CNAS-SC170

信息安全管理体系认证机构认可方案
（征求意见稿）

Accreditation Scheme for ISMS Certification Bodies

中国合格评定国家认可委员会

2024 年 XX 月 XX 日 发布　　2024 年 XX 月 XX 日 实施

目 次

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对信息安全管理体系（ISMS）认证机构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ISMS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。

本文件代替了 CNAS-SC170:2017。

信息安全管理体系认证机构认可方案

1 范围

1.1 为确保CNAS对实施ISO/IEC 27001认证的信息安全管理体系（以下称为“ISMS”）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ISMS认证机构理解和实施认可规范要求，特制定本文件。

1.2 本文件包括对信息安全管理体系认证机构认可规范的补充说明和指南，适用于CNAS对ISMS认证机构的认可。

1.3 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和说明。

2 规范性引用文件

无

3 术语和定义

CNAS-CC01、CNAS-CC170和CNAS-RC01中的术语和定义适用于本文件。

4 ISMS认证机构认可规范的构成

本文件与下列文件共同组成ISMS认证机构认可规范

—CNAS-R01《认可标识使用和认可状态声明规则》

—CNAS-R02《公正性和保密规则》

—CNAS-R03《申诉、投诉和争议处理规则》

—CNAS-RC01《认证机构认可规则》

—CNAS-RC02《认证机构认可资格处理规则》

—CNAS-RC03《认证机构信息通报规则》

—CNAS-RC04《认证机构认可收费管理规则》

—CNAS-RC05《多场所认证机构认可规则》

—CNAS-RC07《具有境外场所的认证机构认可规则》

—CNAS-CC01《管理体系认证机构要求》

—CNAS-CC11《基于抽样的多场所认证》

—CNAS-CC12《已认可的管理体系认证的转换》

—CNAS-CC14《信息和通信技术（ICT）在审核中应用》

—CNAS-CC106《CNAS-CC01在一体化管理体系审核中的应用》

—CNAS-CC170《信息安全管理体系认证机构要求》

R 部分

R.1 认证业务范围的认可

R.1.1 附录 A 规定了 ISMS 认证机构认证业务范围分类与分级。

R.1.2 CNAS 按附录 A 的业务范围分类进行认可。

注：认证机构应在提交认可申请时明确拟申请的业务范围，包括相应的大类或中类。

R.1.3 CNAS 对 ISMS 认证机构认证业务范围的认可不包括中华人民共和国境内（不含香港、澳门特别行政区，台湾地区）的各级政府机关、政府信息系统运行单位和涉密信息系统建设使用单位。

R.2 见证评审

R.2.1 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.2.2 认证业务范围认可的见证评审要求

1）附录 A 中每个大类的一级中类分别为一个独立的需强制见证组别，CNAS 采取抽样的方式对每个技术组中某个中类实施见证评审。

2）附录 A 中的二级和三级中类为一个非强制见证组别，适用时，CNAS 优先选取该技术组中一个风险级别高的某一中类实施见证评审。

R.2.3 对于已获得认可资格的认证机构，每年应进行至少一次见证评审。

在每个完整的 5 年认可周期内，CNAS 至少对一个获认可的强制见证组别实施 1 次见证评审。当不满足完整的 5 年认可周期时，优先选取风险等级高的中类实施见证。

R.3 对认证机构客户的信息及其相关资产的访问安排

当认证机构的客户不同意 CNAS 在认可评审中访问其信息和相关资产时，认证机构应提前告知 CNAS, CNAS 将根据评审所受的影响采取相应的措施。

C 部分

C.1 认证协议（CNAS-CC01:2015 5.1.2）

认证协议应就控制审核和认证活动引发的客户信息安全风险做出规定，包括明确认证机构和客户及其有关人员的责任与义务。

C.2 客户记录的获取（CNAS-CC170:2024 8.4.2）

C.2.1 认证机构直接接触客户信息的认证人员（例如审核组成员）宜按照客户的保密要求与客户签署保密协议，或向客户做出保密承诺。

C.2.2 如果客户事先没有禁止认证机构接触某一信息和相关资产，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资产的资格和条件，应立即向客户提出。

C.2.3 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 ISMS 的变化（CNAS-CC01:2015 8.5.3）

认证机构应要求客户即时报告其 ISMS 范围内活动边界（见 CNAS-CC170:2024 9.1.3.6）和 ISMS 适用法律法规的重大变更。

C.4 认证申请（CNAS-CC01:2015 9.1.2）

C.4.1 认证机构应确保认证申请客户承诺遵守工信部联协[2010]394 号文《关于加强信息安全管理体系认证安全管理的通知》的要求，以及有关主管部门/监管部门对信息安全管理体系认证的管理要求（如工信部 2011 年第 21 号公告《工业和信息化部加强政府部门信息技术外包服务安全管理》等）。

C.4.2 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.5 初次认证第一阶段（CNAS-CC01:2015 9.3.1.2）

认证机构宜合理分配第一阶段审核时间，并予以记录。认证机构应在一阶段对客户的文件化管理体系信息进行充分审核。

C.6 认证机构的管理体系（CNAS-CC170:2024 10.1.1）

C.6.1 认证机构宜在其方针、政策、目标和承诺上体现自身的信息安全意识和追求，并在管理体系的建立和实施中予以体现。

C.6.2 认证机构宜将自身信息安全绩效作为管理评审的输入，包括考虑认证活动对客户信息安全的影响所采取的管控措施。

附录A（规范性附录）

ISMS认证机构认证业务范围分类与分级

大类	中类	级别	描述	备注
01	政务			
	01.01	一	国家机构	包括人大、政府、法院、检察院等，不含税务机关和海关
	01.02	一	税务机关	
	01.03	一	海关	
	01.04	二	其他	例如政党，政协，社会团体等
02			公共	
	02.01	一	通信、广播电视	
	02.02	一	新闻出版	包括互联网内容的提供
	02.03	二	科研	涉及特别重大项目的应提升为一级
	02.04	二	社会保障	例如社会保险基金管理、慈善团体等。包括医疗保险
	02.05	一	医疗服务	
	02.06	三	教育	
	02.07	二	其他	例如市政公用事业（水的生产和供应、污水处理、燃气生产和供应、热力生产和供应、城市水陆交通设施的维护管理等）
03			商务	
	03.01	一	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、审计、公证等
	03.05	二	旅游、宾馆、饭店	
	03.06	三	其他	
04			产品的生产	产品包括软件、硬件、流程性材料和服务
	04.01	一	电力	包括发电和输、变、配电等
	04.02	一	铁路	
	04.03	一	民航	
	04.04	一	化工	
	04.05	一	航空航天	
	04.06	一	水利	
	04.07	二	交通运输	包括公路、水路、城市公共客运交通等，不含航空和铁路
	04.08	二	信息与通信技术	例如软、硬件生产及其服务，系统集成及其服务，数字版权保护等
	04.09	二	冶金	
	04.10	二	采矿	含石油、天然气开采
	04.11	二	食品、药品、烟草	
	04.12	三	农、林、牧、副、渔业	
	04.13	三	其他	

注1：ISMS认证机构认证业务范围分类是为了在规范的框架下对认证机构的能力实施评审，并相应地限定其认可范围，以促使ISMS认证活动规范、有序地发展，控制认可风险；同时给各认证机构开展能力分析和评价提供一致的框架。该分类并不意味着CNAS批准认证机构可以对每个类别中的任何组织实施认证活动。

注2：认证业务范围分为三个级别，一级最高。认证业务范围分级是为了使CNAS在确定认证业务范

围的评审方式时考虑相关的风险，从而对认证机构业务活动的扩展进行控制，降低认可风险。这里的风险是指 CNAS 认可的风险，即 CNAS 认可的 ISMS 认证机构所认证的组织的信息安全发生问题时，连带使 CNAS 声誉受损或承担责任的风险。每个中类的级别主要考虑了在该中类信息安全对于国家安全、社会秩序、公共利益、组织及其相关方合法权益的重要性的典型情况。