The CIA Specialty Challenge Exam Pricing Structure*:

English

First time		Retake	
Members	**Non-members**	**Members**	**Non-members**
$895	$1,095	$595	$795
▪ Application ▪ Registration ▪ Customized digital format of The IIA's CIA Learning System® (access valid for 12 months)	▪ Application ▪ Registration ▪ Customized digital format of The IIA's CIA Learning System® (access valid for 12 months).	▪ Registration	▪ Registration

Chinese Traditional, Japanese, Portuguese, Spanish, Turkish exams

First time		Retake	
Members	**Non-members**	**Members**	**Non-members**
$695	$895	$595	$795
▪ Application ▪ Registration	▪ Application ▪ Registration	▪ Registration	▪ Registration

*All prices are in USD. *The English CIA Specialty Challenge Exam bundle includes the customized CIA Learning System in a digital format. The bundle for the Chinese-Traditional, Japanese, Portuguese, Spanish, and Turkish CIA Specialty Challenge Exams will not include the customized CIA Learning System.*

Appendix A

CIA Specialty Challenge Exam Syllabus

All exam topics are tested at proficiency level unless otherwise indicated.

I. Essentials of Internal Auditing (30%)
A. Foundations of Internal Auditing
1. Interpret The IIA's Mission of Internal Audit, Definition of Internal Auditing, and Core Principles for the Professional Practice of Internal Auditing, and the purpose, authority, and responsibility of the internal audit activity
2. Explain the requirements of an internal audit charter (required components, board approval, communication of the charter, etc.) – Basic Level (B)
3. Interpret the difference between assurance and consulting services provided by the internal audit activity
4. Demonstrate conformance with the IIA Code of Ethics
B. Independence and Objectivity
1. Interpret organizational independence of the internal audit activity (importance of independence, functional reporting, etc.) – (B)
2. Identify whether the internal audit activity has any impairments to its independence – (B)
3. Assess and maintain an individual internal auditor's objectivity, including determining whether an individual internal auditor has any impairments to his/her objectivity
4. Analyze policies that promote objectivity
C. Proficiency and Due Professional Care
1. Recognize the knowledge, skills, and competencies required (whether developed or procured) to fulfill the responsibilities of the internal audit activity – (B)
2. Demonstrate the knowledge and competencies that an internal auditor needs to possess to perform his/her individual responsibilities, including technical skills and soft skills (communication skills, critical thinking, persuasion/negotiation and collaboration skills, etc.)
3. Demonstrate due professional care
D. Governance, Risk Management, and Control
1. Describe the concept of organizational governance – (B)
2. Recognize the impact of organizational culture on the overall control environment and individual engagement risks and controls – (B)
3. Describe corporate social responsibility – (B)
4. Interpret fundamental concepts of risk and the risk management process
5. Examine the effectiveness of risk management within processes and functions
6. Recognize the appropriateness of the internal audit activity's role in the organization's risk management process – (B)
7. Interpret internal control concepts and types of controls
8. Examine the effectiveness and efficiency of internal controls
E. Fraud Risks
1. Interpret fraud risks and types of frauds and determine whether fraud risks require special consideration when conducting an engagement
2. Evaluate the potential for occurrence of fraud (red flags, etc.) and how the organization detects and manages fraud risks
3. Recommend controls to prevent and detect fraud and education to improve the organization's fraud awareness
4. Recognize techniques and internal audit roles related to forensic auditing (interview, investigation, testing, etc.) – (B)

II. Practice of Internal Auditing (40%)
A. Engagement Planning
1. Determine engagement objectives and evaluation criteria and the scope of the engagement
2. Plan the engagement to assure identification of key risks and controls
3. Complete a detailed risk assessment of each audit area, including evaluating and prioritizing risk and control factors
4. Determine engagement procedures and prepare the engagement work program
5. Determine the level of staff and resources needed for the engagement
B. Information Gathering
1. Gather and examine relevant information (review previous audit reports and data, conduct walk-throughs and interviews, perform observations, etc.) as part of a preliminary survey of the engagement area
2. Develop checklists and risk-and-control questionnaires as part of a preliminary survey of the engagement area
3. Apply appropriate sampling (nonstatistical, judgmental, discovery, etc.) and statistical analysis techniques
C. Analysis and Evaluation
1. Use computerized audit tools and techniques (data mining and extraction, continuous monitoring, automated workpapers, embedded audit modules, etc.)
2. Evaluate the relevance, sufficiency, and reliability of potential sources of evidence
3. Apply appropriate analytical approaches and process mapping techniques (process identification, workflow analysis, process map generation and analysis, spaghetti maps, RACI diagrams, etc.)
4. Determine and apply analytical review techniques (ratio estimation, variance analysis, budget vs. actual, trend analysis, other reasonableness tests, benchmarking, etc.) – Basic Level (B)
5. Prepare workpapers and documentation of relevant information to support conclusions and engagement results
6. Summarize and develop engagement conclusions, including assessment of risks and controls
D. Engagement Supervision
1. Identify key activities in supervising engagements (coordinate work assignments, review workpapers, evaluate auditors' performance, etc.) – (B)
E. Communicating Engagement Results and the Acceptance of Risk
1. Arrange preliminary communication with engagement clients
2. Demonstrate communication quality (accurate, objective, clear, concise, constructive, complete, and timely) and elements (objectives, scope, conclusions, recommendations, and action plan)
3. Prepare interim reporting on the engagement progress
4. Formulate recommendations to enhance and protect organizational value
5. Describe the audit engagement communication and reporting process, including holding the exit conference, developing the audit report (draft, review, approve, and distribute), and obtaining management's response – (B)
6. Describe the chief audit executive's responsibility for assessing residual risk – (B)
7. Describe the process for communicating risk acceptance (when management has accepted a level of risk that may be unacceptable to the organization) – (B)
F. Monitoring Progress
1. Assess engagement outcomes, including the management action plan
2. Manage monitoring and follow-up of the disposition of audit engagement results communicated to management and the board

III. Business Knowledge for Internal Auditing (30%)
A. Data Analytics
1. Describe data analytics, data types, data governance, and the value of using data analytics in internal auditing – Basic Level (B)
2. Explain the data analytics process (define questions, obtain relevant data, clean/normalize data, analyze data, communicate results) – (B)
3. Recognize the application of data analytics methods in internal auditing (anomaly detection, diagnostic analysis, predictive analysis, network analysis, text analysis, etc.) – (B)
B. Information Security
1. Differentiate types of common physical security controls (cards, keys, biometrics, etc.) – (B)
2. Differentiate the various forms of user authentication and authorization controls (password, two-level authentication, biometrics, digital signatures, etc.) and identify potential risks – (B)
3. Explain the purpose and use of various information security controls (encryption, firewalls, antivirus, etc.) – (B)
4. Recognize data privacy laws and their potential impact on data security policies and practices – (B)
5. Recognize emerging technology practices and their impact on security (bring your own device [BYOD], smart devices, internet of things [IoT], etc.) – (B)
6. Recognize existing and emerging cybersecurity risks (hacking, piracy, tampering, ransomware attacks, phishing, attacks, etc.) – (B)
7. Describe cybersecurity and information security-related policies – (B)
C. Application and System Software
1. Recognize core activities in the systems development lifecycle and delivery (requirements definition, design, developing, testing, debugging, deployment, maintenance, etc.) and the importance of change controls throughout the process – (B)
2. Explain basic database terms (data, database, record, object, field, schema, etc.) and internet terms (HTML, HTTP, URL, domain name, browser, click-through, electronic data interchange [EDI], cookies, etc.) – (B)
3. Identify key characteristics of software systems (customer relationship management [CRM] systems; enterprise resource planning [ERP] systems; and governance, risk, and compliance [GRC] systems; etc.) – (B)
D. IT Infrastructure and IT Control Frameworks
1. Explain basic IT infrastructure and network concepts (server, mainframe, client-server configuration, gateways, routers, LAN, WAN, VPN, etc.) and identify potential risks – (B)
2. Define the operational roles of a network administrator, database administrator, and help desk – (B)
3. Recognize the purpose and applications of IT control frameworks (COBIT, ISO 27000, ITIL, etc.) and basic IT controls – (B)
E. Financial Accounting and Finance
1. Identify concepts and underlying principles of financial accounting (types of financial statements and terminologies such as bonds, leases, pensions, intangible assets, research and development, etc.) – (B)
2. Recognize advanced and emerging financial accounting concepts (consolidation, investments, fair-value partnerships, foreign currency transactions, etc.) – (B)
3. Interpret financial analysis (horizontal and vertical analysis and ratios related to activity, profitability, liquidity, leverage, etc.)
4. Describe revenue cycle, current asset management activities and accounting, and supply chain management (including inventory valuation and accounts payable) – (B)