

## CIA 考试第一部分：内部审计基础

考察领域			认知水平
I	内部审计基本知识 (15%)		
	A	IIA 的内部审计使命、内部审计定义、内部审计实务的核心原则，以及内部审计活动的宗旨、权力和职责	熟练掌握
	B	内部审计章程的要求（必备的内容、董事会的批准、章程的沟通等）	基本掌握
	C	内部审计的确认服务和咨询服务	熟练掌握
	D	IIA 的《职业道德规范》	熟练掌握
II	独立性与客观性 (15%)		
	A	组织上的独立性（独立性的重要性、职能性报告等）	基本掌握
	B	可能损害内部审计独立性的情形	基本掌握
	C	评估和保持内部审计人员个人的客观性，包括可能损害内部审计人员客观性的情形	熟练掌握
	D	促进客观性的政策	熟练掌握
III	胜任能力及应有的职业审慎(18%)		
	A	履行内部审计职责所需的知识、技能和能力（无论是内部开发的还是外部获得）	基本掌握
	B	内部审计人员应具备的知识和能力，包括技术技能和软技能（沟通技巧、批判性思维、说服/谈判和协作技能等）	熟练掌握
	C	应有的职业审慎	熟练掌握

考察领域			认知水平
	D	持续专业发展以提升内部审计人员的专业能力	熟练掌握
IV	质量保证与改进程序(7%)		
	A	质量保证和改进程序的要素（内部评估\外部评估等）	基本掌握
	B	向董事会或其他治理机构报告质量保证与改进程序的结果	基本掌握
	C	对 IIA《标准》遵循或未遵循情况的披露	基本掌握
V	治理、风险管理和控制(35%)		
	A	与治理相关的概念	基本掌握
	B	文化对整体控制环境和单个审计业务风险和控制的影响	基本掌握
	C	道德与合规相关问题、涉嫌违规行为和处理	基本掌握
	D	社会责任	基本掌握
	E	风险的基本概念和风险管理过程	熟练掌握
	F	全球公认的风险管理框架（COSO-ERM、ISO31000 等）	基本掌握
	G	流程和职能风险管理的有效性	熟练掌握
	H	内部审计在风险管理过程中的作用	基本掌握
	I	内部控制概念和控制类型	熟练掌握
	J	全球公认的内部控制框架（如 COSO 等）	熟练掌握
	K	内部控制的效果和效率	熟练掌握
VI	舞弊风险 (10%)		
	A	舞弊风险和舞弊类型，对舞弊风险的特别考虑	熟练掌握
	B	舞弊危险信号及识别和管理舞弊风险	熟练掌握

考察领域			认知水平
	C	防止和发现舞弊的控制与组织的反舞弊意识	熟练掌握
	D	司法鉴定审计	基本掌握

# CIA 考试第二部分：内部审计实务

考察领域		认知水平
I	管理内部审计活动(20%)	
	1.内部审计业务管理	
	A 计划、组织、指导和监督内部审计业务的政策和程序	基本掌握
	B 内部审计活动的行政工作（如预算、资源、招聘、人员编制等）	基本掌握
	2.制定风险导向的内部审计计划	
	A 识别潜在的审计业务来源（如审计范围、审计循环要求、管理层的需求、监管要求、相关市场和行业趋势、新出现的问题等）	基本掌握
	B 确定风险管理框架，以评估风险，并根据风险评估的结果考虑审计业务的优先级	基本掌握
	C 确认业务的种类（包括风险和控制评估、对第三方和合同遵循情况的审计、安全与隐私、绩效和质量的审计、关键绩效指标和运营的审计，财务和法规遵循性审计等）	熟练掌握
	D 旨在提供建议和洞见的咨询业务的类型（如培训、系统设计、系统开发、尽职调查、隐私、对标、内部控制评估、流程描述等）	熟练掌握

考察领域			认知水平
	E	内部审计与外部审计、监管机构、其他内部确认部门之间的协调，以及内部审计与其他确认服务提供方之间相互利用工作成果的可能性	基本掌握
	3.与高级管理层和董事会沟通并向其报告		
	A	首席审计执行官向高级管理层和董事会报告年度审计计划，并寻求获得董事会的批准	基本掌握
	B	首席审计执行官向董事会报告确定重大风险暴露、控制和治理问题	基本掌握
	C	首席审计执行官向高级管理层和董事会报告内部控制和风险管理过程的整体效果	基本掌握
	D	首席审计执行官与高级管理层和董事会定期沟通内部审计关键绩效指标	基本掌握
II	计划审计业务(20%)		
	1.制定计划		
	A	确定审计业务的目标、评估标准和业务范围	熟练掌握
	B	制定审计业务计划以确保识别主要风险和控制	熟练掌握
	C	对每个审计领域进行详细的风险评估	熟练掌握
	D	确定审计业务程序并编制项目工作方案	熟练掌握
	E	确定审计业务所需的各级人员和各项资源	熟练掌握

考察领域		认知水平	
III	执行审计业务(40%)		
	1.信息收集		
	A	收集和检查相关信息（如以前的审计报告和数据，开展穿行测试，访谈，观察等），并将其作为对审计业务领域开展初步调查的一部分	熟练掌握
	B	编制检查清单和风险控制问卷，并将其作为对审计业务领域开展初步调查的一部分	熟练掌握
	C	应用适当的抽样（如非统计抽样、判断抽样、发现抽样等）和统计分析技术	熟练掌握
	2.分析与评价		
	A	运用计算机辅助审计工具和技术（如数据挖掘和提取、持续监控、自动化的工作底稿、嵌入式审计模块等）	熟练掌握
	B	评估潜在证据来源的相关性、充分性和可靠性	熟练掌握
	C	应用适当的分析方法和过程描述技术（如过程识别、工作流分析、流程图生成和分析、条形图、RACI 图等）	熟练掌握
	D	确定并应用分析性复核技术（如比率估计、差异分析、预算与实际相比较、趋势分析、其他合理性测试、对标等）	基本掌握
	E	编制工作底稿和相关信息文档，以支持审计业务结果和结论	熟练掌握
	F	汇总并生成审计业务结论，包括风险和控制的评估结果	熟练掌握

考察领域		认知水平
	3.业务督导	
	A 确定业务督导过程中的主要活动（如协调任务分配、复核工作底稿、评估审计人员的工作表现等）	基本掌握
IV	沟通审计业务结果并监督进展(20%)	
	1.沟通审计业务结果和风险接受程度	
	A 与审计业务客户的初步沟通	熟练掌握
	B 报告质量（包括准确、客观、清晰、简洁、富有建设性、完整、及时）和要素（包括目标、范围、结论、建议和改进措施）	熟练掌握
	C 审计业务进展中的中期报告	熟练掌握
	D 增加和保护组织价值的建议	熟练掌握
	E 审计业务沟通和报告流程，包括召开离场会，撰写审计报告（起草初稿、复核、批准、发送），并获取管理层的反馈意见	基本掌握
	F 首席审计执行官评估剩余风险的责任	基本掌握
	G 沟通对风险的接受（适用于管理层接受了组织可能无法接受的风险水平的情况）	基本掌握
	2.监督进展	
	A 评估审计业务结果，包括管理层的行动计划	熟练掌握

考察领域			认知水平
	B	对已向管理层和董事会报告的审计业务结果处理情况进行 监督和跟踪	熟练掌握

# CIA 考试第三部分：内部审计知识要素

考察领域		认知水平
I	业务敏感度 (35%)	
	1.组织目标、行为和绩效	
	A	战略规划过程和主要活动（目标设定、全球化和竞争、与组织使命和价值的结合等）  基本掌握
	B	常用的绩效评价方法（财务、运营、定性与定量、生产率、质量、效率、效果等）  熟练掌握
	C	组织行为（组织中的个人、群体和组织的行为等）和不同的绩效管理技术（特征、组织政治、动机、职位设计、激励、工作安排等）  基本掌握
	D	在领导、指导、引导员工、建立组织承诺以及企业家能力方面的管理有效性  基本掌握
	2.组织结构和业务流程	
	A	评估不同组织结构对风险和控制的影响（集权与分权、扁平结构和传统结构等）  基本掌握
	B	常见业务流程对风险和控制的影响（人力资源、采购、产品开发、销售、市场营销、物流、外包流程管理等）  熟练掌握
	C	项目管理技术（项目计划和范围、时间/团队/资源/成本管理、变更管理等）  基本掌握
	D	合同的各种形式和要素（形式、对价、单边、双边等）  基本掌握

考察领域			认知水平
	3.数据分析		
	A	数据分析、数据种类、数据治理以及在内部审计中使用数据分析的价值	基本掌握
	B	数据分析流程（设定问题、获取数据、清理/规范数据、分析数据、结果沟通）	基本掌握
	C	数据分析方法在内部审计中的应用（异常检测、诊断分析、预测分析、网络分析、文本分析等）	基本掌握
II.	信息安全 (25%)		
	1.不同类型的物理安全控制		
	A	物理安全和物理控制（卡片、密钥、生物识别等）	基本掌握
	B	用户认证和授权控制以及潜在风险识别（密码、两级认证、生物识别、数字签名等）	基本掌握
	C	信息安全控制（数据加密、防火墙、杀毒软件等）的目的和用途	基本掌握
	D	数据隐私法规及其对数据安全政策和实务的潜在影响	基本掌握
	E	新兴技术实务及其对安全的影响（自带办公设备[BYOD]、智能设备、物联网[IoT]等）	基本掌握
	F	现有的和新兴的网络安全风险（入侵、盗版、篡改、勒索攻击、网络钓鱼攻击等）	基本掌握
	G	网络安全和信息安全相关政策	基本掌握

考察领域		认知水平
III.	信息技术 (20%)	
	1.应用软件和系统软件	
A	系统开发生命周期和交付过程中的核心活动（需求定义、设计、开发、测试、调试、实施、维护等）以及在整个过程中变更控制的重要性	基本掌握
B	基本的数据库（数据、数据库、记录、对象、字段、模式等）和因特网术语（HTML、HTTP、URL、域名、浏览器、点击进入、电子数据交换[EDI]、cookies 等）	基本掌握
C	软件系统的主要特征（客户关系管理[CRM]，企业资源规划[ERP]系统，治理、风险和合规[GRC]系统等）	基本掌握
2. IT 基本掌握设施和 IT 控制框架		
A	基本的 IT 基本掌握设施和网络概念（服务器、主机、客户机服务器配置、网关、路由器、LAN、WAN、VPN 等）以及潜在的风险识别	基本掌握
B	网络管理员、数据库管理员和服务台的运营角色	基本掌握
C	IT 控制框架（COBIT、ISO 27000、ITIL 等）和基本 IT 控制的目的及应用	基本掌握
3.灾难恢复		
A	灾难恢复计划中的站点概念（热站、暖站、冷站等）	基本掌握
B	系统和数据备份的目的	基本掌握
C	系统和数据恢复的目的	基本掌握

考察领域		认知水平	
IV.	财务管理 (20%)		
	1.财务会计和财务管理		
	A	财务会计的概念和基本原则（财务报表类型和术语，比如债券、租赁、职工福利计划、无形资产、研发支出等）	基本掌握
	B	高级和新兴财务会计概念（合并、投资、合伙、外币交易等）	基本掌握
	C	财务分析（水平和垂直分析，与经营活动、盈利能力、流动性、杠杆等的比率分析等）	熟练掌握
	D	收入循环、流动资产管理和核算、供应链管理（包括存货估值和应付账款）	基本掌握
	E	资本预算、资本结构、基本税收制度和转移定价	基本掌握
	2.管理会计		
	A	管理会计的一般概念（本-量-利分析、预算、费用分配、成本效益分析等）	基本掌握
	B	成本核算系统（完全成本、变动成本、固定成本、作业成本、标准成本等）	基本掌握
	C	各种成本（相关和不相关成本、增量成本等）及其在决策制定中的应用	基本掌握