CNAS-SC175

基于ISO/IEC 20000-1的服务管理体系认证机构认可方案

Accreditation scheme for bodies providing audit and certification of service management systems based on ISO/IEC 20000-1

中国合格评定国家认可委员会

2017 年 01 月 01 日 发布　　2017 年 12 月 29 日第 1 次修订　　2018 年 01 月 01 日 实施

目　　次

前　言 2
1　范围 3
2　规范性引用文件 3
3　术语和定义 3
4　SMS 认证机构认可规范的构成 3
R 部分 4
R.1 预访问（CNAS-RC01 条款 5.1.4） 4
R.2 初次认可的见证评审（CNAS-RC01 条款 5.4.3.1） 4
R.3 认证业务范围的认可（CNAS-RC01 条款 6） 4
R.4 信息通报（CNAS-RC03 条款 5.2） 5
R.5 其他 5
C 部分 5
C.1 通用要求（CNAS-CC01 条款 5.1 至 5.3） 5
C.2 信息要求（CNAS-CC01 条款 8.1 至 8.5） 5
C.3 过程要求（CNAS-CC01 条款 9.1 至 9.9） 5
G 部分 6
G.1 服务点的抽样 6
附录 A（规范性附录）SMS 认证机构认证业务范围分类 8

前　言

本文件由中国合格评定国家认可委员会（CNAS）制定。

本文件是 CNAS 对依据 ISO/IEC 20000-1 实施服务管理体系认证的机构所提出的特定要求和指南，并与相关认可规则和认可准则共同用于 CNAS 对这类认证机构的认可。

本文件中，用术语“应”表示相应条款是强制性的，用术语“宜”表示建议。

本文件附录 A 为规范性附录。

本文件 2017 年 1 月首次发布，本次是第一次修订，主要修订内容如下：

1） 文件名称由“信息技术服务管理体系认证机构认可方案”调整为“基于 ISO/IEC 20000-1 的服务管理体系认证机构认可方案”；

2） R 部分：删除了原 R.1-认可申请，并调整了原 R.4-认证业务范围的认可的相关描述；

3） C 部分：删除了原 C.2-C.5 节中有关能力管理的要求，以及原 C.7.2-针对特定客户的审核和认证能力需求分析价等内容；

4） G 部分：删除了原 G.1-ITSMS 认证范围界定指南、G.2- ITSMS 审核时间确定指南和附录 B，修改了原 G.3-服务点的抽样。

基于 ISO/IEC 20000-1 的服务管理体系认证机构认可方案

1 范围

1.1 为确保中国合格评定国家认可委员会（CNAS）对依据 ISO/IEC 20000-1《信息技术 服务管理 第 1 部分：服务管理体系要求》开展服务管理体系（SMS）认证的认证机构（以下简称“SMS 认证机构”）实施评审和认可的一致性，指导申请和获得认可的 SMS 认证机构理解和实施认可规范要求，特制定本文件。

1.2 本文件包括对 SMS 认证机构认可规范的补充和指南，适用于 CNAS 对 SMS 认证机构的认可。

本文件 R 部分和 C 部分分别是对相关认可规则和认可准则的补充。本文件 G 部分是对相关认可准则的应用指南。

2 规范性引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。注明日期的引用文件，仅该版本适用于本文件；未注明日期的引用文件，其最新版本（包括任何修订）适用于本文件。

CNAS-CC01 管理体系认证机构要求

ISO/IEC TR 20000-10 信息技术 服务管理 第 10 部分：概念与术语

CNAS-CC12 已认可的管理体系认证的转换

3 术语和定义

CNAS-CC01 和 ISO/IEC 20000-10 中的术语和定义以及下列术语和定义适用于本文件。

3.1 服务点：客户在服务级别协议有效期内进行特定工作或服务的地点，该地点不在客户的物理范围内，且不会成为常设场所。例如驻场服务的客户现场等。

注：该定义基于“临时场所”的定义（见 CNAS-CC11，1.3）并进行了改写。

4 SMS 认证机构认可规范的构成

4.1 主要规则和准则：

CNAS-RC01《认证机构认可规则》是 SMS 认证机构认可活动的基本程序规则；

CNAS-CC01《管理体系认证机构要求》是 SMS 认证机构的基本认可准则；

CNAS-CC175《基于 ISO/IEC 20000-1 的服务管理体系认证机构要求》是 SMS 认证机构的专用认可准则。

4.2 其他适用的认可规则包括：

a) CNAS-R01《认可标识使用和认可状态声明规则》
b) CNAS-R02《公正性和保密规则》
c) CNAS-R03《申诉、投诉和争议处理规则》
d) CNAS-RC02《认证机构认可资格处理规则》
e) CNAS-RC03《认证机构信息通报规则》
f) CNAS-RC04《认证机构认可收费管理规则》
g) CNAS-RC05《多场所认证机构认可规则》
h) CNAS-RC07《具有境外场所的认证机构认可规则》

4.3 其他适用的认可准则包括：

a) CNAS-CC11《多场所组织的管理体系认证》
b) CNAS-CC12《已认可的管理体系认证的转换》
c) CNAS-CC14《计算机辅助审核技术在获得认可的管理体系认证中的使用》
d) CNAS-CC106《CNAS-CC01 在一体化管理体系审核中的应用》

R 部分

R.1 预访问（CNAS-RC01 条款 5.1.4）

必要时，CNAS 可在受理申请过程中安排预访问，以了解申请方是否已满足认可申请条件和是否基本具备接受认可评审的条件。

R.2 初次认可的见证评审（CNAS-RC01 条款 5.4.3.1）

初次认可时，CNAS 将至少见证 1 次认证机构对同一客户实施的第一阶段审核和第二阶审核。

R.3 认证业务范围的认可（CNAS-RC01 条款 6）

R.3.1 SMS 认证业务范围分类（CNAS-RC01 条款 6.2）

本文件附录 A 规定了认证业务范围。

CNAS 根据附录 A 来确定认证机构的认可业务范围，通常认可到表 A.1 中的大类。

R.3.2 SMS 认证业务范围认可的见证评审要求（CNAS-RC01 条款 6.3.3）

CNAS 根据认证机构 SMS 认证活动的范围、规模、风险水平和绩效对其认证业务范围的大类实施见证评审。

初次认可时，CNAS 至少选取 1 个所申请认认可的认证业务范围大类实施见证评审。

R.4 信息通报（CNAS-RC03 条款 5.2）

CNAS-RC03 条款 5.2 中“获证组织发生重大事故/事件”是指 SMS 获证客户发生具有下列之一影响的服务质量事故：

a) 已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益；
b) 可能损害颁证机构或 CNAS 的公信力、声誉，或使颁证机构或 CNAS 承担连带责任。

R.5 其他

如果 CNAS 可能需要在评审中接触认证机构的客户的相关信息，认证机构应向相关客户询问是否同意 CNAS 接触这些信息。如果客户同意，认证机构应识别 CNAS 接触这些信息时须满足的所有要求，并告知 CNAS。如果客户不同意或 CNAS 无法满足相关要求，CNAS 将根据评审所受的影响采取相应的措施。

C 部分

C.1 通用要求（CNAS-CC01 条款 5.1 至 5.3）

C.1.1 风险评估和责任安排（CNAS-CC01 条款 5.3.1）

认证机构应对其审核和认证活动可能给客户的信息安全带来的风险以及认证机构可能承担的责任进行评估，并做出充分的安排（例如，购买职业责任保险或设立储备金）。

C.2 信息要求（CNAS-CC01 条款 8.1 至 8.5）

C.2.1 保密（CNAS-CC01 条款 8.4）

C.2.1.1 如果客户事先没有禁止认证机构接触某一信息，或未告知认证机构应满足的要求，但认证机构在认证过程中发现自己并不具备接触该信息的资格和条件，应立即向客户提出。

C.2.1.2 认证机构宜要求直接接触客户信息的认证人员（例如审核组成员）遵守客户的保密政策，例如：按照客户的保密要求与客户签署保密协议。

C.2.1.3 审核组成员不宜在审核过程中以任何方式记录客户的保密或敏感信息。审核组在离开客户前，宜请客户检查和确认审核组携带的文件、资料和设备中未夹带客户的任何保密或敏感信息。

C.3 过程要求（CNAS-CC01 条款 9.1 至 9.9）

C.3.1 申请（CNAS-CC01 条款 9.1.1）

C.3.1.1 认证机构宜要求客户向其说明适用的关于认证机构的资质、诚信守法记录或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求，并即时更新该说明，以便认证机构判断其是否具备对该客户实施认证活动的资格或条件。

C.3.1.2 适用时，认证机构可要求客户指明其在申请认证的 SMS 范围内与其他方共同提供服务的情况。

C.3.2 审核方案（CNAS-CC01 条款 9.1.3）

对于获得CNAS认可的其他认证机构所颁发的SMS认证，认证机构可以按照CNAS-CC12实施转换。

C.3.3 第一阶段（CNAS-CC01 条款 9.3.1.2）

当客户由于信息安全的原因在申请评审阶段不能提供给认证机构足够的信息时，认证机构应通过第一阶段审核在客户的现场补充对上述信息的确认，并完成申请评审。这种情况下，认证机构应增加第一阶段现场审核时间。

G 部分

G.1 服务点的抽样

通过在服务点观察客户的服务状况、与相关人员（如驻场的服务工程师、客户的顾客等）面谈以及调阅现场服务记录，认证机构可以收集客户 SMS 运行和有效性的证据。

G.1.1 抽样条件

当客户拥有满足以下条件的多个服务点时，认证机构可以考虑使用基于抽样的方法对服务点进行审核：

a) 所有场所的工作人员均在同一个 SMS 下进行管理，客户对人员具有分配和调配的权力，有权要求场所内提供服务的工作人员提供工作量和工作质量的数据；
b) 客户在所有的场所提供的服务和活动的变动，或场所的成立和撤销不影响客户的 SMS 运行的完整性；
c) 所有的场所都包含在客户的 SMS 内部审核方案和管理评审方案中。

G.1.2 抽样方法

1) 在确定服务点的抽样量时，针对审核时客户所具有的服务点，认证机构可先考虑确保样本覆盖认证范围内的业务类别，然后再根据服务点数量适当增加抽样量。
   a) 初次认证审核、监督审核和再认证审核时，样本覆盖认证范围内所涉及到的表 A.1 中的中类；
   b) 初次认证审核和再认证审核时，在满足 a）的基础上按照下表增加抽样量：

服务点数量（个）	增加的服务点抽样量（个）
5 ~ 10	1
11 ~ 20	2
21 ~ 40	3
41 ~ 60	4

注：当服务点的数量超过 60 时，可沿用上表的规律确定应增加的抽样量。

2) 抽样时，优先选取同种业务类型中业务复杂程度高且服务交付风险大的服务点；

3) 对出现审核组无法访问服务点的情形规定了应对措施。

G.1.3 审核时间

1) 认证机构分配给每个服务点的审核时间宜与审核组在该服务点所需完成的审核活动相匹配。

2) 通常，每个服务点的审核宜不少于 0.25 个人天。

3) 每个服务点的审核时间不含审核员的旅途时间。

附录 A（规范性附录）

SMS 认证机构认证业务范围分类

表 A.1 SMS 认证机构认证业务范围分类

大类	中类	中类内容	备注
01 规划与设计服务	01.01	信息系统咨询规划	信息系统咨询、规划服务
	01.02	信息系统硬件设计、开发服务	对信息系统硬件的架构、选型和实施策略进行设计，并实施开发。
	01.03	信息系统软件设计、开发服务	软件设计、开发服务。
	01.04	信息技术咨询服务	硬件或软件使用的咨询及培训服务。
02 集成服务	02.01	设备系统集成服务	指以搭建需方的信息化管理支持平台为目的，将设备及其嵌入式软件进行集成设计、安装调试的服务。如网络系统集成服务、智能建筑系统集成服务、安全防护系统集成服务等。
	02.02	软件系统集成服务	将各个分离的软件、功能和信息等集成到相互关联的、统一和协调的平台之中的服务。如界面集成、数据集成、应用集成等。
03 测试与监理服务	03.01	信息系统测试服务	检验信息系统是否与要求相吻合的测试服务。
	03.02	软件产品测试服务	检验软件产品是否与要求相吻合的测试服务。
	03.03	信息系统工程监理	对信息系统工程实施监理的服务。
	03.04	软件工程监理服务	对软件开发实施监理的服务。
	03.05	其他测试与监理服务	
04 运行维护服务	04.01	基础设施运行维护服务	机房电力、空调、消防、安防、网络等设施的运维服务。
	04.02	硬件运行维护服务	计算机及其外部设备、网络设备、音视频设备、自动化控制设备及其他采用信息技术控制的硬件及设备的状态监控、故障处理、性能优化等相关维护服务。
	04.03	软件运行维护服务	基础软件和应用软件的安装、升级、故障处理、病毒防护等维护服务。
	04.04	其他信息技术运行维护服务	

大类	中类	中类内容	备注
05 安全服务	05.01	风险评估	评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。
	05.02	安全运维	通过专业的服务，解决网络和信息系统日常运行中的安全问题，包括系统安全加固、日常安全监控、定期安全审计、安全通告、补丁更新以及安全技术支持等。
	05.03	应急处理	为降低安全事件给客户造成的损失和影响，在处置网络与安全事件时提供一系列的措施和行动。
	05.04	灾难恢复	将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态的活动和流程。
	05.05	其他安全服务	
06 业务流程服务	06.01	电子商务支持服务	电子商务活动的支持和管理服务。
	06.02	软件运营服务	通过网络提供软件功能的服务。
	06.03	数据处理	图片、文字、影像、语音等信息内容运用数字化技术进行加工处理、运用的服务。
	06.04	呼叫中心/服务台服务	呼叫中心服务。
	06.05	其他业务流程服务	

注：依据GB/T 29264-2012《信息技术服务 代码与分类》和国家认证认可监督管理委员会2012年第8号公告《关于开展信息技术服务管理体系认证工作的公告》制定了上表。

——