T/CCUA

中国计算机用户协会团体标准

  T/CCUA XXX—2019

|  |
| --- |
|       |

信息系统审计机构服务能力评价

Evaluation of the service capacity of the information systems audit institution

|  |  |
| --- | --- |
| （征求意见稿） |   |
| 本稿完成日期：2019-08-16 |   |

1. XXXX - XX - XX发布

XXXX - XX - XX实施

        发布

目  次

[前言 II](#_Toc16935768)

[1 范围 1](#_Toc16935769)

[2 规范性引用文件 1](#_Toc16935770)

[3 术语和定义 1](#_Toc16935771)

[3.1 1](#_Toc16935772)

[3.2 1](#_Toc16935773)

[3.3 1](#_Toc16935774)

[4 信息系统审计机构服务能力体系 1](#_Toc16935775)

[4.1 服务能力总体要求 1](#_Toc16935776)

[4.2 信息系统审计机构服务能力知识体系 2](#_Toc16935777)

[4.2.1 信息系统审计知识 2](#_Toc16935778)

[4.2.2 电子政务发展知识 3](#_Toc16935779)

[4.2.3 管理控制审计知识 3](#_Toc16935780)

[4.2.4 应用控制审计知识 3](#_Toc16935781)

[4.2.5 网络控制审计知识 3](#_Toc16935782)

[4.2.6 安全控制审计知识 4](#_Toc16935783)

[4.3 信息系统审计机构服务能力技能体系 4](#_Toc16935784)

[4.3.1 信息系统控制审计 4](#_Toc16935785)

[4.3.2 信息系统审计程序 4](#_Toc16935786)

[4.3.3 信息系统审计方法 4](#_Toc16935787)

[4.3.4 信息系统审计判断 5](#_Toc16935788)

[4.3.5 信息系统审计质量 5](#_Toc16935789)

[5 信息系统审计机构服务能力评价 5](#_Toc16935790)

[5.1 信息系统审计机构服务能力等级 5](#_Toc16935791)

[5.2 信息系统审计机构服务能力评价 5](#_Toc16935792)

[5.2.1 信息系统审计机构服务能力申请条件 5](#_Toc16935793)

[5.2.2 3级服务能力评价 5](#_Toc16935794)

[5.2.3 2级服务能力评价 5](#_Toc16935795)

[5.2.4 1级服务能力评价 5](#_Toc16935796)

[5.3 信息系统审计机构服务能力后续培训 6](#_Toc16935797)

[附录 7](#_Toc16935799)

前  言

本标准按照GB/T 1.1—2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准由中国计算机用户协会提出并归口。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本部分起草单位：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、中国计算机用户协会云应用分会、北京益安在线科技股份有限公司。

本部分主要起草人：周德铭、赵进延、王智玉、张保印、石跃军、胡鹏举、孙卫东、唐常芳、韩松。

信息系统审计机构服务能力评价（征求意见稿）

1. 范围

本标准规定了信息系统审计机构服务能力的知识体系、技能体系和评价要求。

本标准适用于信息系统审计机构和信息系统建设运维单位开展的信息系统审计。

1. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GBT21064-2007 《电子政务系统总体设计要求》

GB/T30850 1至6《电子政务标准化指南》

GB/T\_21063-2007《政务信息资源目录体系》

GB/T 21062-2007《政务信息资源交换体系》

GB/T32180.1至6—2015《财经信息技术 ERP数据接口国家标准》

GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》

GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》

GB/T 25070—2019《信息安全技术 网络安全等级保护安全设计技术要求》

1. 术语和定义

下列术语和定义适用于本文件。

* 1.

信息系统审计机构 Information system audit organization

掌握信息系统审计的知识体系和技能体系，能够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，促进信息系统组织目标实现的组织。

* 1.

信息系统审计机构服务能力知识体系 Information system audit organization serviceability knowledge system

审计机构和运维组织掌握信息系统的审计知识，信息系统的管理控制、应用控制、网络控制、安全控制的控制和审计知识，信息系统的可靠性、安全性、经济性目标的审计知识体系。

* 1.

信息系统审计机构服务能力技能体系 Information system audit organization serviceability skill system

审计机构和运维组织掌握信息系统控制和审计的技术技能，审计程序、审计方法、职业判断、质量管理的审计技能，信息系统可靠性、安全性、经济性目标检查监督的审计技能体系。

1. 信息系统审计机构服务能力体系
	1. 服务能力总体要求

信息系统审计是对信息系统的管理、应用、网络、安全等各类资源进行管理控制、应用控制、网络控制、安全控制的审计监督，提出审计建议和建议，促进信息系统可靠性、安全性、经济性组织目标实现的检查活动。如图1所示。



1. 信息系统审计

信息系统审计机构服务能力体系总体要求包括：信息系统审计知识、电子政务发展知识，信息系统的管理控制审计、应用控制审计、网络控制审计、安全控制审计的6个方面。信息系统审计机构服务能力体系如图2所示。



图2 信息系统审计机构服务能力体系

* 1. 信息系统审计机构服务能力知识体系

信息系统审计机构服务能力的知识体系包括：信息系统审计知识、电子政务发展知识，信息系统的管理控制审计、应用控制审计、网络控制审计、安全控制审计的6个方面30个主题（见附录）。

* + 1. 信息系统审计知识

1）组织体系。具有信息系统审计的组织领导、实施机构和工作机制的组织体系。

2）制度体系。具有信息系统审计的法律法规、标准规范、准则指南的知识体系和执行体系。

3）人员素质。具有与信息系统审计相适应的信息系统审计师或信息系统高级审计师的专业资格证书人员。

4）控制知识。具有信息系统的管理控制、应用控制、网络控制、安全控制，实现可靠性、安全性、经济性的控制知识体系，以及信息系统控制审计的知识和能力。

5）审计程序。具有信息系统审计计划、审前准备、审计实施、审计报告、整改跟踪的审计程序知识体系和执行能力。

6）审计方法。具有信息系统审计方法、审计工具和第三方资源利用的知识体系和执行能力。

* + 1. 电子政务发展知识

7）国际电子政务。具有国际信息系统审计的起步与发展、发展能力和特色的知识体系和培训体系。

8）国内电子政务。具有我国信息系统审计的起步与发展、发展能力和特色的知识体系和培训体系。

9）电子政务创新。具有我国政府治理、公共服务、企业信息化等创新发展的知识体系和培训体系。

10）新技术运用。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知识体系和培训体系。

* + 1. 管理控制审计知识

11）组织管理控制审计。具有对信息系统规划建设的领导、实施、运维、监管等的组织结构和工作机制，以及法规制度和标准规范控制的审计知识和评价能力。

12）项目立项控制审计。具有对信息系统项目需求分析、建议书、可研报告和初步设计等立项报告控制的审计知识和评价能力。

13）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知识和评价能力。

14）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、决算编制等控制的审计知识和评价能力。

15）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知识和评价能力。

16）项目绩效控制审计。具有对信息系统的政务效能贡献、业务信息化推动、可持续发展和能力适配指标等绩效评价控制的审计知识和评价能力。

* + 1. 应用控制审计知识

17）应用规划控制审计。具有对政府治理、公共服务、企业信息化等信息系统规划控制的审计知识和评价能力。

18）业务能力控制审计。具有对信息系统的业务处理能力、数据处理能力、系统整合能力、信息共享能力、数据开放能力、业务连续性能力、系统集约化能力、技术支撑能力、运维服务能力等控制的审计知识和评价能力。

19）分析模型控制审计。具有对信息系统的业务处理模型、数据分析模型、聚类关联分析模型、模拟仿真分析模型、决策支持模型、大数据分析模型等控制的审计知识和评价能力。

20）数据资源控制审计。具有对政府部门、公共服务机构、企业等的数据资源业务目录、共享目录、开放目录，元数据、数据元素、数据表等标准规范，数据库设计等控制的审计知识和评价能力。

21）新技术运用控制审计。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知识和评价能力。

* + 1. 网络控制审计知识

22）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，多网互联和信息共享网络等控制的审计知识和评价能力。

23）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、云计算组织方式等控制的审计知识和评价能力。

24）存储系统控制审计。具有对信息系统的存储分类、存储方式、存储控制、存储性能，以及通用存储、云存储等控制的审计知识和评价能力。

25）备份系统控制审计。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知识和评价能力。

26）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、监视系统等控制的审计知识和评价能力。

* + 1. 安全控制审计知识

27）网络安全控制审计。具有对信息系统的网络安全就是国家安全、正确处理安全和发展、突出关键技术和运用等控制的审计知识和评价能力。

28）等级保护控制审计。具有对信息系统的网络安全等级保护制度控制，包括通用技术控制和通用管理控制，云计算、移动互联、物联网等控制的审计知识和评价能力。

29）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知识和评价能力。

30）应急预案控制审计。具有应急预案目标、任务、指标等控制的审计知识和评价能力。

* 1. 信息系统审计机构服务能力技能体系
		1. 信息系统控制审计

信息系统控制审计的技术技能包括：管理控制审计、应用控制审计、网络控制审计、安全控制审计的技术技能和组织管控能力。

管理控制审计技术技能包括：项目立项控制、项目实施控制、项目投资控制、项目验收控制、项目绩效控制的审计技术技能和组织管控能力。

应用控制审计技术技能包括：应用规划控制、业务能力控制、分析模型控制、数据资源控制、新技术运用控制的审计技术技能和组织管控能力。

网络控制审计技术技能包括：网络系统控制、计算系统控制、存储系统控制、备份系统控制、机房系统控制的审计技术技能和组织管控能力。

安全控制审计技术技能包括：国家网络安全控制、等级保护控制、风险评估控制、应急预案控制的审计技术技能和组织管控能力。

* + 1. 信息系统审计程序

信息系统审计程序包括：审计计划、审前调查、审计实施、审计终结四个阶段的审计技术技能和组织管控能力。

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，组织审计组等。

审前调查包括对审计对象的核心业务、信息系统、关键功能、数据资源等的调查，结合式审计中要提出由于信息系统内控确实可能导致数据风险的报告。

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。

审计终结包括出具形成并出具审计报告，关注审计意见和建议的整改落实情况。

* + 1. 信息系统审计方法

信息系统审计方法包括：审计方法、审计工具、第三方资源利用等的审计技术技能和组织管控能力。

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。

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。

第三方资源利用包括各类专家和第三方机构的资源利用等。

* + 1. 信息系统审计判断

信息系统审计职业判断包括：管理控制、应用控制、网络控制、安全控制完整性、有效性职业判断的审计技术技能和组织管控能力。

管理控制审计职业判断包括对项目立项、项目实施、项目投资、项目验收控制完整性、有效性的审计职业判断。

应用控制审计职业判断包括对应用规划、业务能力、分析模型、数据资源控制完整性、有效性的审计职业判断。

网络控制审计职业判断包括对网络系统、计算系统、存储系统、机房系统控制完整性、有效性的审计职业判断。

安全控制审计职业判断包括对网络安全、等级保护、风险评估、应急预案控制完整性、有效性的审计职业判断。

* + 1. 信息系统审计质量

信息系统审计质量包括：审计流程质量管理、审计目标质量管理的审计技术技能和组织管控能力。

审计流程质量管理是对审计实施方案、审计实施记录、审计取证、审计底稿、审计报告等流程的复核和审理的质量管控。

审计目标质量管理是对信息系统的内部控制、信息系统内控缺失可能导致系统风险和数据风险的质量管控。

1. 信息系统审计机构服务能力评价
	1. 信息系统审计机构服务能力等级

信息系统审计机构服务能力从高到低分为：1级、2级、3级。

* 1. 信息系统审计机构服务能力评价
		1. 信息系统审计机构服务能力申请条件

凡是国家审计、内部审计、社会审计的组织机构，或者是信息系统规划、建设、运用和维护的组织机构，均可申请信息系统审计机构服务能力。

获得第3级服务能力的审计机构，一年后可申请第2级服务能力；获得第2级服务能力的审计机构，一年后可申请第1级服务能力。

* + 1. 3级服务能力评价

具备4.2信息系统审计机构服务能力知识体系、4.3信息系统审计机构服务能力技能体系；具备信息系统审计职业技能证书的5名信息系统审计师。

对申请者的培训、考试进行是否符合信息系统审计机构3级服务能力的职业资格综合评价。

* + 1. 2级服务能力评价

具有较强的信息系统审计机构服务能力知识体系和技能体系，具备相应的信息系统控制审计的关键技术；具备信息系统审计职业技能证书的8名信息系统审计师（中级）、2名信息系统高级审计师。

对申请者的培训、考试进行是否符合信息系统审计机构2级服务能力的职业资格综合评价。

* + 1. 1级服务能力评价

具有较为完善的信息系统审计机构服务能力知识体系和技能体系，具备相应的信息系统控制审计的关键技术；具备信息系统审计职业技能证书的10名信息系统审计师（中级）、4名信息系统高级审计师。

对申请者的培训、考试进行是否符合信息系统审计机构1级服务能力的职业资格综合评价。

* 1. 信息系统审计机构服务能力后续培训

为适应信息系统控制审计知识技能更新的快速发展，自得到《信息系统审计机构服务能力》认证证书之日起的每个3年内，为后续培训和考查评价时间。

后续培训的内容为信息系统审计法律法规、标准规范知识，信息系统控制和审计的更新发展知识，信息系统审计的实践发展知识。

通过后续培训和综合评价合格的，保持《信息系统审计机构服务能力》的后续持续性。

附录

（规范性附录）

信息系统审计机构服务能力知识和技能体系

|  |  |  |
| --- | --- | --- |
| 类别 | 主题 | 职业技能 |
| 一、信息系统审计  | 1.组织体系 | 1.具有信息系统审计的组织领导、实施机构和工作机制的组织体系。 |
| 2.制度体系 | 2.具有信息系统审计的法律法规、标准规范、准则指南的知识体系和执行体系。  |
| 3.人员素质 | 3.具有与信息系统审计相适应的信息系统审计师或信息系统高级审计师的专业资格证书人员。 |
| 4.控制知识 | 4.具有信息系统的管理控制、应用控制、网络控制、安全控制，实现可靠性、安全性、经济性的控制知识体系，以及信息系统控制审计的知识和能力。 |
| 5.审计程序 | 5.具有信息系统审计计划、审前准备、审计实施、审计报告、整改跟踪的审计程序知识和质量监控体系。  |
| 6.审计方法  | 6.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和培训体系。  |
| 二、电子政务知识  | 7.国际电子政务 | 7.具有国际信息系统审计的起步与发展、发展能力和特色的知识体系和培训体系。 |
| 8.国内电子政务 | 8.具有我国信息系统审计的起步与发展、发展能力和特色的知识体系和培训体系。 |
| 9.电子政务创新 | 9.具有我国政府治理、公共服务、企业信息化等创新发展的知识体系和培训体系。  |
| 10.新技术运用  | 10.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知识体系和培训体系。  |
| 三、管理控制审计  | 11.组织管理控制审计 | 11.具有对信息系统规划建设的领导、实施、运维、监管等的组织结构和工作机制，以及法规制度和标准规范控制的审计知识和评价能力。  |
| 12.项目立项控制审计 | 12.具有对信息系统项目需求分析、建议书、可研报告和初步设计等立项报告控制的审计知识和评价能力。  |
| 13.项目实施控制审计 | 13.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知识和评价能力。  |
| 14.项目投资控制审计 | 14.具有对信息化项目预算编制与批复、预算执行、概算调整、决算编制等控制的审计知识和评价能力。  |
| 15.项目验收控制审计 | 15.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知识和评价能力。  |
| 16.项目绩效控制审计  | 16.具有对信息系统的政务效能贡献、业务信息化推动、可持续发展和能力适配指标等绩效评价控制的审计知识和评价能力。  |
| 四、应用控制审计  | 17.应用规划控制审计 | 17.具有对政府治理、公共服务、企业信息化等信息系统规划控制的审计知识和评价能力。 |
| 18.业务能力控制审计 | 18.具有对信息系统的业务处理能力、数据处理能力、系统整合能力、信息共享能力、数据开放能力、业务连续性能力、系统集约化能力、技术支撑能力、运维服务能力等控制的审计知识和评价能力。 |
| 19.分析模型控制审计 | 19.具有对信息系统的业务处理模型、数据分析模型、聚类关联分析模型、模拟仿真分析模型、决策支持模型、大数据分析模型等控制的审计知识和评价能力。 |
| 20.数据资源控制审计 | 20.具有对政府部门、公共服务机构、企业的数据资源业务目录、共享目录、开放目录，元数据、数据元素、数据表等标准规范，数据库设计等控制的审计知识和评价能力。 |
| 21.新技术运用控制审计  | 21.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知识和评价能力。  |
| 五、网络控制审计  | 22.网络系统控制审计 | 22.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知识和评价能力。 |
| 23.计算系统控制审计 | 23.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、云计算组织方式等控制的审计知识和评价能力。 |
| 24.存储系统控制审计 | 24.具有对信息系统的存储分类、存储方式、存储控制、存储性能，以及通用存储、云存储等控制的审计知识和评价能力。 |
| 25.备份系统控制审计 | 25.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知识和评价能力。 |
| 26.机房系统控制审计  | 26.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知识和评价能力。  |
| 六、安全控制审计  | 27.网络安全控制审计 | 27.具有对信息系统的网络安全就是国家安全、正确处理安全和发展、突出关键技术和运用等控制的审计知识和评价能力。 |
| 28.等级保护控制审计 | 27.具有对信息系统的网络安全等级保护制度控制，包括通用技术控制和通用管理控制，云计算、移动互联、物联网等控制的审计知识和评价能力。 |
| 29.风险评估控制审计 | 29.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知识和评价能力。 |
| 30.应急预案控制审计  | 30.具有应急预案目标、任务、指标等控制的审计知识和评价能力。  |