompass and how they interact.
	✓				Explain how the COSO internal control framework can be used to evaluate risks related to the use of blockchain in the context of financial reporting and to design and implement controls to address such risks.
		✓			Determine potential changes to business processes to improve the performance of an accounting information system (e.g., robotic process automation, outsourcing, system changes).
			✓		Reconcile the actual sequence of steps and the information, documents, tools and technology used in a key business process of an accounting information system (e.g., sales, cash collections, purchasing, disbursements, human resources, payroll, production, treasury, fixed assets, general ledger, reporting) to the documented process (e.g., flowchart, business process diagram, narrative).
			✓		Detect deficiencies in the suitability or design and deviations in the operation of controls related to an information system's processing integrity in a SOC 2® engagement using the Trust Services Criteria.

Area I – Information Systems and Data Management (35–45%) (continued)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
A. Information systems (continued)					
3. Availability	✓				Recall the scope, purpose and key considerations for business resiliency, disaster recovery and business continuity plans.
	✓				Explain the objectives of mirroring and replication.
	✓				Summarize steps in a business impact analysis.
	✓				Recall measures of system availability (e.g., agreed service time, downtime).
		✓			Determine the appropriateness of the organization's data backup types (e.g., full, incremental, differential) including recovery considerations.
			✓		Detect deficiencies in the suitability or design and deviations in the operation of controls related to a service organization's availability service commitments and system requirements in a SOC 2® engagement using the Trust Services Criteria.
4. Change management	✓				Explain the purpose of change management related to internal hardware and software applications, including the risks and the different types of documentation used (e.g., system component inventory, baseline configuration).
	✓				Explain the different environments used (e.g., development, staging, production) and the types of tests performed (e.g., unit, integration, system, acceptance).
	✓				Explain the approaches than can be used when converting to a new information system (e.g., direct, parallel, pilot).
	✓				Explain patch management.
		✓			Test the design and implementation of change control policies (e.g., acceptance criteria, test results, logging, monitoring) for IT resources (e.g., applications, infrastructure components, configurations) in organizations, including those that have adopted continuous integration and continuous deployment processes.

Area I – Information Systems and Data Management (35–45%) (continued)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
B. Data management					
	✓				Identify data collection methods and techniques.
	✓				Define the various types of data storage (e.g., data warehouse, data lake, data mart) and database schemas (e.g., star, snowflake).
	✓				Summarize the data life cycle (i.e., the span of the use of information, from creation, through active use, storage and final disposition).
		✓			Examine a relational database's structure to determine whether it applies data integrity rules, uses a data dictionary, and normalizes the data.
		✓			Examine a standard SQL query (common commands, clauses, operators, aggregate functions and string functions) to determine whether the retrieved data set is relevant and complete.
			✓		Integrate the data available from different data sources to provide information necessary for financial and operational analysis and decisions.
			✓		Investigate a business process model (e.g., flowchart, data flow diagram, business process model and notation (BPMN) diagram) to identify potential improvements.

Area II – Security, Confidentiality and Privacy (35–45%)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
A. Regulations, standards and frameworks					
	✓				Recall the covered entities and permitted uses and disclosures of the HIPAA Security and Privacy Rules.
	✓				Recall the scope of the GDPR and the six principles and key concepts for personal data.
	✓				Recall the requirements of the PCI DSS.
	✓				Recall the three parts of the NIST CSF (Framework Core, Framework Implementation Tiers, Framework Profiles).
	✓				Recall the three parts of the NIST Privacy Framework (Framework Core, Framework Profiles, Framework Implementation Tiers).
	✓				Recall the purpose, applicability, target audience and organizational responsibilities of NIST SP 800-53.
	✓				Recall the overview of each CIS Control.
	✓				Recall the governance system principles, governance framework principles and the components of a governance system according to COBIT 2019.
B. Security					
1. Threats and attacks	✓				Classify the different types of threat agents (e.g., internal or external, nation or non-nation state-sponsored, adversary, threat actors, attacker or hacker).
	✓				Identify types of attacks (e.g., physical, distributed denial of service, malware, social engineering, web application attacks, mobile device attacks).
	✓				Identify techniques used in a cyber-attack (e.g., buffer overflow, mobile code, cross-site scripting, SQL injections, race conditions, covert channel, replay and return-oriented attack).

Area II – Security, Confidentiality and Privacy (35–45%) (continued)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
B. Security (continued)					
1. Threats and attacks (continued)	✓				Explain the stages in a cyber-attack (e.g., reconnaissance, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
	✓				Identify the cybersecurity risks related to using cloud environments, platforms and services.
	✓				Identify the cybersecurity risks related to the Internet of Things (IoT).
	✓				Identify the cybersecurity risks related to mobile technologies.
	✓				Explain threat modeling and threat landscape.
		✓			Determine the specific cybersecurity threats in an organization's connections with customers, vendors and partner organizations.
		✓			Determine the specific cybersecurity threats to an organization's on-premise and cloud-based applications, networks and connected devices (e.g., mobile and Internet of Things (IOT) devices).
2. Mitigation	✓				Identify ways to protect networks and devices used to access the network remotely (e.g., isolation and segmentation, virtual private network (VPN), wireless network security, endpoint security, system hardening, intrusion prevention and detection systems).
	✓				Recall the definition and purpose of vulnerability management.
	✓				Explain the concepts of layered security and defense-in-depth.
	✓				Define the concepts of least-privilege, zero-trust, whitelisting and the need-to-know principle.
	✓				Recall the purpose and content of a technology acceptable use policy including considerations specific to mobile technologies and bring-your-own-device (BYOD).

Area II – Security, Confidentiality and Privacy (35–45%) (continued)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
B. Security (continued)					
2. Mitigation (continued)	✓				Explain how the COSO frameworks can be used to assess cyber risks and controls.
		✓			Determine the common preventive, detective or corrective controls (e.g., intrusion prevention systems, device and software hardening, log analysis, intrusion detection systems, virus quarantining, patches) to mitigate risk of cyber-attacks for an organization.
		✓			Determine the appropriate identification and authentication techniques and technologies (e.g., password management, single sign-on, multi-factor authentication, personal identification number (PIN) management, digital signatures, smart cards, biometrics) in a specific scenario.
		✓			Determine the appropriate authorization model (e.g., discretionary, role-based, mandatory) and the controls (e.g., access control list, account restrictions, physical barriers) used to implement the model in a specific scenario.
3. Testing		✓			Perform procedures to obtain an understanding how the entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.
		✓			Provide input into a security assessment report by documenting the issues, findings and recommendations identified while performing tests of controls.
			✓		Perform a walkthrough of an organization's procedures relevant to IT security (e.g., IT risk management, human resources, training and education) and compare the observed procedure with the documented policy requirement.
			✓		Detect deficiencies in the suitability or design and deviations in the operation of controls related to a service organization's security service commitments and system requirements in a SOC 2® engagement using the Trust Services Criteria.

Area II – Security, Confidentiality and Privacy (35–45%) (continued)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
C. Confidentiality and privacy					
	✓				Explain encryption fundamentals, techniques and applications.
	✓				Recall the differences between confidentiality and privacy.
	✓				Identify methods for the protection of confidential data during the design, development, testing and implementation of applications that use confidential data (e.g., data obfuscation, tokenization).
	✓				Explain Data Loss Prevention (DLP).
	✓				Identify financial and operational implications of a data breach.
		✓			Determine controls and data management practices to securely collect, process, store, transmit and delete confidential data or data subject to privacy regulations.
			✓		Detect deficiencies in the suitability or design and deviations in the operation of controls related to a service organization's confidentiality and privacy service commitments and system requirements in a SOC 2® engagement using the Trust Services Criteria.
			✓		Perform a walkthrough of an organization's procedures relevant to confidentiality and privacy (e.g., IT risk management, human resources, training and education) and compare the observed procedure with the documented policy requirement.
D. Incident response					
	✓				Recall the differences between security/cybersecurity events and incidents.
	✓				Explain the use of insurance as a mitigation strategy for a security incident or data breach.
	✓				Summarize contents commonly included in incident response plans (e.g., roles, responsibilities, methods, steps, timelines).
		✓			Perform procedures to test whether the entity responded to cybersecurity incidents in accordance with the incident response plan.

Area III – Considerations for System and Organization Controls (SOC) Engagements (15–25%)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
A. Considerations specific to planning and performing a SOC engagement					
	✓				Explain the purpose of the Trust Services Criteria and its organization (e.g., alignment with the COSO Internal Control – Integrated Framework, supplemental criteria, common criteria and additional specific criteria).
	✓				Recall the types of subject matters a practitioner may be engaged to report on using the Trust Services Criteria.
	✓				Identify management assertions specific to the different categories and types (Type 1 and Type 2) of SOC engagements (SOC 1®, SOC 2®, SOC 3®).
	✓				Recall the intended users of SOC 1®, SOC 2® and SOC 3® reports.
	✓				Summarize the independence considerations between the service auditor, service organization and subservice organizations.
	✓				Explain how materiality is determined and used in performing a SOC engagement (SOC 1®, SOC 2®).
	✓				Identify the risk assessment requirements for a service organization and the service auditor.
	✓				Summarize the criteria for a vendor to be considered a subservice organization.
	✓				Explain the considerations for deciding between, and use of, the inclusive and carve-out method for subservice organizations and complementary subservice organization controls (CSOCs).
	✓				Define service commitments and system requirements in a SOC 2® engagement and how they correspond to an entity's objectives referred to in the Trust Services Criteria.

Area III – Considerations for System and Organization Controls (SOC) Engagements (15–25%) (continued)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
A. Considerations specific to planning and performing a SOC engagement (continued)					
	✓				Recall the impact of subsequently discovered facts on the SOC engagement (SOC 1®, SOC 2®).
	✓				Explain the purpose and common sections of a system description subject to SOC 1® or SOC 2® engagements.
	✓				Recall the Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program.
	✓				Explain the purpose of complementary user entity controls (CUECs) identified by service organization management in their system description.
	✓				Recall requirements about obtaining management's written representations in a SOC engagement (SOC 1®, SOC 2®).
		✓			Obtain an understanding of the system addressed by a SOC 2® engagement, including the clear identification of the boundaries of the system as defined by the service organization.
		✓			Perform procedures to obtain an understanding of how a service organization provides its personnel and external users information on how to report failures, incidents, concerns and other complaints related to a system subject to a SOC 2® engagement.
		✓			Prepare a comparison of management's system description to suitable criteria in a SOC 1® engagement or to the description criteria in a SOC 2® engagement.
		✓			Determine the effect of subsequent events in a SOC 1® or SOC 2® engagement.

Area III – Considerations for System and Organization Controls (SOC) Engagements (15–25%) (continued)

Content group/topic	Skill				Representative Task
	Remembering & Understanding	Application	Analysis	Evaluation	
B. Considerations specific to reporting on a SOC engagement					
	✓				Explain the effect of CUECs on the SOC report (SOC 1®, SOC 2®).
	✓				Summarize the carve-out vs. the inclusive method of reporting on CSOCs.
	✓				Explain the types of opinions and report modifications when deficiencies have been identified.
		✓			Prepare results of testing of controls to be included in the SOC 2® report of the test of a control, including when there was an exception identified by the test.
		✓			Determine the appropriate form and content of a report on the examination of controls at a service organization (SOC 1®, SOC 2®).