

中 华 人 民 共 和 国

行 业 标 准

XX/T XXXXX—XXXX

代替 XX/T

合规管理体系审核和认证机构认可要求

Accreditation requirements for bodies providing audit and certification of compliance
management systems

(点击此处添加与国际标准一致性程度的标识)

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。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

发 布

目 次

前 言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 原则 1

5 通用要求 1

6 结构要求 1

7 资源要求 1

8 信息要求 2

9 过程要求 2

10 认证机构的管理体系要求 4

附 录 A （规范性） 5

附 录 B （规范性） 7

参 考 文 献 9

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。

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专利的责任。

本文件由国家认证认可监督管理委员会提出并归口。

本文件起草单位：

本文件主要起草人：

合规管理体系审核和认证机构认可要求

1 范围

本文件规定了合规管理体系审核和认证机构认可要求，包括原则、通用要求、结构要求、资源要求、信息要求、过程要求和管理体系要求。

本文件适用于申请或持续保持合规管理体系认证认可资格的认证机构，其他机构可参照适用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 27000 合格评定术语和通用原则

GB/T 27021.1 -2017 合格评定 管理体系审核认证机构要求 第1部分

GB/T 35770 合规管理体系 要求和使用指南

3 术语和定义

GB/T 27000、GB/T 27021.1和GB/T 35770界定的术语和定义适用于本文件。

4 原则

合规管理体系（简称CMS）审核和认证机构应通过公正、有能力的评定建立公信力。建立公信力的原则包括公正性、独立性、公开性、保密性、能力、责任、对投诉的回应、基于风险和证据的方法。

5 通用要求

5.1 合规管理体系（简称CMS）认证机构应满足相关国际标准和国家标准要求，在此基础上，如申请或持续保持认可资格时，适用本文件。

5.2 认证机构应对其认证活动的公正性负责，不应允许商业、财务或其他压力损害公正性。影响公正性的管理体系咨询活动包括且不限于：参与组织内部管理体系文件编制；参与组织内部审核；参与组织内部管理评审等。

5.3 认证机构应能证明已对认证活动引发的风险进行了评估，并对各个业务领域和运作地域的认证活动引发的责任作了充分的安排（如保险或储备金）。认证活动引发的风险包括且不限于：

- a) 未获得认证资格从事认证活动；
- b) 提供了有损认证公正性的管理体系咨询；
- c) 减少或遗漏认证程序；
- d) 违背真实性原则，导致认证失效。

6 结构要求

GB/T 27021.1-2017，6的要求适用。

7 资源要求

7.1 通用要求

认证机构应有足够的人员以满足其合规管理体系认证管理活动的有效运行，且有过程证明其人员具备实施特定的认证职能所需要的知识和技能。

认证机构应有获取必要的专业知识与技能的途径，以在其运营涉及的技术领域、法律法规等方面获得相关的建议。这些建议可由外部人员或认证机构人员提供。

7.2 知识和技能

认证机构应根据组织的行业、合规义务和合规风险确定审核组所需的知识和技能。

认证机构应通过多种方式评估并证明审核员和技术专家具备相应的知识和技能。

注：评估和证明的方式可包括专业资格、教育背景、工作经验或有效的培训等。

7.3 选择审核员

认证机构应确保CMS审核员满足：

- a) 至少持有一个在中国境内有效的管理体系认证领域的注册证书；
- b) 具有大学专科（含）以上高等教育学历；
- c) 至少2年合规管理经验或至少3年审核过程相关工作经验；
- d) 至少完成16小时的培训，并提供培训结果证明，培训内容应至少包括 CMS 审核和法律法规知识；
- e) 在承担审核员职责之前，获得 CMS 全部审核认证流程的经验。这些经验应是通过参与 CMS 审核认证获得的。可以是初次认证、再认证或监督审核。参与内容应包括文件审核、风险评估和审核报告。

技术专家应符合b)和c)的要求。

7.4 选择审核组长

认证机构应确保选派的审核组长在 CMS 审核的所有关键流程（包括策划、文件审查、风险评估、实施审核以及审核报告）均具备能力，并且至少参与过两次完整的 CMS 审核（初次审核或再认证审核）。

如认证机构有文件化依据，则：

- a) 已具备其他管理体系审核组长资格的审核员，采取有效评价后确定该审核员为CMS审核组长；
- b) CMS作为机构新开展的认证制度，最初一批CMS审核组长可采取其他有效评价后确定。

8 信息要求

8.1 CMS认证用以确保组织已实施了与GB/T 35770-2022/ISO 37301:2021的要求一致的合规管理体系。

8.2 CMS认证证书不应应对组织运营的合法性和合规性进行保证，不应替代、豁免或担保组织对法律法规和监管要求等合规义务的遵守。

8.3 CMS认证文件应就获证组织在认证范围内的合规管理体系满足相关标准做出表述。

示例：CMS认证文件宜描述：XX公司运行的合规管理体系符合GB/T 35770-2022/ISO 37301:2021要求，认证范围为：印刷生产涉及的合规管理；或XX公司运行的合规管理体系符合GB/T 35770-2022/ISO 37301:2021要求，认证范围为：印刷生产涉及的财务合规管理、税务合规管理。

9 过程要求

9.1 认证前活动

9.1.1 申请

认证机构要求申请CMS认证的组织提供的必要信息应包括但不限于：

- a) 组织对其CMS范围内的合规风险的识别、分析和评价；
- b) 组织所识别的与CMS范围内的产品、服务、过程有关的合规义务和合规风险；
- c) 在CMS范围内代表组织开展工作的代理商、外包方的详细信息。

9.1.2 申请评审

认证机构应制定关于申请评审阶段对客户进行背景调查的文件化规定，以有效评估认证风险。背景调查的方式可包括客户自身的风险评估、查询客户司法诉讼情况、媒体报道、相关方投诉等。

认证机构应将背景调查情况和认证风险评估形成文件化记录。

9.1.3 确定审核时间

认证机构应按附录 A 的规定确定审核时间，并制定文件化程序。

认证机构应确定审核计划和完成客户 CMS 完整有效审核所需的时间，审核时间的确定和调整应进行合理性分析并形成文件化记录。

9.1.4 多场所抽样

对于CMS覆盖多个场所的情况，应基于与活动和过程的性质相关的合规风险评估，确定认证范围内的每个场所可否抽样，并将理由记录在案。当允许抽样时，认证机构应确保被审核的场所样本具有被审核组织过程、活动和合规风险的代表性。

如果多个场所有类似活动、过程或合规风险，认证机构仍应考虑每个场所的业务活动（如技术、设备、工作环境等）及所处环境（如法律、司法、监管、合规文化等）之间的差异。

如果多个场所没有涵盖相同的活动、过程或合规风险，抽样不适用。

每个场所的审核时间计算应基于附录A的要求，且单个被抽样场所审核时间的减少量不超过50%。

9.2 策划审核

CMS审核策划和实施应围绕评估客户的CMS与GB/T 35770-2022/ISO 37301:2021要求的符合性。

CMS审核计划应考虑被审核范围内的合规义务和合规风险。如果客户要求对某些职能、活动或场所进行排除（例如，销售、运营、供应商、业务伙伴等），认证机构需要评估这些排除是否存在可能影响认证范围和客户CMS有效运行的风险，并根据评估结果做出决定。认证机构应将评估过程形成文件化记录。

如果客户将部分CMS职能外包给第三方，认证机构应在审核中包括这些外包职能的管理活动，并确定其有效性。

审核组可以由一个人组成，只要其满足CMS审核能力相关的要求。当为特定认证审核选择审核组时，认证机构应确保每次委派时审核组的能力是适宜的。审核组应：

a) 对拟认证CMS范围内的业务活动和过程具备适当的知识，以及对这些活动中产生的合规风险具备适当的知识；

注：适用时，技术专家可以履行此项职责。

b) 对客户在管理其活动、产品和服务合规方面的CMS范围和组织环境的理解足以达到对其CMS实施可靠的认证审核；

c) 具备并理解适用于客户CMS的法律法规及其他要求。

注：具备一般不意味着要有深厚的法律背景。

9.3 初次认证

GB/T 27021.1-2017，条款9.3的要求适用。

9.4 实施审核

9.4.1 审核组代表认证机构，应：

a) 根据所有适用的认证要求，对包含在认证范围内的客户 CMS 进行审核；

b) 确认客户的合规风险评估和风险处理反映其业务活动，并延伸到认证范围所界定的活动边界；

c) 证实客户对合规风险的评估与 CMS 范围内的 CMS 运行是相关的和充分的；

- d) 确定客户识别、分析和评价合规风险的策划及其控制结果与客户的方针、目标和指标相一致；
- e) 确认客户用于风险评估的过程可靠并得到正确实施。

9.4.2 审核组应与下列人员进行访谈：

- a) 治理机构代表和最高管理者；
- b) 合规职能代表；
- c) 相关职能部门代表；
- d) 不合规疑虑和不合规情形调查部门代表；
- e) 工人组织（工会）代表。

9.5 认证决定

GB/T 27021.1-2017，条款9.5的要求适用。

9.6 保持认证

认证机构应确保在整个认证周期内收集与客户CMS整体相关的证据。

认证机构如发现获证组织发生了与CMS有关的严重事件，如严重违法或具有重大社会影响的司法诉讼等，认证机构应立即采取措施以确认获证组织的合规管理体系是否存在严重问题以及是否有效发挥作用。认证机构应对调查情况和采取的措施进行记录。

这些要求应是认证机构和客户签署的合同协议的一部分。

9.7 申诉

GB/T 27021.1-2017，条款9.7的要求适用。

9.8 投诉

GB/T 27021.1-2017，条款9.8的要求适用。

9.9 客户的记录

GB/T 27021.1-2017，条款9.9的要求适用。

10 认证机构的管理体系要求

GB/T 27021.1-2017，条款10的要求适用。

附录 A (规范性)

合规管理体系审核时间

A.1 总则

本文件提供了具体的要求，包括确定审核时间的要求。本附录包含了与 ISO/IEC 17021-1: 2015 中 9.1.4 有关的进一步要求。认证机构应确定每个客户和已获证组织的合规管理体系初次认证、监督和再认证的审核时间。

A.2 确定审核时间

审核时间应根据 A.3 中描述的 CMS 有效人员数量来确定。审核时间可以基于 A.4 中的各种因素，进行调整。

A.3 确定有效人员

A.3.1 CMS 有效人员应包括认证范围内的长期人员、全职人员、临时人员和兼职人员，每个工作班次都应考虑在内。此外，应考虑影响合规管理体系运行的承包商或外部服务提供者。

A.3.2 认证范围内的 CMS 有效人员应根据认证机构确定的程序进行计算。此程序应确保有足够的信息说明人员对 CMS 和合规绩效的作用和影响，以便认证机构确定有效 CMS 人员的数量。CMS 有效人员应包括以下人员：

- a) 治理机构和最高管理层；
- b) 中心、地区和地方合规职能，若适用；
- c) 负责建立、实施、保持、完善合规管理体系的人员；
- d) 协助合规管理体系运行的职能部门人员，例如人力资源、财务会计、内部控制或负责处理提出合规疑虑的人员；
- e) 管理与认证范围内的合规义务相关的面临合规风险的职能人员；
- f) 履行期任务和职责时面临与认证范围内合规义务相关的合规风险人员；
- g) 负责做出影响合规绩效重要变更的人员。

应避免对以上人员进行重复计算。

A.4 调整审核时间的因素

在确定审核时间时，认证机构应考虑根据以下因素增加审核时间，并形成文件化记录：

- a) 合规管理体系覆盖的合规风险/合规义务数量；
- b) 组织所在行业的法律法规背景；
- c) 不合规情况的类型以及对组织的影响；
- d) 场所数量；
- e) 合规管理体系认证范围包含的分包活动；
- f) 审核实施方法（如信息和通信技术及使用程度）；
- g) 语言或翻译需求；
- h) 合规管理体系的复杂程度。

A.5 审核时间计算

A.5.1 初次认证审核

初次审核时间不应少于根据表 1 确定的时间。

表 A.1 初次审核时间

有效人数	审核时间（1 阶段和 2 阶段）审核天	有效人数	审核时间（1 阶段和 2 阶段）审核天
1-5	2.5	626-875	6.5
6-10	3	876-1175	7
11-15	3	1176-1550	7.5
16-25	3	1551-2025	8
26-45	3	2026-2675	8.5
46-65	3.5	2676-3450	9
66-85	3.5	3451-4350	10
86-125	4	4351-5450	11
126-175	4.5	5451-6800	12
176-275	5	6801-8500	13
276-425	5.5	8501-10700	14
426-625	6	>10700	遵循上述递进规律

[来源：[4] IAF MD5：2023，附录 B，表 EMS 1 类别复杂程度 LIM]

A.5.2 监督审核

监督审核的时间应至少是表 1 要求审核时间的 1/3。由于组织、合规管理体系的范围和/或影响证书所涵盖的合规管理体系的其他因素的变化，审核时间可增加。

A.5.3 再认证审核

再认证审核所需的时间应至少是表 1 要求审核时间的 2/3。由于组织、合规管理体系的范围和/或影响证书所涵盖的合规管理体系的其他因素的变化，审核时间可增加。

附录 B
(规范性)

合规管理体系认证范围

B.1 认证业务范围分组

考虑合规管理体系适用的法律法规、过程技术特点以及认证机构审核组所需的能力，把 39 个大类划分为一系列技术组，并将技术组中对审核组水平有较高要求的类确定为关键类，如表 B.1 所示。

B.2 认证业务范围认可的见证评审要求

B.2.1 技术组中只有 1 个关键类，认可机构对关键类实施见证评审并通过后，方可结合文件评审或办公室评审的结果授予该组的所有类。

B.2.2 技术组中有多个关键类，认可机构至少实施 1 次见证评审，并按以下规则实施见证评审：

a) 同一技术组“和”的关系的所有关键类，认可机构在对其中某项关键类实施见证评审并通过后，可结合文审或办公室评审的结果授予认证机构该关键类和该组的其他非关键类认可资格，不包括该组未经见证评审的其他关键类。

b) 同一技术组“或”的关系的关键类，认可机构在对其中任一关键类实施见证评审并通过后，可结合文件评审或办公室评审的结果授予认证机构该技术组所有类的认可资格。

B.2.3 认可机构授予认证机构某技术组中一个或几个非关键类认可资格，最低要求是认证机构在该技术组接受 1 次见证评审并通过。

B.2.4 如果见证评审未通过，则该见证项目所在技术组的所有认可申请均不授予认可资格。

表 B.1 合规管理体系认证范围

序号	技术组	代码	内容	关键类代码
A	农业、生产和制造业	01	农业、林业和渔业	【03 食品、饮料和烟草或 13 药品或 23 其他未另分类的制造业（仅限医疗器械）】和【10 焦炭及精炼石油制品的制造或 11 核燃料或 12 化学品、化学制品及纤维】
		03	食品、饮料和烟草*	
		04	纺织品及纺织制品	
		05	皮革及皮革制品	
		06	木材及木制品	
		07	纸制品、纸浆及纸的制造	
		08	出版业	
		09	印刷业	
		10	焦炭及精炼石油制品的制造*	
		11	核燃料*	
		12	化学品、化学制品及纤维*	
		13	药品*	
		14	橡胶和塑料制品	
		15	非金属矿物制品	

		16	混凝土、水泥、石灰、石膏及其他	
		17	基础金属及金属制品	
		18	机械及设备	
		19	电和光学设备	
		20	造船业	
		21	航空航天	
		22	其他运输设备	
		23	其他未另分类的制造业	
B	资源	02	采矿业和采石业*	02 采矿业和采石业
C	服务业	24	回收业	【25 供电业或 26 供气业或 27 供水业】和【36 公共行政管理或 37 教育或健康和社会工作】
		29	批发和零售业：汽车、摩托、个人及家庭用品修理业	
		30	宾馆及餐馆	
		31	运输、仓储和通信业	
		35	其他服务	
		39	其他社会服务	
		25	供电业*	
		26	供气业*	
		27	供水业*	
		36	公共行政管理	
		37	教育	
		38	健康和社会工作	
D	建设业	28	建设业*	28 建设业
		34	工程服务	
E	金融业	32	金融中介*、房地产和租赁	32 仅限金融中介
F	信息服务业	33	信息技术*	33 信息技术

参 考 文 献

- [1] GB/T 19011 管理体系审核指南
 - [2] IAF MD 5 确定管理体系审核时间(QMS、 EMS、 OHSMS)
-