ICS 35.040; 03.120.20

CCS L 80; A 00



中华人民共和国国家标准

GB/T 25067－202X/ISO/IEC 27006-1:2024

|  |
| --- |
| 代替 GB/T 25067－2020 |

网络安全技术　信息安全管理体系审核和认证机构要求

Cybersecurity technology — Requirements for bodies providing audit and certification of information security management systems

（ISO/IEC 27006-1:2024, Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General, IDT）

|  |
| --- |
|  |
| （征求意见稿）（完成日期：2025年2月27日） |

XXXX - XX - XX发布

XXXX - XX - XX实施



1. 目 次

前 言 I

引 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 4

5 通用要求 4

5.1 法律与合同事宜 4

5.2 公正性的管理 4

5.3 责任和财力 4

6 结构要求 4

7 资源要求 4

7.1 人员能力 4

7.2 参与认证活动的人员 6

7.3 外部审核员和外部技术专家的使用 7

7.4 人员记录 7

7.5 外包 7

8 信息要求 8

8.1 公开信息 8

8.2 认证文件 8

8.3 认证的引用和标志的使用 8

8.4 保密 8

8.5 认证机构与其客户间的信息交换 8

9 过程要求 8

9.1 认证前的活动 9

9.2 策划审核 11

9.3 初次认证 12

9.4 实施审核 13

9.5 认证决定 13

9.6 保持认证 14

9.7 申诉 15

9.8 投诉 15

9.9 客户的记录 15

10 认证机构的管理体系要求 15

10.1 可选方式 15

10.2 方式A：通用的管理体系要求 15

10.3 方式B：与ISO 9001一致的管理体系要求 15

附录A（规范性）ISMS审核与认证所需的知识和技能 16

附录B（资料性）能力的其他考虑因素 17

附录C（规范性）审核时间 18

附录D（资料性）审核时间计算方法 23

附录E（资料性）对已实现的GB/T 22080—202X附录A中控制的审核指南 27

参考文献 36

1. 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。

本文件代替GB/T 25067—2020《信息技术 安全技术 信息安全管理体系审核和认证机构要求》。

与GB/T 25067—2020相比，主要技术变化如下：

——规范性引用文件中删除了ISO/IEC 27000（见第2章）；

——增加“控制”、“外部环境”、“信息安全”等术语（见第3章）；

——调整审核员的工作经历、培训经历和审核经历要求（见7.2.2.2）；

——调整技术专家的工作经历要求（见7.2.2.3）；

——修改远程审核的相关要求（见8.2.2、9.1.3.3、9.4.3.2、C.3.2）；

——新增认证文件中引用其他标准的要求（见8.2.3）；

——修改审核时间计算的相关要求（见C.2.1、C.3.4、C.6、C.7）；

——新增附录A，描述了认证职能与知识域的对应关系；

——依据GB/T 22080—202X附录A中的信息安全控制，更新附录E（2020版为附录D）；

——删除与GB/T 27021.1—2017重复的内容（见5.2、7.1.3、9.3.2.2、9.4等）。

本文件使用翻译法等同采用ISO/IEC 27006-1:2024《信息安全、网络安全和隐私保护　信息安全管理体系审核和认证机构要求 第1部分：通用》。

本文件做了最小限度的编辑性改动：

——为与我国网络安全国家标准协调一致，标准名称改为《网络安全技术　信息安全管理体系审核和认证机构要求》；

——因ISO Guide 73已废止，术语“3.10 风险”的注3和注4中删除对其的引用；

——7.1.2中增加了关于ISO/IEC TS 27006-2状态的脚注。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国合格评定国家认可中心、中国电子技术标准化研究院、中国网络安全审查认证和市场监管大数据中心等。

本文件主要起草人：付志高、张强、许玉娜、翟亚红、黄俊梅、陈艳、方洁、魏立茹、王秉政等。

本文件所代替标准的历次版本发布情况为:

——2010年首次发布为GB/T 25067—2010，2016年第一次修订，2020年第二次修订；

——本次为第三次修订。

1. 引 言

GB/T 27021.1对实施管理体系审核和认证的机构规定了要求并提供了指南。满足GB/T 27021.1的机构在依据GB/T 22080对组织的信息安全管理体系（英文缩写为“ISMS”）实施审核和认证活动时，有必要对GB/T 27021.1补充一些要求和指南。本文件提供了这些要求和指南。

本文件对提供ISMS审核和认证的机构规定了要求，这类机构被称为认证机构。本文件规定了ISMS认证机构的通用要求。认证机构遵守这些要求，确保其以有能力、一致和公正的方式实施ISMS认证，这将促进国内外对这些机构及其认证结果的承认与接受。

本文件正文与GB/T 27021.1—2017的结构保持一致。

在本文件中，使用了下列助动词：

—— “应”表示要求；

—— “宜”表示推荐；

—— “可”表示允许；

—— “能”表示能力，“可能”表示可能性。

1. 网络安全技术　信息安全管理体系审核和认证机构要求
	1. 范围

本文件在GB/T 27021.1—2017的基础上，对ISMS审核和认证机构规定了要求并提供了指南。

提供ISMS认证的机构从能力和可靠性方面证实其满足本文件中的要求。本文件中的指南提供了对这些要求的进一步解释。

注：本文件能作为认可、同行评审或其他审核过程的准则。

* 1. 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 22080—202X　网络安全技术　信息安全管理体系　要求（ISO/IEC 27001:2022,IDT）

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：要求（ISO/IEC 17021—1:2015,IDT）

* 1. 术语和定义

GB/T 27021.1—2017界定的以及下列术语和定义适用于本文件。

ISO和IEC维护用于标准化的术语数据库，地址如下：

——ISO在线浏览平台：http://www.iso.org/obp

——IEC电子百科：http://www.electropedia.org

认证文件 certification document

表明客户的ISMS符合指定的ISMS标准及ISMS所要求的任何补充性文件的一类文件。

注：本定义并没有限制统称为认证文件的文件数量。

控制　control

保持和/或改变风险（3.10）的措施。

注1：控制包括但不限于保持和/或改变风险（3.10）的任何过程、方针、设备、实践或其他条件和/或行动。

注2：控制并非总能取得预期的改变效果。

[来源：GB/T 22081—2024，3.1.8]

1.

外部环境　external context

组织（3.9）寻求实现其目标时所处的外部状况。

注：外部环境可能包括如下方面：

——文化、社会、政治、法律、监管、金融、技术、经济、自然和竞争环境，无论是国际的、国家的、地区的还是地方的；

——影响组织（3.9）目标的关键驱动力和趋势；

——与外部利益相关方的关系及其认知和价值观。

[来源：GB/T 29246—2023，3.22，有修改]

信息安全　information security

对信息的保密性、完整性和可用性的保全。

注：另外，还可能包括诸如真实性、可问责性、抗抵赖性和可靠性等其他性质。

[来源：GB/T 29246—2023，3.28]

信息安全事件　information security incident

单个或一系列不希望或意外的、极有可能危及业务运营并威胁信息安全（3.4）的信息安全事态。

[来源：GB/T 29246—2023，3.31]

信息系统　information system

应用、服务、信息技术资产或其他信息处理组件的组合。

[来源：GB/T 29246—2023，3.35]

内部环境　internal context

组织（3.9）寻求实现其目标时所处的内部状况。

注：内部环境可能包括如下方面：

——治理、组织结构、角色和职责；

——策略、目标及其实现战略；

——在资源和知识（如资本、时间、人员、过程、系统和技术）方面的能力；

——信息系统（3.6）、信息流和决策过程（正式的和非正式的）；

——与内部利益相关方的关系及其认知和价值观；

——组织（3.9）的文化；

——组织（3.9）采用的标准、指南和模型；

——合同关系的形式和范围。

[来源：GB/T 29246—2023，3.38，有修改]

管理体系 management system

组织(3.9)建立方针和目标以及实现这些目标的过程的相互关联或相互作用的一组要素。

注1：一个管理体系可以针对单一的领域或几个领域，如质量管理、财务管理或环境管理。

注2：管理体系要素规定了组织（3.9）的结构、岗位和职责、策划、运行、方针、惯例、规则、理念、目标，以及实现这些目标的过程。

注3：管理体系的范围可能包括整个组织（3.9），组织（3.9）中可被明确识别的职能或可被明确识别的部门，以及跨组织（3.9）的单一职能或多个职能。

注4：这是ISO/IEC导则 第1部分 ISO补充规定的附件SL中给出的ISO管理体系标准中的通用术语及核心定义之一，最初的定义已经通过修改注1至注3被改写。

[来源：GB/T 19000—2016，3.5.3]

组织　organization

为实现目标,由职责、权限和相互关系构成自身功能的一个人或一组人。

注：组织的概念包括但不限于个体经营者、公司、集团公司、商行、企事业单位、机关、合伙企业、慈善机构或院校，或者其部分或其组合，无论是否法人，是公共的还是私营的。

[来源：GB/T 29246—2023，3.50，有修改]

风险　risk

不确定性对目标的影响。

注1：影响是指对预期的偏离（正向的或反向的）。

注2：不确定性是对事态及其后果或可能性的相关信息、理解或知识缺乏的状态（即使是部分的）。

注3：风险常被表征为潜在的“事态”和“后果”，或者它们的组合。

注4：风险常被表示为事态（包括情况改变）的后果和其发生“可能性”的组合。

注5：在信息安全管理体系的语境下，信息安全风险能被表示为对信息安全目标的不确定性影响。

注6：信息安全风险与威胁利用信息资产或信息资产组的脆弱性对组织（3.9）造成伤害的潜力相关。

[来源：GB/T 29246—2023，3.61，有修改]

风险分析　risk analysis

理解风险（3.10）本质和确定风险级别的过程。

注1：风险分析为风险评价和风险处置（3.14）决策提供基础。

注2：风险分析包括风险估算。

[来源：GB/T 29246—2023，3.63]

风险评估　risk assessment

风险识别、风险分析（3.11）和风险评价的全过程。

[来源：GB/T 29246—2023，3.64]

风险管理　risk management

指导和控制组织（3.9）相关风险（3.10）的协调活动。

[来源：GB/T 29246—2023，3.69]

风险处置　risk treatment

改变风险（3.10）的过程。

注1：风险处置可能涉及如下方面：

——通过决定不启动或不继续进行引发风险的活动来规避风险；

——承担或增加风险以追求机会；

——消除风险源；

——改变可能性；

——改变后果；

——与另外一方或多方共担风险（包括合同和风险融资）；

——有根据地选择保留风险。

注2：处理负面后果的风险处置有时称为“风险缓解”、“风险消除”、“风险防范”和“风险降低”。

注3：风险处置可能产生新的风险（3.10）或改变现有风险。

[来源：GB/T 29246—2023，3.72]

规则　rule

组织所接受的，表明其期望要求做什么、允许什么和禁止什么的原则或指令。

[来源：GB/T 22081—2024，3.1.32，有修改]

* 1. 原则

GB/T 27021.1—2017第4章的原则适用。

* 1. 通用要求
		1. 法律与合同事宜

GB/T 27021.1—2017中5.1的要求适用。

* + 1. 公正性的管理

5.2.1 总则

GB/T 27021.1—2017中5.2的要求适用。并且，5.2.2的要求和指南适用。

5.2.2 利益冲突

认证机构可在认证审核和监督审核过程中开展增值活动，这不会被认为是咨询或存在潜在的利益冲突。例如，在审核过程中，当改进机会明显时识别改进机会但不推荐具体的解决方案。

认证机构不应代表客户对其申请认证的ISMS实施内部的信息安全评审。此外，认证机构应独立于提供ISMS内部审核的机构（包括任何个人）。

* + 1. 责任和财力

GB/T 27021.1—2017中5.3的要求适用。

* 1. 结构要求

GB/T 27021.1—2017第6章的要求适用。

* 1. 资源要求
		1. 人员能力

7.1.1 总则

GB/T 27021.1—2017中7.1的要求适用。并且，7.1.2和7.1.3的要求和指南适用。

7.1.2 通用的能力要求

认证机构应按照GB/T 27021.1—2017的表A.1为每项认证职能确定能力要求。认证机构应考虑GB/T 27021.1—2017以及本文件7.1.2和7.2.2所规定的、与认证机构所确定的ISMS技术领域相关的所有要求。附录B进一步给出了关于能力的指南。

认证机构应根据附录A定义各认证职能所需的知识和技能。

如果特定标准（如ISO/IEC TS 27006-2[[1]](#footnote-0)）中制定了包括能力要求在内的其他特定准则，则这些能力要求应得到应用。

7.1.3 能力准则的确定

7.1.3.1 实施ISMS审核的能力要求

7.1.3.1.1 总体要求

认证机构应有验证审核组成员能力的准则，以确保他们至少具备应用以下知识的技能：

1. 信息安全；
2. 与受审核的活动相关的技术；
3. 管理体系；
4. 审核原则；

注：ISO 19011给出了有关审核原则的详细信息。

1. ISMS的监视、测量、分析和评价。

除b)能在审核组成员之间共享外，以上a）～e）适用于审核组内的所有审核员。

审核组成员作为一个整体，应具备满足上述要求的技能。通过技能的应用情况能证实其是否具备这些技能。

审核组成员作为一个整体，应有能力将客户ISMS中信息安全事件的迹象追溯到ISMS的相应要素。

审核组中的审核员作为个体不必具有所有信息安全领域的全面经验，但审核组整体上应具备适宜能力，以覆盖所审核的ISMS范围。

7.1.3.1.2 信息安全管理术语、原则、实践和技术

ISMS审核组的每位审核员应具备以下知识：

1. ISMS特定的文件结构、层级和相互关系；
2. 信息安全风险评估和风险管理；
3. ISMS适用的过程。

审核组成员作为一个整体，应具备以下知识：

1. 信息安全管理相关的工具、方法、技术及其应用；
2. 当前可能与信息安全相关的或可能面临信息安全问题的技术。

7.1.3.1.3 信息安全管理体系标准和规范性文件

ISMS审核组的每位审核员应具备GB/T 22080—202X的知识。

审核组成员作为一个整体，应具备GB/T 22080—202X附录A中所有控制及其实现的知识。

7.1.3.1.4 业务管理实践

ISMS审核组的每位审核员应具备以下知识：

1. 行业的信息安全最佳实践和信息安全规程；
2. 信息安全策略和业务要求；
3. 通用业务管理的概念、实践，以及方针、目标和结果之间的相互关系；
4. 管理过程和相关术语。

注：这些过程也包括人力资源管理、内部沟通、外部沟通和其他的相关支持过程。

7.1.3.1.5 客户的业务领域

ISMS审核组的每位审核员应具备以下知识：

1. 特定的信息安全领域、地域和管辖范围的法律法规要求；

注：具备法律法规要求的知识，不意味着要有深厚的法律背景。

1. 与业务领域相关的信息安全风险；
2. 与客户业务领域相关的通用术语、过程和技术；
3. 相关业务领域的实践。

列项a）的知识可在审核组内共享。

7.1.3.1.6 客户的产品、过程和组织

审核组成员作为一个整体，应具备以下知识：

1. 组织类型、规模、治理、结构、职能（包括由外部提供的职能）和关系对建立和实现ISMS以及认证活动的影响；
2. 广义上的复杂运营；
3. 适用于产品或服务的法律法规要求。

7.1.3.2 实施申请评审的能力要求

7.1.3.2.1 客户的业务领域

实施申请评审以确定审核组所需能力、选择审核组成员并确定审核时间的人员，应具备与客户业务领域相关的通用术语、过程、技术和风险的知识。

7.1.3.2.2　 客户的产品、过程和组织

实施申请评审以确定审核组所需能力、选择审核组成员并确定审核时间的人员，应具备以下知识：客户的产品、过程、组织类型、规模、治理、结构、职能（包括由外部提供的职能）和关系对建立和实现ISMS以及认证活动的影响。

7.1.3.3 复核审核报告并做出认证决定的能力要求

7.1.3.3.1 总则

复核审核报告并做出认证决定的人员应具备知识，使其能够验证认证范围的适宜性、范围的变更以及变更对审核有效性的影响，特别是识别接口、依赖关系及其相应风险的持续有效性。

此外，复核审核报告并做出认证决定的人员应具备以下知识：

1. 通用的管理体系；
2. 审核过程和程序。

7.1.3.3.2 信息安全管理术语、原则、实践和技术

复核审核报告并做出认证决定的人员，应具备以下知识：

1. 7.1.3.1.2中的a）、b）、c）；
2. 与信息安全相关的法律法规要求。

7.1.3.3.3 客户的业务领域

复核审核报告并做出认证决定的人员，应具备与相关业务领域实践有关的通用术语和风险的知识。

7.1.3.3.4　客户的产品、过程和组织

复核审核报告并做出认证决定的人员，应具备客户的产品、过程、组织类型、规模、治理、结构、职能和关系的知识。

* + 1. 参与认证活动的人员

7.2.1 总则

GB/T 27021.1—2017中7.2的要求适用。并且，7.2.2的要求和指南适用。

7.2.2 证实审核员的知识和经验

7.2.2.1 总体考虑

认证机构应通过以下方式来证实每位审核员均具备知识和经验：

1. 获得承认的ISMS特定资格；
2. 适用时，注册为审核员；
3. 参加ISMS培训课程并获得相关的个人资格；
4. 最新的专业发展记录；
5. 由另一位ISMS审核员见证ISMS审核活动。

7.2.2.2　选择审核员

除7.1.3.1之外，审核员的选择过程应确保每位审核员：

1. 具备相当于大学水平的专业教育或培训；
2. 具备信息技术和信息安全方面的实际工作经历且该工作经历足以担任ISMS审核员；
3. 接受了充足的ISMS审核培训，且已证实具备依据GB/T 22080—202X实施ISMS审核的技能。作为实习审核员，在ISMS评价人员（见GB/T 27021.1—2017,9.2.2.1.4）的监督下，应至少实施1次ISMS初次认证审核（第一阶段和第二阶段）或再认证审核和1次监督审核。审核经历应不低于10个ISMS现场审核人日且应在近5年内获得。参与的审核活动应包括实施文件评审、审核风险评估及其实施和报告审核情况；
4. 保持与信息安全和审核相关的最新知识和技能。

注1：参加持续专业发展活动能证实技能的保持。

注2：认证机构要将上述要求和证据关联到其能力准则清单（见GB/T 27021.1—2017,7.1.2）。

7.2.2.3 选择技术专家

技术专家的选择过程应确保每位技术专家：

1. 具备相当于大学水平的专业教育或培训；
2. 具备信息技术和信息安全方面的实际工作经历且该工作经历足以担任技术专家；
3. 保持与信息安全相关的最新知识和技能。

注：参加持续专业发展活动能证实技能的保持。

7.2.2.4　选择领导审核组的审核员

除7.2.2.2外，领导审核组的审核员的选择准则应确保审核员已实质性参加了至少3次ISMS审核，且覆盖审核的所有阶段。参与的审核活动应包括识别初始范围、策划、实施文件评审、审核风险评估及其实施和正式地报告审核情况。

* + 1. 外部审核员和外部技术专家的使用

GB/T 27021.1—2017中7.3的要求适用。

* + 1. 人员记录

GB/T 27021.1—2017中7.4的要求适用。

* + 1. 外包

GB/T 27021.1—2017中7.5的要求适用。

* 1. 信息要求
		1. 公开信息

GB/T 27021.1—2017中8.1的要求适用。

* + 1. 认证文件

8.2.1 总则

GB/T 27021.1—2017中8.2的要求适用。并且，8.2.2和8.2.3的要求和指南适用。

8.2.2 ISMS认证文件

认证文件应由负责此项职责的人员签署。认证文件应包括适用性声明的版本。

注：如果适用性声明的变更没有改变认证范围中控制的覆盖范围，则不要求更新认证证书。

当组织不是在明确的物理位置实施其认证范围内的任何活动时，认证文件应说明组织所有的活动是远程实施的。

8.2.3 ISMS认证文件中引用其他标准

满足以下条件时，认证文件中可引用国家标准和国际标准：

1. 组织按照GB/T 22080—202X 6.1.3 c)的要求，将其所有的必要控制和参考控制源中的控制进行比较，以确定没有发生无意中遗漏必要控制的情况；
2. 组织按照GB/T 22080—202X 6.1.3 d)的要求，在适用性声明中给出删减参考控制的合理性说明。

参考控制标准能是基于GB/T 22080—202X的附录A或包含信息安全控制的标准。

认证文件应说明适用性声明中的控制集仅用于提及在ISMS中选择和删减控制的相关性，而不是用于合格评定。

* + 1. 认证的引用和标志的使用

GB/T 27021.1—2017中8.3的要求适用。

* + 1. 保密

8.4.1 总则

GB/T 27021.1—2017中8.4的要求适用。并且，8.4.2的要求和指南适用。

8.4.2 组织记录的获取

在认证审核之前，认证机构应要求客户报告是否存在因包含保密信息或敏感信息而导致不能提供给审核组的ISMS相关信息（例如，ISMS记录或关于控制的设计与有效性的信息）。认证机构应确定是否能在缺少这些信息的情况下对ISMS进行充分审核。如果认证机构的结论是若不审核已识别的保密信息或敏感信息就不能对ISMS进行充分地审核，那么认证机构则应告知客户只有在适当的访问安排获得许可后才能进行认证审核。

* + 1. 认证机构与其客户间的信息交换

GB/T 27021.1—2017中8.5的要求适用。

* 1. 过程要求
		1. 认证前的活动

9.1.1　申请

9.1.1.1 总则

GB/T 27021.1—2017中9.1的要求适用。并且，9.1.1.2的要求和指南适用。

9.1.1.2 对认证程序的考虑

认证机构的认证程序不应预先假定ISMS实施的特殊方式或文件和记录的特殊格式。认证程序应将重点放在确认客户的ISMS满足GB/T 22080—202X的要求和客户的策略与目标。

注：组织的必要控制可能是其自行设计的，也可能是从任何控制源中选取的。因此，即使组织的必要控制不是来自于GB/T 22080—202X附录A，组织也有可能获得GB/T 22080—202X的认证。

9.1.2　申请评审

GB/T 27021.1—2017中9.1.2的要求适用。

9.1.3　审核方案

9.1.3.1 总则

GB/T 27021.1—2017中9.1.3的要求适用。并且，9.1.3.2、9.1.3.3、9.1.3.4、9.1.3.5和9.1.3.6的要求和指南适用。

9.1.3.2 总体考虑

ISMS审核的审核方案应考虑组织所确定的信息安全控制。

注1：信息安全控制能来自于GB/T 22080—202X附录A，和/或其他适用的标准，和/或由组织自行设计。

注2：ISO/IEC 27007给出了有关审核的详细指南。

9.1.3.3 远程审核

实施远程审核活动的认证机构应规定程序，以确定在审核客户ISMS时应用远程审核活动（“远程审核”）的程度。程序应包括对在审核客户时使用远程审核的相关风险进行分析，风险分析时应考虑以下因素：

1. 认证机构和客户的可用基础设施；
2. 客户所在的行业；
3. 从初次审核到再认证审核的认证周期内的审核类型；
4. 认证机构和客户参与远程审核的人员的能力；
5. 以往已证实的、对客户实施远程审核的绩效；
6. 认证范围。

应在远程审核实施前进行分析。认证周期内使用远程审核的风险分析和理由应予以记录。

审核计划和审核报告应清楚地说明是否实施了远程审核活动。

如果风险评估发现对审核过程的有效性存在不可接受的风险，则不应使用远程审核。

风险评估应在认证周期内进行评审，以确保其持续适用性。

注：如果客户使用虚拟场所（即：组织利用网络环境完成工作或提供服务的地点，相关人员通过网络环境执行流程，不受其所在物理位置的影响。），远程审核技术是审核计划的一个相关部分。

9.1.3.4 初次审核的总体准备

认证机构应要求客户为调阅内部审核报告和信息安全独立评审报告做出所有的必要安排。

9.1.3.5 审核周期

只有有充分的证据证实覆盖认证范围的管理评审和ISMS内部审核的安排已经实施、是有效的并将得到保持，认证机构才能认证客户的ISMS。

9.1.3.6 ISMS认证范围

审核组应根据所有适用的认证要求，对在确定范围内的客户ISMS进行审核。认证机构应确认客户在其ISMS范围内满足GB/T 22080—202X中4.3的要求。

认证机构应确保：客户的信息安全风险评估和风险处置准确地体现其认证范围所界定的活动，并延伸到其活动的边界。认证机构应确认这在客户的ISMS范围和适用性声明中得到了体现。认证机构应验证认证范围有适用性声明。

认证机构应确保：与不完全包含在ISMS范围内的服务或活动的接口，已在寻求认证的ISMS中得到说明，并已纳入客户的信息安全风险评估中。与其他组织共享设施（例如，信息技术系统、数据库、通信系统或业务职能外包），是这类情形的示例。

9.1.4　确定审核时间

9.1.4.1 总则

GB/T 27021.1—2017中9.1.4的要求适用。并且，9.1.4.2的要求和指南适用。

9.1.4.2 审核时间

认证机构应使用附录C来确定审核时间。

注：附录D进一步提供了计算审核时间的指南和示例。

9.1.5　多场所的抽样

9.1.5.1 总则

GB/T 27021.1—2017中9.1.5的要求适用。并且，9.1.5.2的要求和指南适用。

9.1.5.2 多场所

9.1.5.2.1 当客户拥有满足以下a)至c)的多个场所时，认证机构可以考虑使用基于抽样的方法进行多场所认证审核：

1. 所有的场所在同一个ISMS下运行且该ISMS实行集中统一的管理、审核和管理评审；
2. 所有的场所都包含在客户的ISMS内部审核方案中；
3. 所有的场所都包含在客户的ISMS管理评审方案中。

9.1.5.2.2 认证机构在使用基于抽样的方法时应有程序来确保：

1. 在初次的合同评审时，最大程度地识别场所之间的差异，以便确定适当的抽样水平；
2. 结合以下因素，认证机构抽取具有代表性的场所：
3. 总部（适宜时）及各场所的内部审核结果；
4. 管理评审的结果；
5. 场所规模的差异；
6. 场所业务范围的差异；
7. 不同场所信息系统的复杂程度；
8. 工作实践的差异；
9. 所开展活动的差异；
10. 控制的设计与运行的差异；
11. 与关键信息系统或处理敏感信息的信息系统之间的潜在交互；
12. 任何不同的法律要求；
13. 地域因素和文化因素；
14. 场所的风险状况；
15. 特定场所发生的信息安全事件。
16. 从客户ISMS范围内的所有场所中选择具有代表性的样本，该选择应基于一个可体现上述b)中所列因素的判定，同时也考虑随机因素；
17. 在授予认证之前，认证机构审核了ISMS中每个具有重大风险的场所；
18. 根据上述要求设计审核方案，且审核方案要在三年内覆盖ISMS认证范围内的代表性样本；
19. 在单个场所发现不符合时，纠正措施程序的实施适用于证书所覆盖的所有场所。

审核应关注客户为确保单一的ISMS适用于所有场所并在运行层面实施统一管理所进行的活动。审核应关注上述所有事项。

9.1.6　多管理体系标准

9.1.6.1 总则

GB/T 27021.1—2017中9.1.6的要求适用。并且，9.1.6.2和9.1.6.3的要求和指南适用。

9.1.6.2 ISMS文件与其他管理体系文件的整合

只要能够清楚地识别ISMS以及ISMS与其他管理体系的适当接口，认证机构可以接受多个管理体系（例如，信息安全、质量、健康与安全、环境）文件组合在一起的文件。

9.1.6.3 管理体系结合审核

如果能证实审核满足了ISMS认证的所有要求，ISMS审核可以和其他管理体系审核相结合。在审核报告中，ISMS的所有重要要素应清晰地体现并易于识别。审核的质量不应因结合审核而受到负面影响。

* + 1. 策划审核

9.2.1 确定审核目的、范围和准则

9.2.1.1 总则

GB/T 27021.1—2017中9.2.1的要求适用。并且，9.2.1.2和9.2.1.3的要求和指南适用。

9.2.1.2 审核目的

审核目的应包括：

1. 确定管理体系的有效性；
2. 确保客户根据风险评估识别了必要控制；
3. 确定实现了客户所建立的信息安全目标。

9.2.1.3 审核准则

审核客户ISMS的准则应包括GB/T 22080—202X。

9.2.2　选择和指派审核组

9.2.2.1 总则

GB/T 27021.1—2017中9.2.2的要求适用。

9.2.3　审核计划

9.2.3.1 总则

GB/T 27021.1—2017中9.2.1的要求适用。并且，9.2.3.2和9.2.3.3的要求和指南适用。

9.2.3.2 总体考虑

ISMS审核计划应考虑所确定的信息安全控制。

注：良好的实践是认证机构与接受审核的组织商定一个能够最佳地证实组织全部范围的审核时间。适当时，考虑因素包括季度、月份、日期和班次。

9.2.3.3 远程审核技术

远程审核技术的目标宜是提高审核的有效性和效率，并支持审核过程的完整性。

审核计划应提及用于协助远程审核的工具。

* + 1. 初次认证

9.3.1 总则

GB/T 27021.1—2017中9.3的要求适用。并且，9.3.2的要求和指南适用。

9.3.2 初次认证审核

9.3.2.1 第一阶段

在本阶段，认证机构应获取有关ISMS设计的文件，包括GB/T 22080—202X所要求的文件。

在认证审核的第一阶段，客户应至少提供以下信息：

1. ISMS和其所覆盖活动的一般信息；
2. GB/T 22080—202X要求的ISMS文件的副本，以及需要时，其他相关文件。

认证机构应在客户的组织设置、风险评估与风险处置（包括所确定的控制）、信息安全方针和信息安全目标的背景下充分了解ISMS设计，特别是应充分了解客户的审核准备情况。所了解的信息应用于策划第二阶段。

第一阶段的结果应形成书面报告。在决定进行第二阶段之前，认证机构应评审第一阶段的审核报告，以便为第二阶段选择具备所需能力的审核组成员。如果第一阶段的审核组长具备能力且适宜时，可由其来实施该评审。

注：由未参与审核的认证机构人员来评审第一阶段报告、做出实施第二阶段的决定和确认实施第二阶段的审核组能力，能在一定程度上降低所涉及的风险。然而，其他降低风险的措施也能达到同样的目的。

认证机构应让客户知晓在第二阶段可以要求对其他类型的信息和记录进行详细检查。

9.3.2.2 第二阶段

认证机构应根据第一阶段审核报告中的审核发现，制定实施第二阶段的审核计划。除评价ISMS的有效实施外，第二阶段的目的还包括确认客户遵守自身的策略、目标和规程。

 为此，审核应重点关注客户的以下方面：

1. 最高管理层对信息安全目标的领导和承诺；
2. 信息安全风险评估，包括确保在重复实施风险评估时能产生一致的、有效的和可比较的结果；
3. 根据信息安全风险评估和风险处置过程来确定控制；
4. 信息安全绩效和ISMS有效性，包括根据信息安全目标对其实施评价；
5. 所确定的控制、适用性声明、信息安全风险评估结果、风险处置过程与信息安全方针和信息安全目标之间的对应关系；
6. 控制的实现（见附录E-审核控制的示例）：审核应考虑外部环境、内部环境、相关风险以及组织对信息安全过程和控制的监视、测量与分析过程，并确定待实现的控制是否已经实现且在整体上是有效的；
7. 方案、过程、规程、记录、内部审核和对ISMS有效性的评审，且这些都能追溯到最高管理层的决定、信息安全方针和信息安全目标。
	* 1. 实施审核

9.4.1 总则

GB/T 27021.1—2017中9.4的要求适用。并且，9.4.2和9.4.3的要求和指南适用。

9.4.2 ISMS审核的特定要素

认证机构的审核组应：

1. 要求客户证实在ISMS范围内，信息安全风险评估与ISMS运行是相关的和充分的；
2. 确定客户识别、检查和评价信息安全风险的规程及其实施结果是否与客户的方针、目标和指标相一致。

认证机构还应确定用于风险评估的规程是否合理并得到正确实施。

9.4.3 审核报告

9.4.3.1 审核报告应提供或引用以下信息：

1. 客户信息安全风险分析的审核情况说明；
2. 客户在实施GB/T 22080—202X 6.1.3 c)所要求的比较时，所使用的任何信息安全控制集。

9.4.3.2 审核报告应足够详细，以便于和支持认证决定。审核报告应包括：

1. 所采用的主要审核路线和所使用的审核方法（见 9.1.1.2)；
2. 所引用的适用性声明版本，以及适用时，与客户以往认证审核结果的任何有用的比较。

完成的问卷、检查清单、观察结果、日志或审核员笔记可以构成审核报告的组成部分。如果使用了这些方法，这些文件应作为支持认证决定的证据提供给认证机构。有关审核中所评价的样本的信息，应包含在审核报告或其他认证资料中。

如果使用了远程审核方法，报告应说明远程审核方法在审核中的使用程度及其实现审核目标的有效性。

当组织的活动不是在明确的物理位置实施的，而是其所有活动都是远程实施的时，审核报告应说明组织所有活动都是远程实施的。

报告应考虑客户所采用的内部组织和规程的充分性，以便对其ISMS建立信心。

报告应概述与客户ISMS及其信息安全控制的实现和有效性相关的主要观察结果，包括正面的和负面的。

* + 1. 认证决定

9.5.1 总则

GB/T 27021.1—2017中9.5的要求适用。并且，9.5.2的要求和指南适用。

9.5.2 认证决定

认证决定应基于审核报告中审核组对客户ISMS是否通过认证的推荐意见。

只有有充分的证据证实管理评审和ISMS内部审核的安排已实施、是有效的并将得到保持，才能向客户授予认证。

* + 1. 保持认证

9.6.1　总则

GB/T 27021.1—2017中9.6.1的要求适用。

9.6.2　监督活动

9.6.2.1 GB/T 27021.1—2017中9.6.2的要求适用。并且，9.6.2.2、9.6.2.3和9.6.2.4的要求和指南适用。

9.6.2.2 监督审核程序应是本文件中客户ISMS认证审核程序的子集。

监督的目的包括验证获证ISMS得到持续实施、考虑由客户运作实践变化所引起的管理体系变化的影响和确认与认证要求的持续符合。监督审核方案应至少包括：

1. ISMS维护要素，如信息安全风险评估与控制的维护、ISMS内部审核、管理评审和纠正措施；
2. GB/T 22080—202X要求的与外部各方的沟通，以及认证所需的其他文件。

9.6.2.3 认证机构的每一次监督审核应至少审核以下方面：

1. ISMS在实现客户信息安全方针的目标方面的有效性；
2. 相关信息安全法律法规合规性的定期评价和评审规程的运行情况；
3. 所确定的控制的变更，及其引起的适用性声明变更；
4. 审核方案中所述控制的实现和有效性。

9.6.2.4 认证机构应能调整监督方案，以反映与风险相关的信息安全问题及其对客户的影响，并说明监督方案的合理性。

 监督审核可以与其他管理体系审核相结合。报告应清晰地指出与每个管理体系相关的方面。

在监督审核过程中，认证机构应检查客户提交给认证机构的申诉和投诉记录。当发现任何不符合或不满足认证要求时，认证机构应检查客户是否调查了自身的ISMS和规程，并采取了适当的纠正措施。

特别是，监督报告应包括有关消除以往发现的不符合、适用性声明的版本和上次审核后发生的重大变更的信息。监督审核报告应至少覆盖9.6.2.2和9.6.2.3的全部要求。

9.6.3　再认证

9.6.3.1 总则

GB/T 27021.1—2017中9.6.3的要求适用。并且，9.6.3.2的要求和指南适用。

9.6.3.1 再认证审核

再认证审核程序应是本文件中客户ISMS认证审核程序的子集。

实施纠正措施的时限，应与不符合的严重程度和相关的信息安全风险相一致。

9.6.4　特殊审核

GB/T 27021.1—2017中9.6.4的要求适用。

9.6.5　暂停、撤销或缩小认证范围

GB/T 27021.1—2017中9.6.5的要求适用。

* + 1. 申诉

GB/T 27021.1—2017中9.7的要求适用。

* + 1. 投诉

9.8.1 总则

GB/T 27021.1—2017中9.8的要求适用。并且，9.8.2的要求和指南适用。

9.8.2 投诉

投诉意味着一个潜在事件，表明可能存在不符合。

* + 1. 客户的记录

GB/T 27021.1—2017中9.9的要求适用。

* 1. 认证机构的管理体系要求
		1. 可选方式

10.1.1 总则

GB/T 27021.1—2017中10.1的要求适用。并且，10.1.2的要求和指南适用。

10.1.2 实施ISMS

建议认证机构根据GB/T 22080—202X实施ISMS。

* + 1. 方式A：通用的管理体系要求

GB/T 27021.1—2017中10.2的要求适用。

* + 1. 方式B：与ISO 9001一致的管理体系要求

GB/T 27021.1—2017中10.3的要求适用。

1. 附录A
2. （规范性）
3. ISMS审核与认证所需的知识和技能

A.1 概述

除GB/T 27021.1—2017的要求外，表A.1规定了认证机构应为特定认证职能定义的知识和技能。“X”表示认证机构应确定相应知识和技能的准则和深度。表A.1中规定的知识和技能要求在第7章中有更详细的解释，并在表A.1的括号中给出了对应的条款号。

表A.1 ISMS审核与认证所需的知识

|  **知识** | **认证职能** |
| --- | --- |
| 实施申请评审，以确定审核组所需能力、选择审核组成员并确定审核时间 | 复核审核报告并做出认证决定 | 审核及领导审核组 |
| 信息安全管理术语、原则、实践和技术 |  | X（见7.1.3.3.2） | X（见7.1.3.1.2） |
| 信息安全管理体系标准/规范性文件 |  |  | X（见7.1.3.1.3） |
| 业务管理实践 |  |  | X（见7.1.3.1.4） |
| 客户的业务领域 | X（见7.1.3.2.1） | X（见7.1.3.3.3） | X（见7.1.3.1.5） |
| 客户的产品、过程和组织 | X（见7.1.3.2.2） | X（见7.1.3.3.4） | X（见7.1.3.1.6） |

注：附录B给出了能力的其他考虑因素。

1. 附录B
2. （资料性）
3. 能力的其他考虑因素

B.1 通用能力

审核员的知识和经验的证实方法有很多，例如，通过使用获得承认的资格来评价知识和经验。人员认证方案下的注册记录也能用来评价所需的知识和经验。宜确定审核组所需的能力水平，使其能体现组织的行业/技术领域和ISMS的复杂性。

B.2 特定知识和经验

B.2.1 与ISMS相关的典型知识

除7.1.3中的要求外，宜考虑以下方面。审核员宜具备下列审核和ISMS的知识：

——审核方案和审核策划；

——审核类型和审核方法；

——审核风险；

——信息安全过程分析；

——持续改进；

——信息安全内部审核。

审核员宜具备下列相关法规要求的知识：

——知识产权；

——组织记录的内容、保护和保留；

——数据保护与隐私；

——密码控制的法规；

——电子商务；

——电子签名和数字签名；

——工作场所监控；

——通信侦听和数据监视（例如，电子邮件）；

——计算机滥用；

——电子证据收集；

——渗透测试；

——国际和国家层面针对特定行业（例如，银行业）的要求。

特定标准（如ISO/IEC TS 27006-2）可能针对特定领域提出审核员宜具备的知识。

1. 附录C
2. （规范性）
3. 审核时间

C.1 概述

本附录进一步给出了与GB/T 27021.1—2017中9.1有关的要求。本附录为认证机构制定有关确定审核时间的程序提供了最低要求和指南，以便其在对涉及广泛的活动且具有不同规模和复杂度的ISMS范围实施认证时确定所需的时间。

认证机构应允许审核员有充足的时间来开展与初次审核、监督审核或再认证审核相关的所有活动。总审核时间的计算应包括报告审核情况所需的充足时间。

认证机构应针对每个客户和其获证ISMS，识别初次认证、监督审核和再认证审核所需的审核时间。在审核策划阶段，使用本附录能确保采用一致的方法来确定适当的审核时间。此外，可以根据审核过程（尤其是第一阶段）的发现（例如，ISMS范围的复杂度的不同评价结果，或范围中增加的场所）来调整审核时间。

本附录阐述了：

——审核时间计算所用的概念（见C.2）；

——确定初次审核不同阶段所需时间的程序的要求（见C.3）；

——监督审核和再认证审核的审核时间要求（见C.4、C.5）；

——与多场所审核相关的要求（见C.6）；

——扩大认证范围的审核时间要求（见C.7）。

附录D给出了审核时间计算的示例，对本附录的应用做出了说明。

对本附录的方法的基本假设是，确定审核时间的计算方案宜：

1. 仅考虑那些能客观评价的属性；
2. 足够简单，使认证机构能够应用它并获得有效、可比较和可重现的结果；
3. 足够精确，确保属性值的变化将导致审核时间发生可比较的变化。

审核时间的确定，是基于表C.1中的数值，并应考虑审核时间调整因素。

认证机构应定期评审其确定审核时间的方法，以验证其方法是否足以体现ISMS的复杂性。

C.2 概念

C.2.1 在组织控制下工作的人员的数量

在认证范围内的、处于组织控制下工作的、所有班次的人员的总数，是确定审核时间的起点。

注：在组织控制下工作的人员包括认证范围内要求按ISMS要求工作的所有人员(无论其是否为组织成员)。

在组织控制下工作的兼职人员，按照其工作小时数与在组织控制下工作的全职雇员的工作小时数的比例，计入在组织控制下工作的人员的数量。具体比例的确定，取决于兼职人员工作小时数与全职雇员工作小时数的比较。

当在认证范围内、处于组织控制下工作的人员中有很大比例从事某些相同的活动时，允许在使用表C.1计算审核时间之前减少人员数量。认证机构在确定如何减少认证范围内的人员数量时，应使用C.3.4给出的因素，并考虑活动对信息安全风险的影响。一致的程序是能重复应用的且在应用时能考虑不同组织的具体情况。程序应形成文件。

C.2.2 审核人日

表C.1中的审核时间，是用审核中花费的审核人日来表述。本附录的计算基础是每天（英文缩写为“d”）工作8小时。

C.2.3 临时场所

认证范围内的临时场所是认证文件所注明的场所之外的位置，其活动在认证范围内并在规定的时间周期内实施。此类场所的范围能从大型项目管理场所到较小的服务或安装场所。在确定对这些场所的访问需求及其抽样范围时，宜基于对在临时场所为实现信息安全目标而开展的活动的风险评价。所选择的场所样本宜考虑活动的规模与类型和实施中的项目的不同阶段，并体现组织的能力需求和服务变化的范围。对于一般的抽样，见9.1.5.2。

C.3 确定初次认证审核时间的程序

C.3.1 总则

认证机构应具有并遵循计算审核时间的文件化程序。

C.3.2 远程审核

如果使用了远程审核方法（例如，基于网络的交互式协作、网络会议、电话会议和/或电子验证组织的过程）来与组织接触，这些活动宜在审核计划（见9.2.3）中加以识别，可以考虑将其作为总的“现场审核时间”的一部分。

注：现场审核时间是指分配给单个场所的现场审核时间。对远程场所的电子化审核被视为远程审核，即使电子化审核是在组织的物理场所进行。

C.3.3 审核时间的计算

表C.1给出了初次审核天数平均值的起点（在本附录和附录D中，这个数值包括初次审核（第一阶段和第二阶段）的天数）。经验表明，对于一个覆盖了给定数量的、在组织控制下工作的人员的ISMS范围来说，这一数值是适当的。经验还表明，对于相似规模的ISMS范围，有些需要更多的审核时间。

表C.1提供了审核策划应使用的框架。该表基于在组织控制下工作的、所有班次的人员的总数来确定审核时间的起点。根据适用于待审核ISMS范围的重要因素来调整审核人日数：通过对每个因素赋予增减权重来修改基数。使用表C.1时应考虑审核时间调整因素和对偏离的限制(见C.3.5和C.3.6)。C.2解释了表C.1中所使用的术语，附录D提供了如何使用本附录计算方法的示例。

C.3.4 确定初始人数

认证机构应要求客户提供与大量人员从事某些相同活动有关的信息，包括:

——从事该活动的人数；

——活动或过程的类型。

因人员从事某些相同活动而减少作为审核时间计算基础的人数的示例包括:

——履行职责时对信息只有读取访问权限的人员；

——不能使用组织ISMS范围内的信息处理设施的人员；

——对组织ISMS范围内的信息处理设施具有明确且可证实的受限访问权限的人员；

——在有严格限制以防信息泄露的场所工作的人员，例如采取措施禁止个人物品和设备进入工作区域。

在减少从事相同活动的人数时，应基于工作任务相关的活动的风险。对实施每项相同活动的人数开平方根，然后将其四舍五入取整，得到用于计算审核时间的有效人数。该数值是允许减少到的最小值。

工作任务的性质、法规要求以及组织人员可访问信息的重要性能限制这种减少。

经由本过程确定的人数是表C.1中确定审核时间的起点。

注：该表的结构与IAF MD5相同。

表C.1 审核时间表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 在组织控制下工作的人员的数量 | 质量管理体系初次审核审核时间（审核人日，d） | 环境管理体系初次审核审核时间（审核人日，d） | 信息安全管理体系初次审核审核时间（审核人日，d） | 增加或减少的因素 | 总审核时间 |
| 1～10 | 1.5～2 | 2.5～3 | 5 | 见C.3.5 |  |
| 11～15 | 2.5 | 3.5 | 6 | 见C.3.5 |  |
| 16～25 | 3 | 4.5 | 7 | 见C.3.5 |  |
| 26～45 | 4 | 5.5 | 8.5 | 见C.3.5 |  |
| 46～65 | 5 | 6 | 10 | 见C.3.5 |  |
| 66～85 | 6 | 7 | 11 | 见C.3.5 |  |
| 86～125 | 7 | 8 | 12 | 见C.3.5 |  |
| 126～175 | 8 | 9 | 13 | 见C.3.5 |  |
| 176～275 | 9 | 10 | 14 | 见C.3.5 |  |
| 276～425 | 10 | 11 | 15 | 见C.3.5 |  |
| 426～625 | 11 | 12 | 16.5 | 见C.3.5 |  |
| 626～875 | 12 | 13 | 17.5 | 见C.3.5 |  |
| 876～1175 | 13 | 15 | 18.5 | 见C.3.5 |  |
| 1176～1550 | 14 | 16 | 19.5 | 见C.3.5 |  |
| 1551～2025 | 15 | 17 | 21 | 见C.3.5 |  |
| 2026～2675 | 16 | 18 | 22 | 见C.3.5 |  |
| 2676～3450 | 17 | 19 | 23 | 见C.3.5 |  |
| 3451～4350 | 18 | 20 | 24 | 见C.3.5 |  |
| 4351～5450 | 19 | 21 | 25 | 见C.3.5 |  |
| 5451～6800 | 20 | 23 | 26 | 见C.3.5 |  |
| 6801～8500 | 21 | 25 | 27 | 见C.3.5 |  |
| 8501～10700 | 22 | 27 | 28 | 见C.3.5 |  |
| ＞ 10700 | 沿用以上规律 | 沿用以上规律 | 沿用以上规律 | 见C.3.5 |  |

C.3.5　审核时间调整因素

不应孤立地使用表C.1。所安排的时间还应考虑以下与ISMS复杂程度和ISMS审核工作量相关的因素：

1. ISMS的复杂程度（例如，信息的关键程度、ISMS的风险状况）；
2. ISMS范围内所开展业务的类型；
3. 以往已证实的ISMS绩效；
4. 在ISMS各部分的实施过程中，所应用的技术的水平和多样性（例如，不同IT平台的数量、隔离网络的数量）；
5. ISMS范围内所使用的外包和第三方安排的程度；
6. 信息系统开发程度；
7. 场所数量和灾难恢复场所数量；
8. 第一阶段之后，认证机构将考虑控制的数量和复杂性；
9. 对于监督或再认证审核：GB/T 27021.1-2017 8.5.3中所述的ISMS相关变更的数量和程度。

附录D提供了在计算审核时间时如何考虑这些不同因素的示例。

需要增加审核时间的因素，例如：

* 1. 复杂的过程和后勤，ISMS范围内涉及不止一处建筑物或地点；
	2. 员工的语言不止一种（需要口译员或审核员个人无法独立工作），或提供的文件使用了多种语言；
	3. 为确认管理体系认证范围内永久场所的活动，需要访问临时场所的活动；（见下一列表之后的段落）
	4. 适用于ISMS的标准和法规数量很多。

允许减少审核时间的因素，例如：

* 1. 没有风险或者低风险的过程；
	2. 过程只涉及单一的常规活动（例如，只有服务）；
	3. 对组织已经有所了解（例如，如果组织获得了同一认证机构授予的另一个标准的认证）；
	4. 客户的认证准备情况较好（例如，已经获得了另一个第三方认证方案的认证或承认）；
	5. 高度成熟的管理体系。

当客户或获证组织在临时场所提供其产品或服务时，将对这类场所的评价纳入到认证审核和监督方案中是十分重要的。

能根据以上因素来调整审核时间。审核时间增加因素和减少因素对审核时间的影响可能会相互抵消。在任何情况下，对审核时间表中的时间的调整，应保持足够的证据和记录来证实其变化的合理性。

C.3.6　对审核时间偏离的限制

为了确保能够实施有效的审核并确保可靠和可比较的结果，对表C.1中审核时间的减少，不应超过30%。

应确定和记录偏离审核时间表的适当理由。

C.3.7　现场审核时间

策划和编制报告合计所用的时间，通常不宜使总的现场“审核时间”（物理/远程）减少到根据C.3.3、C.3.4和C.3.5所计算出的时间的70%以下。当策划和/或编制报告需要增加时间时，这不应成为减少现场审核时间的理由。审核员的旅途时间未包含在本附录的审核时间计算内，应在表C.1的审核时间的基础上另行增加。

注1：70%是基于ISMS审核经验所得出的系数。

注2：术语“物理/远程”是指“现场”审核(对客户的物理场所或电子化场所)能以物理或远程的方式进行(见9.2.3和C.3.2)。关于“现场”审核，请参见GB/T 27021.1-2017, 9.4.1。

C.4　监督审核的审核时间

在初次认证审核周期，对一个组织的监督时间宜与初次审核时间成比例，每年用于监督审核的时间总量大约是初次审核时间的1/3。宜不定期地评审所策划的监督审核时间，以考虑可能影响审核时间的变更。为审核ISMS的变更（例如，审核新的或发生变更的信息安全控制、过程和服务），应增加监督审核时间。

C.5　再认证审核的审核时间

用于再认证审核的总时间，应取决于9.4.3和GB/T 27021.1-2017中9.6.3所述的、任何以往审核的结果。再认证审核所需的时间，宜与同一组织的初次认证审核所用的时间成比例，宜至少是同一组织初次认证审核时间的2/3。

C.6　多场所的审核时间

通常，总的现场审核时间应考虑在组织控制下工作的人员总数，而不考虑人员所在的位置。

或者，基于形成文件的合理理由，允许对每个场所单独计算的审核时间进行汇总，只要总审核时间大于按照本条第一段的计算结果。适用时，若某些审核内容与总部办公室或本地场所无关，则可以减少审核时间。认证机构应记录这类减少的理由。

根据C.3.3和C.3.4以及本条规定的程序，为认证范围计算出总的现场审核人日。应根据场所与管理体系的相关性、场所所开展的活动和所识别的风险，将总的现场审核人日分配到不同的场所。认证机构应记录分配的理由。

任何审核时间的减少，应在现场审核时间与总审核时间的比较之前进行。

C.7 扩大认证范围的审核时间

扩大ISMS范围所需的审核时间应考虑以下因素:

* 1. 扩大的类型；
	2. 当前的认证活动；
	3. 开展活动的地点的数量；
	4. 与活动相关的信息安全风险；
	5. 与所扩范围相关的控制的数量；
	6. 所扩范围内、在组织控制下工作的人数；
	7. 在审核客户将所扩范围整合到ISMS时，所需的审核时间。

认证机构应制定程序，为扩大范围的审核时间计算提供一致的方法。

对于所扩范围的初次审核，审核时间应根据在当前认证范围内增加的人员和场地的数量，使用C.3.3、C.3.4和C.3.5所述的方法来计算。

扩大ISMS范围所需的审核时间，应增加到审核客户获证ISMS所需的审核时间中。当扩大范围审核是结合监督审核或再认证审核进行时，应至少增加为0.5天(审核人日)；当扩大范围审核是单独进行时，相应的时间应至少为1.0天(审核人日)。

1. 附录D
2. （资料性）
3. 审核时间计算方法

D.1　总则

本附录进一步提供了推导审核时间计算公式的指南。D.2给出了对因数进行分级的示例，它能用作审核时间计算的基础。D.3提供了一个审核时间计算的示例。

注：本附录涉及的是在对从事某些相同活动的人员数量进行减少（见C.3.4）之后的活动。

D.2　审核时间计算因数的分级

表D.1给出了主要的审核时间计算因数[见C.3.5 中a）-i）]的分级示例。认证机构能使用该分级来制定一个符合9.1.4.2的审核时间计算方案。

表D.1 审核时间计算因数的分级

|  |  |
| --- | --- |
| 因数（见C.3.5） | 对审核工作量的影响 |
| 减少工作量 | 正常工作量 | 增加工作量 |
| 1. ISMS的复杂性：

——信息安全要求[保密性、完整性和可用性（CIA）]——关键资产的数量——过程和服务的数量 | ——只有少量的敏感信息或保密信息，可用性要求低；——很少的关键资产（根据CIA）；——只有一个关键业务过程，该过程的接口和涉及的业务单元很少。 | ——较高的可用性要求或有若干敏感信息或保密信息；——若干关键资产；——2-3个简单的业务过程，这些过程的接口和涉及的业务单元很少。 | ——比较多的保密信息或敏感信息（例如，健康、个人可识别信息、保险、银行），或可用性要求高；——很多关键资产；——超过2个复杂的过程，这些过程的接口和涉及的业务单元很多。 |
| b）ISMS范围内所开展业务的类型 | ——低风险的业务，没有法规要求。 | ——法规要求高。 | ——高风险的业务，有（仅有）有限的法规要求。 |
| c）以往已证实的ISMS绩效 | ——最近刚获得认证；——没有获得认证，但ISMS已充分实施了多个审核与改进周期，包括文件化的内部审核、管理评审和有效的持续改进体系。 | ——最近刚通过监督审核；——没有获得认证，但部分实施了ISMS：获得并实施了一些管理体系工具，一些持续改进过程是适宜的但未全部文件化。 | ——未获得认证且最近未接受审核；——ISMS是新的且没有完全建立（例如，缺少管理体系的特定控制机制，不成熟的持续改进过程，特别的流程执行）。 |
| d）在ISMS各部分的实施过程中，所应用的技术的水平和多样性（例如，不同IT平台的数量、隔离网络的数量） | ——高标准化、低多样性的环境（例如，很少的IT平台、服务器、操作系统、数据库、网络等）。 | ——标准化且多样性的IT平台、服务器、操作系统、数据库和网络。 | ——高多样性或复杂的IT环境（例如，很多不同的网段、服务器或数据库的类型、关键应用的数量）。 |

表D.1（续）

|  |  |
| --- | --- |
| 因数（见C.3.5） | 对工作量的影响 |
| 减少工作量 | 正常工作量 | 增加工作量 |
| e）ISMS范围内所使用的外包和第三方安排的程度 | ——没有外包且对供应商的依赖较小；——对外包协议进行了明确的规定、良好的管理和监视；——外包方获得了ISMS认证；——可获得相关的独立保证报告。 | ——多个管理不充分的外包协议。 | ——高度依赖外包或供应商，它们对重要业务活动有很大影响；——对外部的数量或程度不清楚；——多个未得到管理的外包协议。 |
| f）信息系统开发程度 | ——没有内部的系统开发；——使用标准化的软件平台。 | ——使用标准化的、具有复杂配置/参数化的平台；——（高度）定制软件；——若干开发活动（内部的或外包的）。 | ——大量的内部软件开发活动，有若干正在实施的、针对重大业务目的的项目。 |
| g）场所数量和灾难恢复场所数量 | ——较低的可用性要求，且没有或有一个可选的灾难恢复场所。 | ——中等或高的可用性要求，且没有或有一个可选的灾难恢复场所。 | ——高可用性要求，例如，7×24服务； ——若干个可选的灾难恢复场所；——若干个数据中心。 |
| h)控制的数量和复杂性 | ——控制数量比平常的少，不包括一些常见的控制域。例如，没有系统开发控制或没有物理控制。 | ——控制数量和复杂性是平常的。 | ——数量比平常的多且详细和复杂的控制，例如，许多与网络协议或密码相关的控制。 |
| i）对于监督或再认证审核：GB/T 27021.1-2017 8.5.3中所述的ISMS相关变更的数量和程度。 | ——自上次再认证审核后未发生变化。 | ——ISMS范围或适用性声明有微小的变化，例如，一些策略、文件发生变化；——以上因素有微小变化。 | ——ISMS范围或适用性声明有重大变化，例如，新的过程、新的业务单元、区域、风险评估管理方法、策略、文件、风险处置；——以上因素有重大变化。 |

D.3　审核时间计算的示例

以下示例阐述了认证机构如何使用C.3中的因数来计算审核时间。本示例中的审核时间计算，是按照以下方法进行的：

第一步：确定与业务和组织相关的（非IT）因数：识别表D.2中每个分级的适宜分值，并对结果求和；

第二步：确定与IT环境相关的因数：识别表D.3中每个分级的适宜分值，并对结果求和；

第三步：基于以上第一步和第二步的结果，通过选择表D.4中的适宜条目，识别这些因数对审核时间的影响；

第四步：最终计算：将由审核时间表（表C.1）所确定审核人日数乘以第三步中得出的系数。当使用多场所抽样时，要将实施多场所抽样计划所需的工作量增加所计算出的审核人日。

这个结果是最终的审核人日数。

表D.2 与业务和组织（非IT）相关的因数

|  |  |
| --- | --- |
| 类别 | 分值 |
| 业务类型和法规要求 | 1. 组织所处的是一个非关键业务领域，且不受管制的领域；
2. 组织的客户处于关键业务领域；
3. 组织处于关键业务领域。
 |
| 过程与任务 | 1. 标准过程，标准任务，很少的产品或服务；
2. 标准的但不重复的过程，涉及大量的产品或服务；
3. 复杂的过程，大量的产品和服务，许多业务单元包含在认证范围内（ISMS有复杂性高的过程，或相对较多的独特活动）。
 |
| 管理体系的建立水平 | 1. 已经很好地建立了ISMS，和（或）存在其他管理体系；
2. 其他管理体系的要素，有些已经实施，有些没有实施；
3. 根本没有实施其他管理体系，ISMS是新的且尚未建立。
 |

注：关键业务领域是能影响关键公共服务的领域，这些公共服务将引起健康、安全、经济、信誉和政府履职能力的风险，从而可能对国家造成非常重大的负面影响。

表D.3 与IT环境相关的因数

|  |  |
| --- | --- |
| 类别 | 分值 |
| IT基础设施的复杂程度 | 1. 很少的或高度标准化的IT平台、服务器、操作系统、数据库、网络等；
2. 多个不同的IT平台，服务器、操作系统、数据库、网络；
3. 很多不同的IT平台、服务器、操作系统、数据库、网络。
 |
| 对外包和供应商（包括云服务）的依赖程度 | 1. 很少或不依赖外包或供应商；
2. 有些依赖外包或供应商，这些外包或供应商与某些重要业务活动相关，但不是与所有的重要业务活动相关；
3. 高度依赖外包或供应商，外包或供应商对重要业务活动有着很大影响。
 |
| 信息系统开发 | 1. 没有或非常有限的内部系统/应用开发；
2. 有一些服务于某些重要业务目的的、内部的或外包的系统/应用开发；
3. 有大量服务于重要业务目的的、内部的或外包的系统/应用开发。
 |

表D.4 因数对审核时间的影响

|  |  |  |  |
| --- | --- | --- | --- |
| IT复杂性业务复杂性 | 低（3～4） | 中（5～6） | 高（7～9） |
| 高（7～9） | +5%～+20% | +10%～+50% | +20%～+100% |
| 中（5～6） | -5%～−10% | 0% | +10%～+50% |
| 低（3～4） | -10%～−30% | -5%～−10% | +5%～+20% |

示例1：

受审核的组织有700人，因此根据表C.1，其初次认证审核需要17.5人天。该组织不属于关键业务领域，从事高度标准化和重复性的任务且刚建立ISMS。根据表D.2，得出与业务和组织相关的因数为1+1+3=5。该组织具有非常少的IT平台和数据库，但大量地使用外包。该组织没有内部的或外包的开发活动。根据表D.3，得出与IT环境相关的因数为1+3+1=5。利用表D.4，可以得出该审核时间无需调整。

示例2：

还是示例1中的这个组织，但其已有多个管理体系且已较好地建立了ISMS。根据表D.2，与业务和组织相关的因数将变为：1+1+1=3。根据表D.4，将得出需要减少5%∽10%的审核时间，即：审核时间将减少1到1.5人天，变为16到16.5人天。

1. 附录E
2. （资料性）
3. 对已实现的GB/T 22080—202X附录A中控制的审核指南

E.1 目的

根据9.3.2.2 f)的要求，在初次认证审核的第二阶段以及监督或再认证活动中，应根据适用性声明审核客户ISMS所确定的必要控制的实现情况。审核目的是确定控制是否已实现且有效，是否满足其所述的信息安全目标。

通常，只有在审核员访问组织之后，认证机构才能对组织的必要控制有所了解。即使组织在描述其必要控制时使用与GB/T 22080—202X附录A相同的文本，认证机构也无法了解这些信息安全控制之间的关系，或者信息安全控制与组织过程之间的关系。因此，最初的审核可能局限于各单项控制，而后续的审核能在了解部署控制的组织过程和风险处置计划的情况下，采用更有效的方法来审核控制。

然而，认证机构要知晓：组织需要将其必要控制与GB/T 22080—202X附录A中的控制进行比较，因此组织的必要控制与GB/T 22080—202X附录A中的控制之间存在对应关系。基于这种关系，认证机构在根据客户确定的必要控制制定审核计划时，表E.1中的指南能提供支持。

E.2　如何使用表E.1

E.2.1　总则

表E.1提供了必要控制的审核指南示例。表E.1使用的是GB/T 22080—202X附件A中的控制，然而，在收集证实控制有效性的审核证据时，审核员宜使用GB/T 22080—202X附件A中的控制与组织必要控制之间的对应关系来理解表E.1中的指南。

注：表E.1没有为GB/T 22080—202X附录A之外的控制提供审核指南。

大多数控制是具有组织性的且能够被证实，例如，通过面谈或观察，审核客户关于控制、过程或规程的文件。

多数控制是基于客户制定的规则。这些规则能是特定主题策略、过程或规程中的要求，或传达给工作人员的其他类型的规则。表E.1使用通用术语“规则”来表示由客户管理层设定的要求或期望。

多数控制能通过抽样来验证，即审核控制活动结果的样本。

E.2.2　“系统测试”列

GB/T 22080—202X附录A中的多数控制是作为技术控制，例如，通过特定的系统设置、配置或技术功能。通常是通过系统设置或通过使用专门的审计或报告工具来收集技术控制的实施证据。系统测试是指对信息系统的直接审核：审核员能审核系统设置和配置，或评价测试工具的测试结果。如果审核员了解客户使用的测试工具，那么这些工具也能用来支持审核，或者审核员能审核由客户实施的评价的结果。

表E.1中的“系统测试”栏提供了技术控制的审核指南：

——“空白”：是指系统测试在ISMS审核中通常不适用或没有必要；

—— “可能的”：是指系统测试对于评价控制的实现来说是可能的，但在ISMS审核中不一定是必需的；

——“推荐的”：是指在ISMS审核中，系统测试通常是必需的。

E.2.3　“目视检验”列

能通过现场“目视检验”来审核GB/T 22080—202X附件A中的其他控制的实现情况和有效性。通过审核相应的书面文件或访谈来评价控制的有效性是不够充分的，审核员宜在实现控制的场所对控制进行验证。

注：现场的目视检验也能使用远程检验技术来实现，例如，现场人员向审核员提供实时视频。

表E.1中的“目视检验”栏提供了对控制的实物证据的审核指南。

——“空白”：是指目视检验在ISMS审核中通常不适用或没有必要；

——“可能的”：是指目视检验对于评价控制的实现来说是可能的，但在ISMS审核中不一定是必需的；

——“推荐的”：是指在ISMS审核中，目视检验通常是必需的。

E.2.4 控制设计与实现的可能证据

“控制设计与实现的可能证据”一列为审核员评估是否符合GB/T 22080—202X, 8.3（实施风险处置计划的要求，从而实现必要的控制）提供了证据方面的指南。本列中的各项内容不是要求，也不构成一个完备的列表。因为这些内容是来自GB/T 22080—202X附录A中的控制文本，所以它们不一定适用于组织相应的必要控制。在这种情况下，宜使用其他形式的证据。组织的适用性声明和相关的ISMS文件宜作为组织必要控制的规范。组织的适用性声明宜包含必要的控制，选择这些控制的合理性说明、这些控制是否已实现，以及删减GB/T 22080-202X附录A中任何控制的合理性说明。

表E.1 控制的评价

|  |  |  |  |
| --- | --- | --- | --- |
| GB/T 22080—202X附录A中的控制[[2]](#footnote-1) | 系统测试 | 目视检验 | 控制设计与实施的可能证据 |
| 5 组织控制 |   |   |   |
| 5.1 信息安全策略 |   |   | ——信息安全方针——组织认为必要的信息安全特定主题策略——传达给有关工作人员和相关方的策略 |
| 5.2 信息安全角色和责任 |   |   | ——为信息安全的实施、运行和管理分配角色和职责 |
| 5.3 职责分离 |   |   | ——识别相互冲突的职责或责任范围，以及相应的分离规则 |
| 5.4 管理责任 |   |   | ——对信息安全目标、策略、规程等的管理声明和支持——提及工作人员的个人信息安全责任 |
| 5.5 与职能机构的联系 |   |   | ——与有关职能机构的、明确的联系点——事故报告规则——来往于相关职能部门的信息 |
| 5.6 与特定相关方的联系 |   |   | ——特定相关方或其他论坛和协会的成员资格和明确的联络点[例如，计算机应急响应小组（CERTs）、网络安全机构]——关于能在这类组织内交流的信息的规则——来往于这类组织的信息 |
| 5.7 威胁情报 |   |   | ——收集相关威胁情报的方法——分析与组织有关的威胁情报，并将其分享给适宜的相关方 |
| 5.8 项目管理中的信息安全 |   |   | ——在贯穿项目生存周期的项目管理中建立信息安全，例如，在需求定义、测试中——对于所抽取的项目，所识别的信息安全风险和相应的风险处置 |
| 5.9 信息及其他相关资产的清单 | 可能的 |   | ——由ISMS维护的信息和其他相关资产的清单——维护资产清单中资产的所有权——资产所有者责任的规则，如分级 |
| 5.10 信息及其他相关资产的可接受使用 |   |   | ——信息和其他相关资产可接受使用的文件化规则——处理信息和其他相关资产的规程 |
| 5.11 资产归还 |   |   | ——组织资产的归还规则，如发生变更的或终止的雇佣、合同或协议时的检查清单——文件化资产归还记录的样本 |
| 5.12 信息分级 |   |   | ——信息分级规则和方案，例如，在特定主题策略中——不同来源的、宜分级的信息样本 |
| 5.13 信息标记 |   | 可能的 | ——信息和其他相关资产的标记规则——特定类型信息和其他相关资产的标记规程 |
| 5.14 信息传输 | 可能的 |   | ——信息传输规则，例如在特定主题策略中——在ISMS所识别的信息传输用例以及相应的规则、规程或协议，包括物理传输、电子传输或口头传递——所实施的信息传输规程或协议的样本 |
| 5.15 访问控制 | 可能的 |   | ——控制对信息和其他相关资产进行物理和逻辑访问的规则，例如，在访问控制的特定主题策略中——对信息和其他资产的高风险物理或逻辑访问的访问权限摘录（样本），以检查是否符合上述规则 |
| 5.16 身份管理 |   |   | ——对分配给个人或非人实体的身份进行全生存周期管理的规程 |
| 5.17 鉴别信息 | 推荐的 |   | ——描述分配和管理鉴别信息的过程——正确处理鉴别所用信息的用户操作指南——使用口令时，口令管理系统的安全设置（例如，长度、复杂度、轮换) |
| 5.18 访问权限 | 推荐的 |   | ——访问控制规则，例如，在访问控制（物理和逻辑）的特定主题策略中——分配、更新或撤销访问权限的过程描述——定期评审访问权限的规则和规程——分配给某一身份的访问权限——已有的访问权限评审结果 |
| 5.19 供应商关系中的信息安全 |   |   | ——管理供应商关系中的信息安全风险的规则，例如，在使用供应商产品和服务的特定主题策略中——在供应商关系的整个生存周期中管理信息安全的过程或规程——供应商评价结果[例如，信息通信技术（ICT）基础设施组件、服务]——对是否符合已建立的信息安全要求的监视结果（例如，对某一供应商关系） |
| 5.20 在供应商协议中强调信息安全 |   |   | ——与供应商关系类型相关的外部协议的登记册——包含相关信息安全要求和服务级别协议的供应商协议样本 |
| 5.21 管理信息通信技术供应链中的信息安全 |   |   | ——信息通信技术（ICT）产品或服务获取中的信息安全处理规则——信息通信技术供应链中信息安全风险管理实践——风险分析结果，即针对特定信息通信技术（ICT）供应链样本的、缓解风险的控制 |
| 5.22 供应商服务的监视、评审和变更管理 |   |   | ——供应商信息安全实践和服务交付的变更管理过程——定期监视、评审、评价供应商信息安全实践的计划（例如，通过服务报告、供应商审核）——监视和评审活动的结果，包括行动计划 |
| 5.23 云服务使用的信息安全 |   |   | ——管理云服务中的信息安全风险的规则，例如，在云服务使用的特定主题策略中——组织在用的云服务列表——管理与使用云服务相关的信息安全风险的过程——当云服务协议未包括组织的保密性、完整性、可用性和信息处理要求时，为保护组织的数据和服务可用性所做出的具体规定 |
| 5.24 信息安全事件管理规划和准备 |   |   | ——处理信息安全事件的过程、计划、角色和责任——信息安全事件的报告规程和此类报告的示例 |
| 5.25 信息安全事态的评估和决策 |   |   | ——信息安全事态的评估准则——信息安全事态的分类和优先级方案 |
| 5.26 信息安全事件的响应 |   |   | ——信息安全事件响应规程——事件记录和相应的事件响应 |
| 5.27 从信息安全事件中学习 |   |   | ——信息安全事件的记录，包括类型、数量和成本——从信息安全事件分析中得的经验教训，例如，加强事件管理计划、完善控制和提高意识 |
| 5.28 证据收集 |   |   | ——处理与信息安全事件有关的证据的规程，例如，识别、收集、获取和保存证据的规程 |
| 5.29 中断期间的信息安全 |   |   | ——在中断期间维持适当信息安全级别的计划——将信息安全要求纳入业务连续性管理规划和过程 |
| 5.30 业务连续性的信息通信技术就绪 |   |   | ——从业务影响分析中得到信息通信技术（ICT）连续性要求——信息通信技术连续性计划——定期的信息通信技术连续性测试的测试结果 |
| 5.31 法律、法规、规章和合同要求 |   |   | ——组织在其开展业务或使用了其产品和服务（这些产品和服务可能影响组织信息安全）的相关国家的列表——所识别的外部要求，包括与信息安全相关的法律、法规或合同要求，特别是与任何形式使用加密技术有关的要求 |
| 5.32 知识产权 |   |   | ——管理知识产权的规则，例如在特定主题策略策中——文件版权、设计权、商标、专利和源代码许可证的处理规程以及相应的清单 |
| 5.33 记录的保护 | 推荐的 |   | ——与适用的法律、法规和合同要求相关的记录管理规则，例如在特定主题策略中——关于存储、处理、保管链、保留和处置记录的规程——数据存储系统的配置能满足记录管理的要求（例如，保护、保存) |
| 5.34 隐私和个人可识别信息保护 |   |   | ——个人可识别信息（PII）处理规则，例如，在特定主题策略中——组织在其开展业务或使用其产品和服务[这些产品和服务可能影响隐私和个人可识别信息（PII）保护]的相关国家的列表——所识别的外部要求，包括隐私和个人可识别信息（PII）保护的法律、法规或合同要求——个人可识别信息（PII）处理者的分析显示通过适当的技术措施和组织措施满足了要求 |
| 5.35 信息安全的独立评审 |   |   | ——信息安全独立评审的实施计划——向最高管理层报告独立评审的结果（样本）——发现组织管理信息安全的方法不充分时，所采取的纠正措施 |
| 5.36 符合信息安全的策略、规则和标准 |   |   | ——评审组织遵守信息安全方针、特定主题策略、规则和标准的计划——评审结果（样本）和所采取的纠正措施 |
| 5.37 文件化的操作规程 |   |   | ——与信息安全有关的信息处理设施的操作规程 |
| 6 人员控制 |   |   |   |
| 6.1 审查 |   |   | ——背景调查的规则和过程，考虑了适用的法律、法规和道德规范——对新入职人员进行背景调查，适用时包括在职人员（例如，职位晋升、敏感岗位画像) |
| 6.2 任用条款和条件 |   |   | ——与信息安全责任有关的一般规则或一般条款和条件，例如，行为准则——工作人员接受有关信息安全的条款和条件——担任关键角色（例如，可访问敏感资料或可特许访问系统）的人员同意的特定信息安全责任的样本 |
| 6.3 信息安全意识、教育和培训 |   |   | ——信息安全意识、教育和培训方案，包括针对重要目标群体的具体内容——信息安全培训的出勤名单——与选取的参会者就其预期行为进行访谈的结果 |
| 6.4 违规处理过程 |   |   | ——正式的纪律处分规程，并传达给相关人员和其他相关方 |
| 6.5 任用终止或变更后的责任 |   |   | ——工作人员签署接受在离职或工作变动后仍有效的具体责任和职责 |
| 6.6 保密或不泄露协议 |   |   | ——员工和其他相关方签署的保密协议 |
| 6.7 远程工作 | 可能的 |   | ——关于远程工作的规则，例如，在特定主题策略中——物理安全措施和通信安全措施的样本——允许远程使用的安全信息处理设备的安排[例如，“自携设备”（BYOD），笔记本电脑] |
| 6.8 信息安全事态的报告 |   |   | ——工作人员发现信息安全事态时的报告机制——为提高报告信息安全事态的意识而提供的指导或开展的沟通 |
| 7 物理控制 |   |   |   |
| 7.1 物理安全边界 |   | 可能的 | ——安全区域的建造规则和物理屏障的强度——为每个相关场所设计的物理安全边界和安全区域 |
| 7.2 物理入口 | 可能的 | 推荐的 | ——安全区域入口的访问鉴别系统（物理的或电子的）——用于追踪工作人员和访客进入的访问日志——交接区的物理设计及相应的过程描述 |
| 7.3 办公室、房间和设施的安全保护 |   | 可能的 | ——办公室和设施的物理安全设计和实现，以屏蔽正在处理的敏感信息 |
| 7.4 物理安全监视 | 可能的 | 可能的 | ——物理监视系统的设计，以检测未经授权的物理访问——监视系统的保护——物理监视系统运行产生的日志 |
| 7.5 物理和环境威胁防范 |   | 推荐的 | ——物理威胁和环境威胁的风险评估结果——用于防止物理和环境威胁的适当措施的设计 |
| 7.6 在安全区域工作 |   | 可能的 | ——安全区域工作规则（说明具体的安全措施）——对安全区域实施的安全措施 |
| 7.7 清理桌面和屏幕 |   | 推荐的 | ——清理桌面和屏幕的规则，例如，在特定主题策略中——抽查清理桌面和屏幕的行为（例如，工作区域和打印机） |
| 7.8 设备安置和保护 |   | 可能的 | ——设备安置和保护规则——抽查设备安置和保护 |
| 7.9 组织场所外的资产安全 |   |   | ——组织场所外资产的使用规则[例如，自携设备（BYOD）指南]——对使用组织场所外资产的工作人员进行访谈或调查的结果 |
| 7.10 存储媒体 | 可能的 |   | ——使用可移动存储媒体的规则，例如，在特定主题策略中——限制或保护与可移动存储媒体发生信息传输的设备配置（包括例如，加密）——安全处置过程，以及这类过程的记录 |
| 7.11 支持性设施 |   | 推荐的 | ——为设施安装的保护措施，特别是在数据中心（例如，温度、电力供应、水）——切断电力、水、气或其他设施的紧急规定 |
| 7.12 布缆安全 |   | 可能的 | ——物理布线和布缆保护 |
| 7.13 设备维护 |   |   | ——不同类型设备的维护规程——设备维护记录 |
| 7.14 设备的安全处置或重复使用 | 可能的 | 可能的 | ——含存储媒体的设备的处置或重复使用规则——信息或设备的物理或逻辑毁坏记录 |
| 8 技术控制 |   |   |   |
| 8.1 用户终端设备 | 可能的 |   | ——用户终端设备的安全配置和处理规则，例如，在特定主题策略中——终端用户的意识教育活动，涵盖终端设备的安全要求和保护规程——适用时，自携设备（BYOD）上隔离和保护业务信息的规则——对允许远程使用的信息处理设备的安全设计[例如，自携设备（BYOD）、笔记本电脑] |
| 8.2 特许访问权限 | 可能的 |   | ——特许访问权限的受限分配、使用和监视的规则，例如，在特定主题策略中——鉴别和评审过程，以管理特许访问权限 |
| 8.3 信息访问限制 | 推荐的 |   | —— 限制访问信息和其他相关资产的规则，例如，在特定主题策略中—— 在敏感信息的整个生存周期（即创建、处理、存储、传输、处置）内保护对其访问的访问管理技术和过程 |
| 8.4 源代码的访问 | 推荐的 |   | —— 源代码、开发工具和软件库的（读、写）访问管理规程 |
| 8.5 安全鉴别 | 推荐的 |   | ——关于访问控制的鉴别技术和规程的规则，例如，在特定主题策略中——基于风险的决策和相应的系统或应用程序登录规程的的实施——对关键信息系统使用强鉴别或多因素鉴别 |
| 8.6 容量管理 | 可能的 |   | ——当前和预期的容量需求——测量资源的使用情况，例如，信息处理设施、人力资源、办公室和其他设施——提供充足容量或减少容量需求的规程 |
| 8.7 恶意软件防范 | 推荐的 |   | ——恶意软件防范规则——基于风险的资产覆盖以及相应的恶意软件检测软件配置——保护信息和其他资源免受恶意软件侵害的其他规程和措施——针对恶意软件的终端用户意识教育活动 |
| 8.8 技术脆弱性管理 | 推荐的 |   | ——收集和管理在用信息系统的技术脆弱性信息——脆弱性扫描（定期执行）或渗透测试的结果——对组织暴露于技术脆弱性的评估以及计划的缓解措施——软件更新过程，确保安装最新的且获批准的补丁和应用程序更新 |
| 8.9 配置管理 | 推荐的 |   | ——硬件、软件、服务和网络的配置规则，包括安全配置——管理、实施或应用、监视和评审配置的过程——硬件、软件、服务和网络安全配置的标准模板（即加固） |
| 8.10 信息删除 |   |   | ——及时删除存储在信息系统、设备或任何其他存储媒体中的信息的规则，例如，根据组织数据保留的特定主题策略——安全删除系统、应用程序和服务中敏感信息的规程——当第三方存储组织的信息时，包含信息删除条款的第三方协议 |
| 8.11 数据脱敏 |   |   | ——数据脱敏规则，例如，根据组织访问控制的特定主题策略——分析结果，以确定敏感信息[例如，个人可识别信息（PII）]的保护需要使用的诸如数据屏蔽、假名化或匿名化等技术——数据脱敏、假名化或匿名化所用的技术 |
| 8.12 数据防泄露 | 可能的 |   | ——适用于处理、存储或传输敏感信息的系统、网络和任何其他设备的数据防泄漏措施的规则——所识别的需防泄漏的信息——所识别的相关泄漏渠道，以及防泄漏的措施，包括监视——数据防丢失系统的配置 |
| 8.13 信息备份 | 推荐的 |   | ——信息、软件和系统的备份规则，例如，在备份特定主题策略中——基于组织既定业务需求的备份计划——对及时、正确地执行备份和处理备份失败进行监视的操作规程——定期执行备份恢复测试 |
| 8.14 信息处理设施的冗余 |   |   | ——所识别的、业务服务和信息系统的可用性需求——高可用性要求的系统架构，能提供适当的冗余——故障切换的测试结果 |
| 8.15 日志 | 推荐的 |   | ——关于创建日志的目的、收集哪些数据以及处理日志数据的任何特定要求的规则，例如，在日志特定主题策略中——与安全相关的日志列表，以确保日志免受未授权操作的措施——对日志事态进行定期分析和解释的规程，例如，识别异常活动或异常行为——日志系统的配置 |
| 8.16 监视活动 | 可能的 |   | ——监视网络、系统和应用程序异常行为的规则——建立正常行为的基线和派生的警报触发准则——在规定的保留期限内所维护的监视日志——分析结果，以识别异常行为 |
| 8.17 时钟同步 | 可能的 |   | ——组织使用的参考时间源列表——时钟同步的方法和时间差的处理 |
| 8.18 特权实用程序的使用 | 可能的 |   | ——所使用的、能超越系统和应用程序控制的实用程序列表——用于限制和严格控制这类实用程序的过程、规程和其他方法 |
| 8.19 运行系统软件的安装 | 可能的 |   | ——管理在运行系统上安装软件的规程和措施，包括已安装软件及其版本的清单——关于用户能安装的软件类型的规则——限制由工作人员而不是由经过培训的管理员安装软件 |
| 8.20 网络安全 | 推荐的 |   | ——确保网络中信息的安全和保护连接的网络服务不受未授权访问的规则——为保护网络中的信息及其支持性信息处理设施而实施的措施和安全功能，例如，配置模板、密码控制配置、网关规则集、网络设备配置示例——网络架构文档（图、配置文件、隔离）——系统连接到网络的鉴别规则 |
| 8.21 网络服务的安全 |   |   | ——安全使用网络和网络服务的规则——所用的、具有安全机制和服务级别的网络和网络服务列表——获得网络服务提供商的保证 |
| 8.22 网络隔离 |   |   | ——基于信任程度、关键性、敏感性和访问控制特定主题策略的网络域隔离规则——网络拓扑（包括无线）以及附有目的和规则描述的网络域隔离——定义的网络域安全边界——管理网络域的安全边界和防火墙规则的过程 |
| 8.23 网页过滤 | 可能的 |   | ——安全且适当地使用在线资源的规则，包括对不良或不适宜网站的任何限制——为减少接触外部网站的恶意内容而采取的措施，例如，过滤规则——向所有工作人员提供关于安全和适当地使用在线资源的意识教育和培训活动 |
| 8.24 密码技术的使用 | 推荐的 |   | ——有效使用密码技术的规则，包括可接受的密码和密钥管理，例如在密码技术特定主题策略中——组织所用的密码技术列表——密钥管理的标准、规程和方法，包括生成、存储、归档、检索、分发、停用和销毁密钥 |
| 8.25 安全开发生存周期 | 可能的 |   | ——软件安全开发规则，以确保在安全开发生存周期内设计和实现信息安全——开发、测试和生产环境之间的隔离——确保在整个软件开发过程中充分覆盖信息安全需求的安全过程和检查点——软件开发外包时，获得妥善处理信息安全要求的保证 |
| 8.26 应用程序安全要求 |   |   | ——基于具体的风险评估来定义应用程序安全要求的过程——已实施的应用程序风险评估，所描述的具体信息安全要求——最近开发或实现的应用程序样本所识别的要求，尤其是交易服务、电子订购和支付应用程序 |
| 8.27 系统安全架构和工程原则 |   |   | ——所建立的系统架构和安全工程原则，以确保信息系统在开发生存周期内得到安全设计、实现和运行——在软件开发中集成安全工程原则——具体应用程序的安全实现样本，证实上述工程原理的使用——适用时，在外包开发合同中嵌入安全工程原则 |
| 8.28 安全编码 | 可能的 |   | ——新开发和重用场景中所用的安全编码原则的规则——确保在规划、编码前、编码期间以及评审和维护期间应用安全编码原则的过程——最近开发活动样本中具体安全编码原则的应用，包括代码扫描技术——代码的保护机制，包括访问限制 |
| 8.29 开发和验收中的安全测试 | 推荐的 |   | ——安全测试规则，以便在将应用程序或代码部署到生产环境时，验证信息安全要求是否得到满足——实际用于安全测试的要求集样本，以及相应的测试结果——自动化测试工具（例如，代码分析工具、漏洞扫描器、功能测试）的输出和后续行动 |
| 8.30 开发外包 |   |   | ——关于如何在系统开发外包中实现组织要求的信息安全措施的规则——指导、监督和评审与系统开发外包有关的活动的规程的实施——供应商的监视或评审结果，以确保达到预期结果 |
| 8.31 开发、测试和生产环境的隔离 | 可能的 |   | ——生产、测试和开发环境之间隔离级别的规则，包括针对不同开发环境的特定要求——开发、测试和生产环境之间的隔离——测试和生产环境的保护（例如，访问限制、网络隔离，确保不使用敏感的生产信息） |
| 8.32 变更管理 | 推荐的 |   | ——变更管理规则，以保护信息安全——变更控制规程，例如，文件、规范、测试、质量控制和受控的实施——变更的实施示例，显示了如何测试、批准和部署变更 |
| 8.33 测试信息 | 可能的 |   | ——适当地选择、使用、保护和管理测试信息的规则——保护用于测试的运行信息的规程（例如，脱敏）——从测试环境中删除的信息样本 |
| 8.34 在审计测试中保护信息系统 | 可能的 |   | ——涉及运行系统评估的审计测试或其他保障活动的清单——已完成的审计测试样本，以及是如何商定和实施这些测试的 |

1. 参 考 文 献

[1] ISO 9000 Quality management systems — Fundamentals and vocabulary

[2] ISO 9001 Quality management systems — Requirements

[3] ISO 19011 Guidelines for auditing management systems

[4] ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[5] ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls

[6] ISO/IEC TS 27006-2 Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems

[7] ISO/IEC 27007 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

[8] IAF MD5 Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. ISO/IEC TS 27006-2将被ISO/IEC 27706取代。 [↑](#footnote-ref-0)
2. 本列中的编号与GB/T 22080—202X附录A中控制的编号相一致。 [↑](#footnote-ref-1)