中国计算机用户协会团体标准

《信息系统审计机构服务能力评价》（征求意见稿）编制说明

一、任务来源，起草单位，协作单位，主要起草人

根据中国计算机用户协会下达的2019年团体标准制修订计划，将《信息系统审计机构服务能力评价》列为团体标准制订项目，该标准项目计划号为T/CUAA 002-2019，归口单位为中国计算机用户协会。

主要起草单位是：中国计算机用户协会政务信息化分会，协作单位是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。

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。

二、制定标准的必要性和意义

（一）制定标准的必要性

随着我国信息系统遍及政治、经济、文化、社会等各领域，加强对信息系统各类控制的审计，保障我国网络强国和政务信息化、社会信息化的健康安全可持续发展，是我国当前信息系统建设和监督的重要任务。

1978年，美国信息系统审计与控制协会（ISACA）组建了[信息系统审计师](https://baike.so.com/doc/5574511-5788929.html)([CISA](https://baike.so.com/doc/5019145-5244832.html))，1996年开发了《信息及相关技术控制目标》([COBIT](https://baike.so.com/doc/4952738-5174265.html))等标准，在世界160 多个国家中培养了10多万信息系统审计师。目前尚无信息系统审计机构服务能力的评价。

20世纪90年代以来，我国启动了信息系统审计。2012年，国家审计署发布了《信息系统审计指南》；2014年，中国内部审计协会发布了《第2203号内部审计具体准则——信息系统审计》；1999年，中国注册会计师协会发布《独立审计具体准则第20号——计算机信息系统环境下的审计》。我国信息系统审计在一系列指南、准则指导下得到了快速发展。但是到目前为止，我国尚无信息系统审计的国家标准、行业标准、企业标准、地方标准和团体标准，也无国家的信息系统审计职业队伍和职业机构，与我国推进网络强国和政务信息化、社会信息化的发展目标极不相符。为此，中国计算机用户协会政务信息化分会决定在全国启动信息系统审计职业机构建设，编制和推广《信息系统审计机构服务能力评价》团体标准。

（二）制定标准的意义

根据中国计算机用户协会《关于开展中国计算机用户协会团体标准工作的通知》（中计用协（2017）022号）的要求,为适应标准化工作改革的形势，满足广大计算机用户以及各行业单位对开展信息系统审计机构服务能力的实际需求，编制《信息系统审计机构服务能力评价》的团体标准。

《信息系统审计机构服务能力评价》团体标准根据当前信息系统审计的工作需要，确定了信息系统审计机构服务能力的6个方面、30个主题的知识体系和技术技能，即：在掌握信息系统审计、电子政务发展知识技能基础上，对信息系统的管理控制、应用控制、网络控制、安全控制进行审计监督，提出审计意见和建议，促进信息系统可靠性、安全性、经济性组织目标的实现。提升信息系统审计机构的服务能力，有助于保障我国网络强国和政务信息化、社会信息化的健康安全可持续发展。

三、主要工作过程

2019年初，中国计算机用户协会发布《中国计算机用户协会团体标准暂行管理办法》（2019年）。2019年3月，中国计算机用户协会政务信息化分会借着换届工作，联合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成立了信息系统审计机构服务能力的团体标准起草组，对信息系统审计机构服务能力的知识体系、技能体系和评价办法进行了调研和讨论。5月20日，团体标准调研小组受政务信息化分会委托向中国计算机用户协会提交了信息系统审计机构服务能力团体标准立项申请。5月30日，通过了中国计算机用户协会标委会组织的2019年第1批团体标准立项专家评审会。

2019年6月至7月，标准起草组走访了国家审计、内部审计、社会审计和相关信息系统建设运维组织对信息系统审计机构服务能力的业务需求。同时，依据《中国计算机用户协会团体标准暂行管理办法》的规定，讨论了信息系统审计机构服务能力的知识体系、技能体系、评价办法和行文格式等，形成信息系统审计机构服务能力团体标准的征求意见稿初稿。

2019年8月，标准起草组将征求意见稿初稿在中国计算机用户协会的政务信息化分会、信息科技审计分会、云应用分会和北京益安在线科技股份有限公司等单位的范围内进行内部征求意见。起草组根据所提意见和建议讨论修改后，形成征求意见稿。

四、制定标准的原则和依据，与现行法律、法规、标准的关系

标准的用语、格式按照GB/T1.1-2009给出的规则起草。

标准内容的编制坚持以下原则：

1.结合国内审计机构服务能力的需求

在标准制定过程中，参考了审计署《信息系统审计指南》、中国内部审计协会《第2203号内部审计具体准则——信息系统审计》的意见，遵循了《国务院关于加强审计工作的意见》（国发〔2014〕48号）提出的推进信息系统安全性、可靠性和经济性的规定，调研了国家审计署信息系统审计处室、内部审计和社会审计的信息系统审计服务的实际需求，标准提出的信息系统审计目标、知识体系、技能体系和评价办法等符合相关法律法规的要求，符合我国开展信息系统审计的实际需要。

2.借鉴国外成熟经验

标准起草组结合美国为首的《信息及相关技术控制目标》([COBIT](https://baike.so.com/doc/4952738-5174265.html))标准提出的过程性控制，提出了结构性控制的信息系统审计知识技能体系，应当说对信息系统审计知识体系具有一定的发展性。

虽然目前我国在信息系统审计方面尚无国家标准、行业标准、地方标准、企业标准和团体标准，但本标准与现行法律、法规、指南规范都不存在冲突。

五、主要条款的说明，主要技术指标、参数、实验验证的论述

本标准规定了信息系统审计机构服务能力的知识体系和技能体系，以及信息系统审计机构服务能力的等级分类和考核评价。

本标准适用于国家审计、内部审计、社会审计组织中从事信息系统审计的机构，适用于规划、建设、运用和维护信息系统的各类专业机构。

有关本标准起草过程中的一些技术问题说明如下：

（一）信息系统审计目标的说明

本标准提出：信息系统审计是指具有信息系统审计和电子政务发展基础知识和技术技能的审计机构及审计人员，对被审计单位信息系统的管理控制、应用控制、网络控制和安全控制进行可靠性、安全性、经济性的检查监督和评价活动。

依据一：2001年11月，《国务院办公厅关于利用计算机信息系统开展审计工作有关问题的通知》提出审计机关有权检查被审计单位运用计算机管理财政收支、财务收支的信息系统。2006年2月修订的《中华人民共和国审计法》提出了审计机关有权检查被审计单位的运用电子计算机管理财政收支、财务收支电子数据的系统。2014年10月，《国务院关于加强审计工作的意见》（国发〔2014〕48号）提出，推进对各部门、单位计算机信息系统安全性、可靠性和经济性的审计。

依据二：我国从20世纪90年代以来尤其是2014年国发〔2014〕48号文件后开展的信息系统审计实践，突出了对信息系统的可靠性、安全性、经济性的检查监督。

我国信息系统审计实践表明：信息系统的可靠性、安全性、经济性不仅是信息系统组织关心的问题，更是信息系统审计机构关心的问题，也是我国网络强国和政务信息化、社会信息化关心的重大问题。

（二）信息系统控制审计的说明

本标准提出：对被审计单位信息系统的管理控制、应用控制、网络控制和安全控制进行审计检查。

依据一：2012年2月，审计署发布《信息系统审计指南》（审计发〔2012〕11号）提出，项目管理审计、应用控制审计、一般控制审计。其中，一般控制审计包括物理、网络、主机、应用、数据和信息化装备自主可控。

依据二：2013年，中国内部审计协会发布的《第2203号内部审计具体准则——信息系统审计》提出，信息系统审计的内容是组织层面信息技术控制、信息技术一般性控制、业务流程层面相关应用控制。

依据三：根据我国信息系统审计实践，参照《信息系统审计指南》、《信息系统审计具体准则》关于开展信息系统控制审计的要求，本标准提出了管理控制、应用控制、网络控制和安全控制的4大控制和控制审计理论。

（三）信息系统审计机构服务能力的说明

本标准提出：具有1级、2级信息系统审计机构服务能力的组织，应当具有相应的信息系统高级审计师，而信息系统高级审计师应当具有信息系统管理控制审计、应用控制审计、网络控制审计、安全控制审计中的任一专业方向关键技术的突破能力。

依据一：信息系统的关键技术已经成为我国信息化发展的重要问题。2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上的讲话中指出，互联网核心技术是我们最大的“命门”，核心技术受制于人是我们最大的隐患。我们要掌握我国互联网发展主动权，保障互联网安全、国家安全，就必须突破核心技术这个难题，争取在某些领域、某些方面实现“弯道超车”。

依据二：突破信息系统的关键技术必须发展具有信息系统高级审计师的审计机构。习近平总书记在网络安全和信息化工作座谈会上说，聚天下英才而用之，为网信事业发展提供有力人才支撑。我国网信事业发展，必须充分调动企业家、专家学者、科技人员积极性、主动性、创造性。

因此，具有1级、2级信息系统审计机构服务能力的组织，应当具有突破信息系统审计关键技术的能力，这正是本标准的重要预期。

六、重大意见分歧的处理依据和结果

无。

七、采用国际标准和国外先进标准的，说明采标程度，以及与国内外同类标准水平的对比情况

（一）与国际标准的比较

1996年，美国信息系统审计与控制协会（ISACA）开发的《信息及相关技术控制目标》([COBIT](https://baike.so.com/doc/4952738-5174265.html))标准中，提出了“规划与组织、获取与实施、交付与支持、监控与评价”的4类过程性控制审计，有效性、高效性、机密性、完整性、可用性、符合性、可靠性7类目标。

信息系统的内部控制既有过程性控制，也有结构性控制。在我国的信息系统审计中，既关心信息系统生命周期的过程性控制，也关心管理控制、应用控制、网络控制、安全控制的结构性控制。

为此，本标准根据我国信息系统审计发展的实践，提出了管理控制、应用控制、网络控制、安全控制的结构性控制审计。

（二）与国内标准的比较

目前，国内尚无信息系统审计的国家、行业、地方、企业和团体的标准。根据审计署发布的《信息系统审计指南》、中国内部审计协会发布的《第2203号内部审计具体准则——信息系统审计》、中国注册会计师协会发布的《独立审计具体准则第20号——计算机信息系统环境下的审计》的相关要求，本标准提出的信息系统审计目标、信息系统控制和审计的知识体系与技术技能、较高等级审计机构服务能力的关键技术突破，不仅符合国内标准的要求，更具有较为完整的和长远的意义。

八、作为推荐性标准的建议及其理由

（一）作为推荐性标准的建议

本标准对于强化我国的网络强国和政务信息化、社会信息化的可持续发展具有重要意义。信息系统审计机构服务能力既是国家治理体系和治理能力现代化的重要标志，也需要在全国范围内普遍推广。为此，建议将本标准作为推荐性标准。

（二）作为推荐性标准的理由

目前，我国尚无信息系统审计的国家标准、行业标准、地方标准、企业标准和团体标准。作为一个发展中的大国和强国，没有理由不编制团体标准，在全国推广信息系统审计职业机构的建设。这是建议将本标准作为推荐性标准的重要理由。

九、强制性标准实施的风险点、风险程度、风险防控措施和预案。

无（该标准为推荐性标准）

十、实施标准的措施建议

根据本标准的编制和推广，政务信息化分会已经联合相关分会、培训机构着手信息系统审计职业队伍建设的相关工作：编写了《信息系统审计教学大纲》和《信息系统审计》《电子政务发展》教材、相应的讲稿、题库，进行信息系统审计机构服务能力的培训和考察等研究，联合相关的培训机构开展信息系统审计职业机构的培训发展。

根据《信息系统审计机构服务能力评价》团体标准的要求，2019年开展信息系统审计机构服务能力的培训前期准备，2020年开展信息系统审计机构的服务能力培训。

十一、其他应说明的事项

无

标准起草组

2019年8月20日