ICS 35.240.01
CCS L79

T/CCUA

中 国 计 算 机 用 户 协 会 团 体 标 准

T/CCUA 007—202X
代替 T/CCUA 007-2019

信息系统审计师专业能力等级评价

Professional skills evaluation of information system auditors

（征求意见稿）

（本草案完成时间：2023 年 3 月 16 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2023－XX－XX 发布　　2023－XX－XX 实施

中国计算机用户协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替T/CCUA 007--2019《信息系统审计师职业技能评价》，与T/CCUA 007—2019相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 标准名称更改为“信息系统审计师专业能力等级评价”；
b) 文中涉及的“职业技能”均改为“专业能力”；
c) 更改了范围的内容表述（见第 1 章）；
d) 删除了规范性引用文件的表述内容（见 2020 版第 2 章）；
e) 更改了术语和定义中“信息系统审计师”的内容表述（见 3.1，2020 版 3.1）；
f) 删除了术语和定义中“信息系统控制”“信息系统审计知识体系”和“信息系统审计技能体系”（2020 版 3.2，3.3，3.4）；
g) 删除了“职业体系总体要求”的内容表述（见 2020 版 4.1），更改为“信息系统审计专业能力体系”（见 4.1）；
h) 将“信息系统审计师知识体系”更改为“技术专业能力要求”，将该条下所涉“知识”改为“能力”（见 4.3，2020 版 4.2）；将“信息系统审计师技能体系”更改为“审计专业能力要求”（见 4.2，2020 版 4.3）；调整了“技术专业能力要求”和“审计专业能力要求”的顺序（见 4.3、4.2，2020 版 4.3、4.2），在附录 A 表 A.1 做了相应调整；
i) 删除了“项目立项控制审计”的内容表述[见 2020 版 4.2.1 b）]，在附录 A 表 A.1 做了相应删除；
j) 更改了“网络安全控制审计”的内容表述[见 4.3.4 a），2020 版 4.2.4 a）]在附录 A 表 A.1 做了相应更改；
k) 增加了“数据安全控制审计”内容表述[见 4.3.4 b）]，在附录 A 表 A1 做了相应增加；
l) 更改了“审计流程质量管理”的内容表述[见 4.2.5 a），2020 版 4.3.4 a）]，并在附录 A 表 A.1 做了相应更改；
m) 更改了“安全控制审计判断”的内容表述[见 4.2.4 d），2020 版 4.3.3 d）]，并在附录 A 表 A.1 做了相应更改；
n) 删除了“电子政务常规知识”见（2020 版 4.3.5），在附录 A 表 A.1 做了相应删除；
o) 将“信息系统审计师技能评价”改为“信息系统审计师专业能力等级评价”（见第 5 章，2020 版第 5 章）；
p) 更改了“信息系统审计师的评价”的内容表述（见 5.2，2020 版 5.2.1）；
q) 更改了“信息系统高级审计师的评价”的内容表述（见 5.2，2020 版 5.2.1）；
r) 增加了附录 B 信息系统审计师能力评价（见附录 B）；
s) 增加了参考文献《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》《国家政务信息化项目建设管理办法》《中华人民共和国国家审计准则》《信息系统审计指南》《关于进一步加强国家电子政务网络建设和应用工作的通知》（见参考文献）。

本文件由中国计算机用户协会提出并归口。

本文件起草单位：中国计算机用户协会政务信息化分会、中国计算机用户协会信息科技审计分会、北京中科卓信软件测评技术中心、北京国信新网通讯技术有限公司、统信软件技术有限公司、北京中帧四方资讯有限公司、杭州安恒信息技术股份有限公司、紫光软件系统有限公司行业事业部、北明软件有限公司、北京易柯森特科技有限公司、北京国信杰云科技有限公司、中科软科技股份有限公司、北京中宇万通科技股份有限公司、武汉深之度科技有限公司、拓尔思天行网安信息技术有限公司、杭州数政科技有限公司、中国计算机用户协会云应用分会、北京华信汇聚科技有限公司、北京华宇恒通工程咨询有限公司。

本文件主要起草人：周德铭、王智玉、赵进延、张保印、石跃军、孔祥清、彭维民、杜维成、孙卫东、唐常芳、黄鹂、胡陈勇、董海英、樊睿、何新、陈太博、关键、赵华、才依明、庄蓉茹、牟巍、张东、张彦峰、宁宇鹏、刘闻欢、令狐永兴、周志凯、胡鹏举、张强、于丽丽。

本文件历次版本发布情况为：

——2020年5月首次发布为T/CCUA 007-2020；

——本次为第一次修订。

信息系统审计师专业能力等级评价

1 范围

本文件确定了信息系统审计师专业能力体系，规定了审计专业能力和技术专业能力要求，描述了对应的评价方法。

本文件适用于信息系统审计机构和信息系统建设、运行及维护单位的信息系统审计相关人员。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统审计师 information system auditor

掌握信息系统审计的专业能力，对信息系统的管理控制、应用控制、网络控制、安全控制进行检查监督，提出审计意见和建议的人员。

注：我国现行有效的法律、行政法规、司法解释、地方法规、地方规章、部门规章及其他规范性文件对信息系统的管理、应用、网络和安全提出了法规类控制；国家标准、行业标准、地方标准、企业标准、团体标准对信息系统的管理、应用、网络和安全提出了标准类控制；由信息系统规划建设和运行维护组织制定了所有成员共同遵守的规则类控制。

4 信息系统审计专业能力体系和要求

4.1 信息系统审计专业能力体系

信息系统审计专业能力体系包括信息系统审计概述、审计程序、审计方法、审计判断、质量管理的审计专业能力，信息系统的管理控制、应用控制、网络控制、安全控制的技术专业能力（见附录A）。

4.2 审计专业能力要求

4.2.1 信息系统审计概述

应具有国内外信息系统和信息系统审计的建立和发展，信息系统审计定义等的能力。

4.2.2 信息系统审计程序

信息系统审计程序应包括：

a) 审计计划。包括独立式和结合财政财务收支审计的组织方式，确定审计对象、审计期间、审计重点、审计方法，组织审计组开展审计等。

b) 审前调查。包括对审计对象的核心业务、信息系统、关键功能、数据资源、分析模型等的调查，结合式审计中要提出由于信息系统内控缺失可能导致数据和系统风险的报告。

c) 审计实施。包括结合审计计划的审计重点，采用审计方法、审计工具等，提取审计证据、形成审计工作底稿，开展信息系统审计。

d) 审计报告。包括出具审计报告，关注审计意见和建议的整改落实情况。

4.2.3 信息系统审计方法

信息系统审计方法应包括：

a) 审计方法。包括一般审计方法、审计测评方法、数据审计方法、其他审计方法等。

b) 审计工具。包括一般审计工具、安全检测工具、安全审计工具等。
c) 第三方资源利用。包括信息系统的专家和第三方机构的资源利用等。

4.2.4 信息系统审计判断

信息系统审计判断应包括：
a) 管理控制审计判断。包括对组织管理、项目实施、项目投资、项目验收、项目绩效控制的可靠性、安全性、经济性的审计判断能力。
b) 应用控制审计判断。包括对应用规划、业务能力、数据资源、分析模型、新技术运用控制的可靠性、安全性、经济性的审计判断能力。
c) 网络控制审计判断。包括对网络系统、计算系统、存储系统、备份系统、机房系统控制的可靠性、安全性、经济性的审计判断能力。
d) 安全控制审计判断。包括对网络安全、数据安全、等级保护、风险评估、应急预案控制的可靠性、安全性、经济性的审计判断能力。

4.2.5 信息系统审计质量

信息系统审计质量应包括：
a) 审计流程质量管理。包括审计人员、审计组组长、审计机构法制部门、审计机构负责人在审计计划、审前调查、审计实施、审计报告等流程的质量管控。
b) 审计目标质量管理。包括对信息系统 4 类控制的有效性，尤其是内控缺失可能导致系统风险和数据风险的质量管控。

4.3 技术专业能力要求

4.3.1 管理控制审计能力

管理控制审计能力应包括：
a) 组织管理控制审计。具有对信息系统的领导机构、业务机构、实施机构、财务机构、监督机构等的领导能力、工作机制,以及项目建议书、可研报告和初步设计等立项报告控制的审计评价能力。
b) 项目实施控制审计。具有对信息系统详细设计、招标投标和政府采购、系统建设、系统和数据安全、运行维护等控制的审计评价能力。
c) 项目投资控制审计。具有对信息化项目预算编制与批复、预算执行、概算调整、决算编制、资产管理等控制的审计评价能力。
d) 项目验收控制审计。具有信息系统单项验收、建设部门验收、审批部门验收控制的审计评价能力。
e) 项目绩效控制审计。具有信息系统的绩效评价指标、绩效评价方法、绩效评价结果和运用的审计评价能力。

4.3.2 应用控制审计能力

应用控制审计能力应包括：
a) 应用规划控制审计。具有对政府治理、公共服务、企业和社会信息化等信息系统规划控制的审计评价能力。
b) 业务能力控制审计。具有对门户网站、管理系统、业务系统、数据中心、共享平台、运维系统、安全系统的系统整合，信息系统目录的更新和总目录的构建，信息系统的集约化、持续性、业务连续性等业务能力控制的审计评价能力。
c) 数据资源控制审计。具有对政府治理、公共服务、企业和社会信息化等方面分类分级建设的数据资源控制，数据资源的业务目录、共享目录、开放目录，元数据、主数据、数据元素、数据表、主题数据等制度标准控制的审计评价能力。
d) 分析模型控制审计。具有对信息系统的业务流程和业务逻辑等的业务处理模型，多维数据分析、聚类关联分析、模拟仿真分析等的数据分析模型，知识图谱分析、决策支持分析等的算法和大数据分析算法模型等控制的审计评价能力。

e) 新技术运用控制审计。具有移动互联、物联网、大数据、人工智能等新一代信息技术运用的审计评价能力。

4.3.3 网络控制审计能力

网络控制审计能力应包括：

a) 网络系统控制审计。具有对信息系统利用的政务内网、政务外网、互联网，局域网、城域网、广域网，多网互联和网络布线等控制的审计评价能力。
b) 计算系统控制审计。具有对计算系统的硬件、软件、支撑系统、计算指标，以及分布式计算、虚拟化计算、云计算等控制的审计评价能力。
c) 存储系统控制审计。具有对信息系统的存储分类、存储方式、存储性能，以及通用存储、云存储等控制的审计评价能力。
d) 备份系统控制审计。具有对数据备份和系统备份、在线备份和离线备份、同城备份和异地备份，以及备份指标等控制的审计评价能力。
e) 机房系统控制审计。具有对计算机房物理选择、功能布局，以及供电系统、空调系统、消防系统、防雷接地系统、监视系统等辅助系统控制的审计评价能力。

4.3.4 安全控制审计能力

安全控制审计能力应包括：

a) 网络安全控制审计。具有网络安全关键技术应用、确保信息系统持续运行等的国家网络安全法律制度的理解力和执行力，具有应用系统、网络系统、计算系统、存储系统、备份系统、机房系统等方面的系统安全控制的审计评价能力。
b) 数据安全控制审计。具有数据安全治理、数据安全保障等的国家数据安全法律规章的理解力和执行力，具有对数据资源分类分级安全保护，数据采集加工、数据汇聚存储、数据分析利用、数据共享开放、跨境数据等方面的数据安全控制的审计评价能力。
c) 等级保护控制审计。具有对信息系统网络安全等级保护的基本要求、设计技术要求、测评要求的制度控制，包括通用技术控制和通用管理控制，云计算、移动互联、物联网、工业控制等网络安全等级保护的审计评价能力。
d) 风险评估控制审计。具有风险评估对象、风险评估指标、风险评估规范等控制的审计评价能力。
e) 应急预案控制审计。具有应急预案目标、任务、指标等控制的审计评价能力。

5 信息系统审计师专业能力等级评价

5.1 信息系统审计师能力等级

信息系统审计师包括信息系统审计师、信息系统高级审计师两个能力等级。

5.2 信息系统审计师能力评价

5.2.1 信息系统审计师的评价

中华人民共和国境内所有成年公民，均可向中国计算机用户协会申请信息系统审计师专业能力资格。

中国计算机用户协会应对申请者进行考试后经综合评价（见附录 B）。合格的颁发《信息系统审计师》证书。

5.2.2 信息系统高级审计师的评价

具有信息系统审计师专业能力证书者，或具有其他专业的高级资格证书者，可向中国计算机用户协会申请信息系统高级审计师专业能力资格。

中国计算机用户协会应对申请者提交的信息系统工作报告、信息系统审计实例报告进行综合评价（见附录B）。合格的颁发《信息系统高级审计师》证书。

5.3 信息系统审计师专业能力后续教育

为适应信息系统审计专业能力更新的快速发展，信息系统审计师证书有效期为3年，自取得证书之日起的每个3年内，为后续培训和考查评价时间。

后续培训的内容应为信息系统审计法律法规、标准和工作规则的法规类能力，管理控制、应用控制、网络控制、安全控制的实操类能力，信息系统审计方法的应用类能力，以及信息系统审计关键技术突破等的专业能力。

通过后续培训和综合评价的，重新颁发《信息系统审计师》、《信息系统高级审计师》专业能力相应等级证书。

附 录 A
（规范性）
信息系统审计师专业能力体系

信息系统审计师专业能力体系见表A.1.

表A.1 信息系统审计师专业能力体系

能力类别	一级指标	二级指标	具体要求
审计专业能力	1 信息系统审计	1.1 审计概述	应具有国内外信息系统和信息系统审计的建立和发展,信息系统审计定义等的能力
		1.2 审计程序	应具有信息系统审计计划、审前准备、审计实施、审计报告的审计程序能力
		1.3 审计方法	应具有信息系统审计方法、审计工具和第三方资源利用的能力
		1.4 审计判断	应具有对信息系统管理控制、应用控制、网络控制、安全控制的可靠性、安全性、经济性的审计判断能力
		1.5 审计质量	应具有对审计实施方案、审计取证、审计底稿、审计报告等流程的材料复核和质量管控的能力
技术专业能力	2 管理控制审计	2.1 组织管理控制审计	应具有对信息系统规划建设的领导、实施、财务、运维、监管等的组织结构和工作机制，具有对信息系统项目建议书、可研报告和初步设计等立项报告控制的审计评价能力
		2.2 项目实施控制审计	应具有对信息系统招标投标和政府采购、详细设计、系统建设、系统运行、系统维护等控制的审计评价能力
		2.3 项目投资控制审计	应具有对信息系统项目预算编制与批复、预算执行、概算调整、决算编制等控制的审计评价能力
		2.4 项目验收控制审计	应具有信息系统单项验收、建设部门验收、审批部门验收控制的审计评价能力
		2.5 项目绩效控制审计	应具有对信息系统的政务效能贡献、业务信息化推动、可持续发展、能力适配指标等绩效控制的审计评价能力
	3 应用控制审计	3.1 应用规划控制审计	应具有对政府治理、公共服务、企业和社会信息化等信息系统规划控制的审计评价能力。
		3.2 业务能力控制审计	应具有对门户网站、管理系统、业务系统、数据中心、共享平台、运维系统、安全系统等的系统整合,信息系统目录的更新和总目录的构建,信息系统的集约化、组件化、持续性、业务连续性等业务能力控制的审计评价能力
		3.3 数据资源控制审计	应具有对政府治理、公共服务、企业和社会信息化等方面分类分级建设的数据资源控制，数据资源的业务目录、共享目录、开放目录，元数据、主数据、数据元素、数据表、主题数据等制度标准控制的审计评价能力
		3.4 分析模型控制审计	应具有对信息系统的业务流程和业务逻辑等的业务处理模型，多维数据分析、聚类关联分析、模拟仿真分析等的数据分析模型，知识图谱分析、决策支持分析等的大数据分析算法控制的审计评价能力
		3.5.新技术运用控制审计	应具有对信息系统的移动互联、物联网、大数据、云计算、人工智能等新一代技术运用控制的审计评价能力
	4 网络控制审计	4.1 网络系统控制审计	应具有对信息系统利用的政务内网、政务外网、互联网，局域网、城域网、广域网，多网互联和信息共享网络等控制的审计评价能力
		4.2 计算系统控制审计	应具有对计算系统的硬件、软件、支撑系统、计算指标，以及分布式计算、虚拟化计算、云计算等控制的审计评价能力
		4.3 存储系统控制审计	应具有对信息系统的存储分类、存储方式、存储性能，以及通用存储、云存储等控制的审计评价能力
		4.4 备份系统控制审计	应具有对信息系统的数据备份和系统备份、在线备份和离线备份、同城备份和异地备份，以及备份指标等控制的审计评价能力
		4.5 机房系统控制审计	应具有对计算机房物理选择、功能布局，以及供电系统、空调系统、消防系统、防雷接地系统、监视系统等控制的审计评价能力

表A.1　信息系统审计师专业能力体系（续）

能力类别	一级指标	二级指标	具体要求
	5 安全控制审计	5.1 网络安全控制审计	应具有网络安全关键技术应用、确保信息系统持续运行等的国家网络安全法律制度的理解力和执行力，具有应用系统、网络系统、计算系统、存储系统、备份系统、机房系统等方面的系统安全控制的审计评价能力
		5.2 数据安全控制审计	应具有数据安全治理、数据安全保障等的国家数据安全法律规章的理解力和执行力，具有对数据资源分类分级保护，数据采集加工、数据汇聚存储、数据分析利用、数据共享开放、跨境数据等方面的数据安全控制的审计评价能力
		5.3 等级保护控制审计	应具有对信息系统网络安全等级保护的基本要求、设计技术要求、测试要求的制度控制，包括通用技术控制和通用管理控制，云计算、移动互联、物联网、工业控制等网络安全等级保护的审计评价能力
		5.4 风险评估控制审计	应具有风险评估对象、风险评估指标、风险评估规范等控制的审计评价能力
		5.5 应急预案控制审计	应具有应急预案目标、任务、指标等控制的审计评价能力

附 录 B
（规范性）
信息系统审计师能力等级评价

B.1 信息系统审计师考试评价

由中国计算机用户协会编制考试题库，每次考试分为A卷、B卷、C卷。考试题目采用单选题40题（每题1分）、多选题15题（每题2分）、简答题、计算题、案例题各1题（每题10分）。考试时间：150min。考试评价：试卷总分100分，得分70分及以上为合格。

B.2 信息系统高级审计师评价

中国计算机用户协会应对申请者提交的信息系统工作报告（格式见表B.1）、信息系统审计实例报告（文字量4000字左右，格式见表B.2）进行综合评价。信息系统工作报告、信息系统审计实例报告总分均为100分，得分70分及以上为合格。

表B.1 信息系统高级审计师信息系统工作报告格式

信息系统高级审计师信息系统工作报告

申请人姓名		单位	
地址		电话	
行政职务		技术职称	
简历			
何时何地参与信息系统检查监督和成效			
发表涉及信息系统的论文或专著			
何时获得国家行业省市级奖励			
得分			

表B.2 信息系统高级审计师信息系统审计实例报告格式

信息系统高级审计师信息系统审计实例报告

报告名称			
作者		单位	
行政职务		技术职称	
地址		电话	
一、实例背景 （一）履职业务情况 （二）信息系统情况 （三）信息系统检查因素 1.推进工作； 2.解决遇到的问题； 3.其他。			
二、问题分析（利用信息系统审计方法对发生的问题进行分析，找到问题发生的原因） （一）问题1分析 （二）问题2分析 （三）…			

表B.2　信息系统高级审计师信息系统审计实例报告（样本）（续）

三、改进意见和建议（依据管理控制、应用控制、网络控制、安全控制的法规类、标准类、规则类要求，提出改进的审计意见和建议） （一）改进意见 1.问题1改进意见 2.问题2改进意见 … （二）改进建议 1.问题4改进建议 2.问题5改进建议 …
四、工作成效（根据审计意见和建议的整改落实，取得的工作成效） （一）成效1 （二）成效2 …

得分	

参 考 文 献

[1] GB/T 30850.1—2014 电子政务标准化指南 第 1 部分：总则

[2] GB/T 30850.2—2014 电子政务标准化指南 第 2 部分：工程管理

[3] GB/T 30850.3—2014 电子政务标准化指南 第 3 部分：网络建设

[4] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

[5]《中华人民共和国审计法》（2021 年 10 月 23 日第十三届人大第三十一次会议修正）

[6]《中华人民共和国数据安全法》（2021 年 6 月 10 日全国人大会议通过）

[7]《关键信息基础设施安全保护条例》（国务院令第 745 号）

[8]《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》（2022 年 12 月 2 日）

[9]《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）

[10]《中华人民共和国国家审计准则》（审计署令第 8 号）

[11]《信息系统审计指南》（审计发〔2012〕11 号）

[12]《关于进一步加强国家电子政务网络建设和应用工作的通知》（发改高技[2012]1986 号）