ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25067—2020/ISO/IEC 27006:2015
代替 GB/T 25067—2016

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

Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

（ISO/IEC 27006:2015,IDT）

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 25067—2016《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—2016 相比，主要技术变化如下：

——在规范性引用文件中，删除了 ISO 19011，新增了 ISO/IEC 27000(见第 2 章)；

——删除了术语“证书”“认证机构”“标志”和“组织”(见 2016 年版的第 3 章)；

——基于 GB/T 27021.1—2017 的附录 A，细化了参与信息安全管理体系认证的各类人员的能力要求(见 7.1.2)；

——遵从 GB/T 27021.1—2017 的标准结构，调整了第 9 章过程要求的内容(见第 9 章，2016 年版的第 9 章)；

——审核时间计算由资料性附录调整为规范性附录(见附录 B)，并新增了审核时间计算示例(见附录 C)。

本标准使用翻译法等同采用 ISO/IEC 27006:2015《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》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2016，IDT)

本标准做了以下编辑性修改：

——因 ISO 9000:2005 已经废止，所以引言中管理体系的定义调整为参见 GB/T 19000—2016；

——增加了资料性附录 NA；

——词汇“procedure”，在针对认证机构运作管理时翻译为“程序”[见 7.1.2.4.1 b)、9.1.3.2、9.1.5.1.2 等]，在针对客户信息安全控制管理时翻译为“规程”[见 7.1.2.1.4 a)、9.2.2.2 a)、9.3.1.2.1 a)等]，两者意思并无差异；

——由于附录 A 只在 7.1.1 中被引用，根据国家标准起草规定，将 7.1.1 的注调整为标准条文；

——对表 D.1 中控制“A.13.1.3 网络中的隔离”的“审核的评审指南”，更正了网段和网络隔离的示例。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国合格评定国家认可中心、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、广州赛宝认证中心服务有限公司、华夏认证中心有限公司、国家认证认可监督管理委员会、山东省标准化研究院。

本标准主要起草人：付志高、张强、黄俊梅、魏军、田刚、夏芳、张志国、尤其、方洁、王曙光、刘鑫。

本标准所代替标准的历次版本发布情况为：

——GB/T 25067—2010、GB/T 25067—2016。

引　言

GB/T 27021.1—2017 为机构对组织的管理体系实施审核和认证建立了准则。如果这类机构按照 GB/T 22080—2016 开展以信息安全管理体系(以下简称“ISMS”)审核和认证为目的活动,并准备依据 GB/T 27021.1—2017 获得认可,对 GB/T 27021.1—2017 补充一些要求和指南是必要的。本标准提供了这样的内容。

本标准正文遵循 GB/T 27021.1—2017 的结构,针对 ISMS 审核和认证所增加的特定要求和指南,用字母“IS”加以标识。

本标准的主要目的是使得认可机构在应用其评审认证机构所依据的标准时能更有效地协调一致。

本标准中术语“管理体系”和“体系”可以互换使用。管理体系的定义见 GB/T 19000—2016。请不要将本标准中使用的管理体系与其他类型的系统混淆,例如,信息技术(以下简称“IT”)系统。

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

1　范围

本标准在GB/T 27021.1—2017和GB/T 22080—2016的基础上，对实施ISMS审核和认证的机构规定了要求并提供了指南。本标准的主要目的是为ISMS认证机构的认可提供支持。

任何提供ISMS认证的机构，需要在能力和可靠性方面证实其满足本标准中的要求。本标准中的指南提供了对这些要求的进一步解释。

注：本标准可以作为认可、同行评审或其他审核过程的准则性文件。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2016　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2013，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)

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

3　术语和定义

GB/T 27021.1—2017和ISO/IEC 27000界定的以及下列术语和定义适用于本文件。

3.1

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。

4　原则

GB/T 27021.1—2017中第4章的原则适用。

5　通用要求

5.1　法律与合同事宜

GB/T 27021.1—2017中5.1的要求适用。

5.2　公正性的管理

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

5.2.1 IS 5.2 利益冲突

认证机构可以从事以下工作,不会被视为咨询或具有潜在的利益冲突:

a) 安排培训课程并参与讲授。如果这些课程涉及信息安全管理、有关的管理体系或审核时,认证机构应仅限于提供可公开获取的通用信息和建议,即认证机构不应针对具体公司提供那些违反下面 b)要求的建议。

b) 根据请求,提供或发布认证机构对认证审核标准要求的解释性信息(见 9.1.3.6)。

c) 审核前活动,仅以确定认证审核是否就绪为目的,但是这些活动不应导致提供违反本条款的建议和意见。认证机构应能够证实这些活动不违反本条款的要求,且没有把这些活动作为减少最终认证审核时间的理由。

d) 按照认可范围之外的标准或法规,实施第二方审核或第三方审核。

e) 在认证审核和监督审核过程中的增值活动,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。

认证机构不应为客户寻求认证的 ISMS 提供内部信息安全评审。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)。

5.3 责任和财力

GB/T 27021.1—2017 中 5.3 的要求适用。

6 结构要求

GB/T 27021.1—2017 中第 6 章的要求适用。

7 资源要求

7.1 人员能力

GB/T 27021.1—2017 中 7.1 的要求适用。并且,以下要求和指南适用。

7.1.1 IS 7.1.1 总体考虑

7.1.1.1 通用的能力要求

认证机构应确保其具备与所评估的客户 ISMS 有关的、最新的技术知识和法律法规知识。

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 规定的以及 7.1.2 和 7.2.1 中所规定的、与认证机构所确定的 ISMS 技术领域相关的所有要求。

附录 A 概括了特定认证职能的人员能力要求。

7.1.2 IS 7.1.2 能力准则的确定

7.1.2.1 实施 ISMS 审核的能力要求

7.1.2.1.1 总体要求

认证机构应有验证审核组成员的背景经验、特定培训或情况说明的准则,以确保审核组至少具备:

a) 信息安全的知识;

b) 与受审核的活动相关的技术知识；

c) 管理体系的知识；

d) 审核原则的知识；

注：有关审核原则的进一步信息，参见 ISO 19011。

e) ISMS 监视、测量、分析和评价的知识。

除了 b)可以在作为审核组成员的审核员之间共享外，以上 a)～e)适用于作为审核组成员的所有审核员。

审核组应有能力将客户 ISMS 中信息安全事件的迹象追溯到 ISMS 的相应要素。

审核组应有关于上述知识项的适当工作经历且实际应用过这些知识项(这不意味着一个审核员需要具有信息安全所有领域的全面的经验，但审核组整体上应对被审核的领域具备足够的认识和经验)。

7.1.2.1.2 信息安全管理术语、原则、实践和技术

审核组所有成员作为一个整体，应具有以下知识：

a) ISMS 特定文件的结构、层级和相互关系；

b) 信息安全管理相关的工具、方法、技术及其应用；

c) 信息安全风险评估和风险管理；

d) ISMS 适用的过程；

e) 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。

每个审核员应满足 a)、c)和 d)。

7.1.2.1.3 信息安全管理体系标准和规范性文件

参与 ISMS 审核的审核员，应具有以下知识：

a) GB/T 22080—2016 的所有要求；

审核组所有成员作为一个整体，应具有以下知识：

b) GB/T 22081(如确定有必要，还可来源于特定行业标准)中的所有控制及其实现，这些控制分为以下类别：

1) 信息安全策略；
2) 信息安全组织；
3) 人力资源安全；
4) 资产管理；
5) 访问控制，包括授权；
6) 密码；
7) 物理和环境安全；
8) 运行安全，包括 IT 服务；
9) 通信安全，包括网络安全管理和信息传输；
10) 系统获取、开发和维护；
11) 供应商关系，包括外包服务；
12) 信息安全事件管理；
13) 业务连续性管理的信息安全方面，包括冗余；
14) 符合性，包括信息安全评审。

7.1.2.1.4 业务管理实践

参与 ISMS 审核的审核员，应具有以下知识：

a) 行业的信息安全最佳实践和信息安全规程；
b) 信息安全的策略和业务要求；
c) 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；
d) 管理过程和相关的术语。

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。

7.1.2.1.5 客户的业务领域

参与 ISMS 审核的审核员，应具有以下知识：

a) 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。
b) 与业务领域相关的信息安全风险；
c) 与客户业务领域相关的通用术语、过程和技术；
d) 相关业务领域的实践。

其中的 a)可在审核组内共享。

7.1.2.1.6 客户的产品、过程和组织

审核组所有成员作为一个整体，应具有以下知识：

a) 组织类型、规模、治理、结构、职能和关系对 ISMS 的开发与实施和认证活动的影响，包括外包；
b) 广义上的复杂运营；
c) 适用于产品或服务的法律法规要求。

7.1.2.2 领导 ISMS 审核组的能力要求

除了 7.1.2.1 中的要求以外，审核组组长还应满足以下要求，且应在有指导和监督的审核中予以证实：

a) 具备管理认证审核过程和审核组的知识和技能；
b) 具备有效的口头和书面沟通能力。

7.1.2.3 实施申请评审的能力要求

7.1.2.3.1 信息安全管理体系标准和规范性文件

实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间的人员，应具备以下知识：

a) 认证过程中所用的相关 ISMS 标准和其他规范性文件。

7.1.2.3.2 客户的业务领域

实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间的人员，应具备以下知识：

a) 与客户业务领域相关的通用术语、过程、技术和风险。

7.1.2.3.3 客户的产品、过程和组织

实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间的人员，应具备以下知识：

a) 客户产品、过程、组织类型、规模、治理、结构、职能以及 ISMS 的开发与实施和认证活动之间的关系，包括外包的职能。

7.1.2.4 复核审核报告并做出认证决定的能力要求

7.1.2.4.1 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，特别是识别接口与依赖关系的持续有效性和相应的风险。

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：

a) 通用的管理体系；

b) 审核过程和程序；

c) 审核原则、实践和技巧。

7.1.2.4.2 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：

a) 7.1.2.1.2 中 a)、c)、d)所列条目；

b) 与信息安全相关的法律法规要求。

7.1.2.4.3 信息安全管理体系标准和规范性文件

复核审核报告并做出认证决定的人员，应具备以下知识：

a) 认证过程中所用的相关 ISMS 标准和其他规范性文件。

7.1.2.4.4 客户的业务领域

复核审核报告并做出认证决定的人员，应具备以下知识：

a) 与相关业务领域实践有关的通用术语和风险。

7.1.2.4.5 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，应具备以下知识：

a) 客户的产品、过程、组织类型、规模、治理、结构、职能和关系。

7.2 参与认证活动的人员

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

7.2.1 IS 7.2 证实审核员的知识和经验

认证机构应通过以下方面来证实审核员具备知识和经验：

a) 获得承认的 ISMS 特定资格；

b) 适用时，注册为审核员；

c) 参加 ISMS 培训课程并获得相关的个人证书；

d) 最新的持续专业发展记录；

e) 由另一个 ISMS 审核员见证 ISMS 审核。

7.2.1.1 选择审核员

除 7.1.2.1 之外，选择审核员的准则应确保每位审核员：

a) 具备相当于大学教育水平的专业教育或培训。

b) 在信息技术方面具备至少 4 年的全职实际工作经历，其中至少 2 年的工作经历来自与信息安

全有关的职责或职能。

c) 成功地完成至少 5 天的培训,培训范围包括 ISMS 审核和审核管理。

d) 在被赋予审核员责任之前,已获得整个信息安全评估过程的经验。宜通过参与最少 4 次、总天数至少 20 天(其中最多 5 天可来自监督审核)的 ISMS 认证审核(包括再认证审核和监督审核)来获得这种经验。参与审核时,应包括评审文件与风险评估,评估实施情况和报告审核情况。

e) 具备相关的且合乎时宜的经验。

f) 通过持续的专业发展,保持当前在信息安全和审核方面的知识和技能是最新的。

技术专家应符合准则 a)、b)和 e) 。

7.2.1.2 选择领导审核组的审核员

除了 7.1.2.2 和 7.2.1.1 外,选择领导审核组的审核员的准则应确保该审核员:

a) 已经积极参与过至少 3 次 ISMS 审核的所有阶段。参与审核时,应包括初次的范围识别与策划、评审文件与风险评估、评估实施情况和正式地报告审核情况。

7.3 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。并且,以下要求和指南适用。

7.3.1 IS 7.3 使用外部审核员或外部技术专家作为审核组的一部分

技术专家应在审核员的监督下进行工作。7.2.1.1 列出了技术专家的最低要求。

7.4 人员记录

GB/T 27021.1—2017 中 7.4 的要求适用。

7.5 外包

GB/T 27021.1—2017 中 7.5 的要求适用。

8 信息要求

8.1 公开信息

GB/T 27021.1—2017 中 8.1 的要求适用。

8.2 认证文件

GB/T 27021.1—2017 中 8.2 的要求适用。并且,以下要求和指南适用。

8.2.1 IS 8.2 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。

认证文件也可以包括对所用的特定行业标准的标识。

8.3 认证的引用和标志的使用

GB/T 27021.1—2017 中 8.3 的要求适用。

8.4 保密

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

8.4.1 IS 8.4 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性或敏感性信息而导致不能提供给审核组核查的 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 ISMS 是否能在缺少这些信息的情况下得到充分审核。如果认证机构的结论是若不核查已识别的保密性或敏感性信息就不能对 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。

8.5 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。

9 过程要求

9.1 认证前的活动

9.1.1 申请

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

9.1.1.1 IS 9.1.1 申请准备

认证机构应要求客户具有一个已文件化且已实施的、符合 GB/T 22080—2016 和认证所要求的其他文件的 ISMS。

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

GB/T 27021.1—2017 中 9.1.3 的要求适用。并且,以下要求和指南适用。

9.1.3.1 IS 9.1.3 总则

ISMS 审核的审核方案应考虑所确定的信息安全控制。

9.1.3.2 IS 9.1.3 审核方法

认证机构的程序不应预先假定 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定客户的 ISMS 满足 GB/T 22080—2016 的要求和客户的策略与目标。

注:ISO/IEC 27007 给出了有关审核的进一步指南。

9.1.3.3 IS 9.1.3 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。在认证审核的第一阶段,客户应至少提供以下信息:

a) ISMS 和其所覆盖活动的一般信息;

b) GB/T 22080—2016 中所规定的、必要的 ISMS 文件的副本，以及必要的相关文件。

9.1.3.4 IS 9.1.3 评审周期

如果一个 ISMS 没有至少实施过一次覆盖认证范围的管理评审和内部审核，认证机构不应对该 ISMS 实施认证。

9.1.3.5 IS 9.1.3 认证范围

审核组应根据所有适用的认证要求，对包含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 范围内满足了 GB/T 22080—2016 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了其活动，并延伸到认证范围内所界定的、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。认证机构应验证每个认证范围至少有一个适用性声明。

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，并已包括在客户的信息安全风险评估中。与其他机构共享设施(例如，IT 系统、数据库、通信系统或外包一项业务职能)，是这类情形的一个示例。

9.1.3.6 IS 9.1.3 认证审核准则

客户 ISMS 接受审核的准则应是 ISMS 标准 GB/T 22080—2016。与所履行的职能相关的其他文件，可以作为认证要求。

9.1.4 确定审核时间

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

9.1.4.1 IS 9.1.4 审核时间

认证机构应给予审核员足够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。

认证机构应按照附录 B 来确定审核时间。

注：附录 C 提供了计算审核时间的进一步指南和示例。

9.1.5 多场所的抽样

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

9.1.5.1 IS 9.1.5 多场所

9.1.5.1.1 当客户拥有满足以下 a)～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：

a) 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；

b) 所有的场所都包含在客户的 ISMS 内部审核方案中；

c) 所有的场所都包含在客户的 ISMS 管理评审方案中。

9.1.5.1.2 认证机构使用基于抽样的方法时，应有适宜的程序以确保：

a) 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。

b) 结合以下因素，认证机构抽取具有代表性的场所：

1) 总部及其他场所的内部审核的结果；

2) 管理评审的结果；

3） 场所规模的差异；
4） 各场所业务目的的差异；
5） 不同场所的信息系统的复杂程度；
6） 工作实践的差异；
7） 所实施的活动的差异；
8） 控制的设计与运行的差异；
9） 与关键的信息系统或处理敏感信息的信息系统之间的潜在交互；
10） 任何不同的法律要求；
11） 地域因素和文化因素；
12） 场所的风险状况；
13） 发生在特定场所的信息安全事件。

c） 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。
d） 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。
e） 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。
f） 无论是在总部还是在单个场所发现不符合，纠正措施程序的实施适用于证书所覆盖的总部和所有场所。

审核应关注客户总部为确保一个单一的 ISMS 适用于所有场所并在运行层面上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

GB/T 27021.1—2017 中 9.1.6 的要求适用。并且，以下要求和指南适用。

9.1.6.1 IS 9.1.6 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文件相结合的文件（例如，信息安全、质量、健康与安全、环境）。

9.1.6.2 IS 9.1.6 管理体系结合审核

只要能够证实审核满足了 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，所有对 ISMS 重要的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。

9.2 策划审核

9.2.1 确定审核目的、范围和准则

GB/T 27021.1—2017 中 9.2.1 的要求适用。并且，以下要求和指南适用。

9.2.1.1 IS 9.2.1 审核目的

审核目的应包括确定管理体系的有效性，以确保客户已根据风险评估实施了适用的控制并实现了所设立的信息安全目标。

9.2.2 选择和指派审核组

GB/T 27021.1—2017 中 9.2.2 的要求适用。并且，以下要求和指南适用。

9.2.2.1 IS 9.2.2 审核组

认证机构应正式任命审核组并为其提供相应的工作文件。认证机构应明确地规定审核组的任务，并使客户知晓。

审核组可以由一个人组成，只要其满足 7.1.2.1 中所规定的全部准则。

9.2.2.2 IS 9.2.2 审核组能力

7.1.2 的要求适用。对于监督和特殊审核活动，仅与所安排的监督活动和特殊审核活动相关的那些要求适用。

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) 对拟认证的 ISMS 范围内的特定活动具备适当的技术知识，以及相关时，对这些活动的相关规程和其潜在信息安全风险具备适当的技术知识（技术专家可以履行此项职责）；

b) 理解客户，足以基于客户 ISMS 范围和组织环境对其 ISMS（该体系管理着客户的活动、产品和服务的信息安全）进行可靠的认证审核；

c) 适当地理解适用于客户 ISMS 的法律法规要求。

注：适当地理解法规要求不意味着要有深厚的法律背景。

9.2.3 审核计划

GB/T 27021.1—2017 中 9.2.1 的要求适用。并且，以下要求和指南适用。

9.2.3.1 IS 9.2.3 总则

ISMS 审核计划应考虑所确定的信息安全控制。

9.2.3.2 IS 9.2.3 网络支持审核技术

如适宜，审核计划应识别审核中将使用的网络支持审核技术。

网络支持审核技术可包括：例如，电话会议、网络会议、基于网络的交互式通信和远程电子访问 ISMS 文件和（或）ISMS 过程。对这些技术的关注重点，宜是提高审核的有效性和效率，并支持审核过程的完整性。

9.2.3.3 IS 9.2.3 审核时间的选择

认证机构宜与拟审核的组织就选择一个能最有效地证实其全部范围的审核时间达成一致。适当时，可考虑季度、月份、日期和班次。

9.3 初次认证

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

9.3.1 IS 9.3.1 初次认证审核

9.3.1.1 IS 9.3.1.1 第一阶段

在该审核阶段，认证机构应获取有关 ISMS 设计的文件，其中包括 GB/T 22080—2016 所要求的文件。

认证机构应充分了解在组织环境下所进行的 ISMS 设计、风险评估和处置（包括所确定的控制）、信息安全方针和目标，以及特别是客户的审核准备情况。在此基础上，才能进行第二阶段的策划。

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,认证机构应审查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。

认证机构应让客户知晓第二阶段可能需要详细检查的、更多类型的信息和记录。

9.3.1.2 IS 9.3.1.2 第二阶段

9.3.1.2.1 基于第一阶段审核报告中的审核发现,认证机构制定实施第二阶段的审核计划。除了评价ISMS的有效实施之外,第二阶段的目的是:

a) 确认客户遵守自身的方针、目标和规程。

9.3.1.2.2 为此,审核应重点关注客户的:

a) 最高管理层对信息安全方针和信息安全目标的领导和承诺;
b) GB/T 22080—2016 中所列的文件要求;
c) 对与信息安全有关的风险的评估,以及在重复评估时可产生一致的、有效的和可比较的结果;
d) 基于风险评估和风险处置过程所确定的控制目标和控制;
e) 根据信息安全目标对其实施了评价的信息安全绩效和 ISMS 有效性;
f) 所确定的控制、适用性声明和风险评估与风险处置过程的结果,与信息安全方针和目标之间的一致性;
g) 控制的实现(参见附录 D),考虑了外部环境、内部环境、相关的风险,以及组织为确定控制是否得以实现、有效且达到其所规定的信息安全目标而对信息安全过程和控制进行的监视、测量与分析;
h) 方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审,以确保其可被追溯至管理决定、信息安全方针和信息安全目标。

9.4 实施审核

GB/T 27021.1—2017 中 9.4 的要求适用。并且,以下要求和指南适用。

9.4.1 IS 9.4 总则

认证机构应具备文件化的程序,以:

a) 依据 GB/T 27021.1—2017 的规定,对客户的 ISMS 进行初次认证审核;
b) 依据 GB/T 27021.1—2017,对客户的 ISMS 定期进行监督审核和再认证审核,以确认其持续符合相关要求,并验证和记录客户为纠正所有的不符合而及时采取了纠正措施。

9.4.2 IS 9.4 ISMS 审核的特定要素

认证机构,由审核组所代表,应:

a) 要求客户证实对信息安全相关风险的评估与 ISMS 范围内的 ISMS 运行是相关的和充分的;
b) 确定客户识别、检查和评价信息安全相关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健全并得到正确实施。

9.4.3 IS 9.4 审核报告

9.4.3.1 除了 GB/T 27021.1—2017 中 9.4.8 对审核报告的要求之外,审核报告应提供以下信息或对这些信息的引用:

a) 审核的说明,其中包括文件评审摘要;
b) 对客户信息安全风险分析进行认证审核的说明;

c) 与审核计划的偏离(例如:在某一预定的活动上花费更多或更少的时间);

d) ISMS 的范围。

9.4.3.2 审核报告应足够详细,以帮助和支持认证决定。审核报告应包括:

a) 所采用的主要审核路线和所使用的审核方法(见 9.1.3.2);

b) 形成的观察结果,包括正面的(例如,值得注意的特征)和负面的(例如,潜在的不符合);

c) 对客户的 ISMS 符合认证要求的评价意见和对不符合的清楚说明、所引用的适用性声明的版本,以及适用时,与客户以往认证审核结果的任何有用的对照。

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完整的审核报告的一部分。如果使用这些方法,这些文件应作为支持认证决定的证据提供给认证机构。在审核过程中,有关被评价的样本的信息应包含在审核报告或其他认证资料中。

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。

除了 GB/T 27021.1—2017 中 9.4.8 对审核报告的要求之外,报告还应包括:

a) 关于 ISMS 要求和信息安全控制的实现与有效性的、最重要的观察(正面的和负面的)的摘要;

b) 审核组关于客户的 ISMS 是否获得认证的建议,以及支持该建议的信息。

9.5 认证决定

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

9.5.1 IS 9.5 认证决定

除了 GB/T 27021.1—2017 的要求外,认证决定应基于审核报告(见 9.4.3)中审核组对客户的 ISMS 是否通过认证的建议。

通常情况下,对授予认证做出决定的人员或委员会不宜推翻审核组的负面建议。如果发生这种情况,认证机构应记录其做出推翻建议的决定的依据,并说明其合理性。

只有具备充分的证据证实管理评审和 ISMS 内部审核的安排已经实施,且是有效的并将得到保持,才可向客户授予认证。

9.6 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

GB/T 27021.1—2017 中 9.6.2 的要求适用。并且,以下要求和指南适用。

9.6.2.1 IS 9.6.2 监督活动

9.6.2.1.1 监督审核程序,应与本标准中有关客户 ISMS 的认证审核的要求和指南保持一致。

监督的目的是验证已被认证的 ISMS 得到持续实施、考虑由客户运作变化所引起的管理体系变化的影响并确认与认证要求的持续符合。监督审核方案应至少包括:

a) 管理体系的保持要素,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;

b) 根据 ISMS 标准 GB/T 22080—2016 和认证所需的其他文件的要求,与来自外部各方沟通;

c) 文件化的管理体系的变更;

d) 发生变更的区域;

e) 所选择的 GB/T 22080—2016 的要求；

f) 适宜时，其他所选择的区域。

9.6.2.1.2 认证机构的每一次监督应至少审查以下方面：

a) ISMS 在实现客户信息安全方针的目标方面的有效性；

b) 对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

c) 所确定的控制的变更，及其引起的适用性声明的变更；

d) 控制的实现和有效性(根据审核方案来审查)。

9.6.2.1.3 认证机构应能够针对与风险相关的信息安全问题及其对客户的影响来调整监督方案，并说明监督方案的合理性。

监督审核可以与其他管理体系的审核相结合。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，并且在发现任何不符合或不满足认证要求时，还应检查客户是否对其自身的 ISMS 和规程进行了调查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出现的不符合、适用性声明的版本和从上次审核之后发生的重大变更的信息。监督审核报告应至少完全覆盖 9.6.2.1.1 和 9.6.2.1.2 的要求。

9.6.3 再认证

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

9.6.3.1 IS 9.6.3 再认证审核

再认证审核程序，应与本标准中有关客户 ISMS 的初次认证审核的要求和指南保持一致。

允许采取纠正措施的时间，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。并且，以下要求和指南适用。

9.6.4.1 IS 9.6.4 特殊情况

如果获得 ISMS 认证的客户对其管理体系做了重大修改，或者发生影响其获证基础的其他变更，实施特殊审核所必需的活动应遵从特别规定。

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。

9.7 申诉

GB/T 27021.1—2017 中 9.7 的要求适用。

9.8 投诉

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

9.8.1 IS 9.8 投诉

投诉意味着一个潜在的事件，表明可能存在不符合。

9.9 客户的记录

GB/T 27021.1—2017 中 9.9 的要求适用。

10 认证机构的管理体系要求

10.1 可选方式

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

10.1.1 IS 10.1 ISMS 实施

建议认证机构依据 GB/T 22080—2016 实施 ISMS。

10.2 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。

10.3 方式 B:与 GB/T 19001 一致的管理体系要求

GB/T 27021.1—2017 中 10.3 的要求适用。

附 录 A
（资料性附录）
ISMS 审核与认证的知识与技能

A.1 概述

表 A.1 提供了 ISMS 审核与认证所要求的知识与技能的摘要。然而，表 A.1 是资料性的，因为它只识别了特定认证职能所需的知识与技能的领域。

本标准的正文阐述了每项认证职能的能力要求，表 A.1 给出了对具体要求的引用。

表 A.1 ISMS 审核与认证的知识

	认证职能		
	实施申请评审（实施申请评审，以确定所需的审核组能力、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
知识			
信息安全管理术语、原则、实践和技术		7.1.2.4.2	7.1.2.1.2
信息安全管理体系标准/规范性文件	7.1.2.3.1	7.1.2.4.3	7.1.2.1.3
业务管理实践			7.1.2.1.4
客户的业务领域	7.1.2.3.2	7.1.2.4.4	7.1.2.1.5
客户的产品、过程和组织	7.1.2.3.3	7.1.2.4.5	7.1.2.1.6

A.2 对通用能力的考虑

有很多途径可以证实审核员的知识和经验，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可以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，使其与组织的行业/技术领域和 ISMS 的复杂性相符。

A.3 对特定知识和经验的考虑

A.3.1 与 ISMS 相关的典型知识

除了 7.1.2 中的要求外，宜考虑以下要求。审核员宜具备并理解下列审核和 ISMS 方面的知识：

——审核方案和策划；

——审核类型和方法；

——审核风险；

——信息安全过程分析；
——持续改进；
——信息安全内部审核。

审核员宜具备并理解下列法规要求方面的知识：

——知识产权；
——组织记录的内容、保护和保存；
——数据保护与隐私；
——密码控制规则；
——电子商务；
——电子签名与数字签名；
——工作场所监督；
——通信侦听与数据监视(例如,电子邮件)；
——计算机滥用；
——电子证据收集；
——渗透测试；
——国际的和国家的行业特定要求(例如,银行业)。

附 录 B
（规范性附录）
审 核 时 间

B.1 概述

本附录包含了与 GB/T 27021.1—2017 中 9.1 有关的进一步要求。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，以便其在对客户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。

认证机构应针对每一个客户及其被认证的 ISMS，识别初次认证、监督审核和再认证审核所需花费的审核时间。在审核策划阶段，使用本附录可以确保使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（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：

——用于审核时间计算的概念（见 B.2）；

——确定不同审核阶段所需时间的程序的要求（见 B.3～B.5）；

——与多场所审核相关的要求（见 B.6）。

附录 C 给出了审核时间计算的示例，对附录 B 的应用做出了说明。

该方法的基本假设是，确定审核时间的计算方案宜：

a） 仅考虑那些能够被确定和证实的属性；

b） 足够简便，以得到认证机构的有效应用；

c） 足够复杂，以能够体现充分的差异。

审核时间的确定，是基于下面表 B.1（“审核时间表”）所提供的数值，并应考虑调整的促成因素。

B.2 概念

B.2.1 在组织控制下工作的人员的数量

在组织控制下工作的、所有班次的人员的总数，是确定审核时间的起点。

注：术语“在组织控制下工作的人员”，在 GB/T 27021.1—2017 中称之为员工。

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一名全职雇员工作小时数的比较。

B.2.2 审核人天

表 B.1 中所引用的“审核时间”，是根据审核中花费的“审核人天”来阐述的。附录 B 的计算基础是一个 8 h 的工作日。

B.2.3 临时场所

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。此类场所的范围可从大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发生的不符合而导致没能满足信息安全目标的风险的评价。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 9.1.5.1。

B.3 确定初次认证审核时间的程序

B.3.1 总则

审核时间的计算，应遵从文件化的程序。

B.3.2 远程审核

如果使用了远程审核技术（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）与组织接触，这些活动宜在审核计划中加以识别（见 9.2.3），可以考虑将其作为总的“现场审核时间”的一部分。

如果认证机构制定的审核计划中远程审核活动占据了大于 30%的现场审核时间，认证机构宜证实审核计划的合理性，并在审核计划实施前得到认可机构的专门批准。

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

B.3.3 审核时间的计算

表 B.1 给出了初次审核天数平均值的起点[在此处及后面的内容中，这个数值包括一次初次审核（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，有些需要较多的审核时间，有些需要较少的审核时间。

表 B.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，然后根据适用于所审核的 ISMS 范围的重要因素来调整它，通过对每一个因素赋予增、减权重来修正基数。使用表 B.1 时应考虑调整的促成因素和最大偏移的限制（见 B.3.4 和 B.3.5）。B.2 解释了表 B.1 中所使用的术语，附录 C 提供了如何计算审核时间的示例。

表 B.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时间（审核人日）	环境管理体系初次审核时间（审核人日）	ISMS 初次审核时间（审核人日）	增加或减少的因素	总审核时间
1～10	1.5～2	2.5～3	5	见 B.3.4	
11～15	2.5	3.5	6	见 B.3.4	
16～25	3	4.5	7	见 B.3.4	
26～45	4	5.5	8.5	见 B.3.4	
46～65	5	6	10	见 B.3.4	
66～85	6	7	11	见 B.3.4	
86～125	7	8	12	见 B.3.4	
126～175	8	9	13	见 B.3.4	
176～275	9	10	14	见 B.3.4	

表 B.1（续）

在组织控制下工作的人员的数量	质量管理体系初次审核时间（审核人日）	环境管理体系初次审核时间（审核人日）	ISMS初次审核时间（审核人日）	增加或减少的因素	总审核时间
276～425	10	11	15	见 B.3.4	
426～625	11	12	16.5	见 B.3.4	
626～875	12	13	17.5	见 B.3.4	
876～1 175	13	15	18.5	见 B.3.4	
1 176～1 550	14	16	19.5	见 B.3.4	
1 551～2 025	15	17	21	见 B.3.4	
2 026～2 675	16	18	22	见 B.3.4	
2 676～3 450	17	19	23	见 B.3.4	
3 451～4 350	18	20	24	见 B.3.4	
4 351～5 450	19	21	25	见 B.3.4	
5 451～6 800	20	23	26	见 B.3.4	
6 801～8 500	21	25	27	见 B.3.4	
8 501～10 700	22	27	28	见 B.3.4	
＞10 700	沿用以上规律	沿用以上规律	沿用以上规律	见 B.3.4	

B.3.4 调整审核时间的因素

不能孤立地使用表 B.1。所安排的时间，还应考虑以下因素。这些因素与 ISMS 复杂程度相关，并因此与 ISMS 审核工作量相关：

a) ISMS 的复杂程度（例如，信息的关键程度、ISMS 的风险状况）；
b) ISMS 范围内所开展的业务的类型；
c) 以往已证实的 ISMS 绩效；
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]；
e) ISMS 范围内所使用的外包和第三方安排的程度；
f) 信息系统开发的程度；
g) 场所的数量和灾难恢复场所的数量；
h) 对于监督或再认证审核：符合 GB/T 27021.1—2017 中 8.5.3 要求的、与 ISMS 相关的变更的数量和程度。

附录 C 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其他因素，例如：

a) 复杂的后勤，在 ISMS 范围中涉及不止一处建筑物或地点；
b) 员工的语言超过一种（需要翻译或审核员个人无法独立工作），提供的文件使用了一种以上的语言；
c) 为了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；
d) 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：

a） 没有风险或者低风险的产品/过程；

b） 过程只涉及单一的常规活动（例如，只有服务）；

c） 在组织控制下工作的雇员大部分是从事相同的任务；

d） 对组织已经有些了解（例如，如果组织获得了同一个认证机构的、另一个标准的认证）；

e） 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）；

f） 高度成熟的管理体系。

当认证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。

宜考虑上述因素，并根据这些因素对审核时间做出调整。这些因素可证实一次有效审核所需更多或更少的审核时间的合理性。增加时间的因素可被减少时间的因素冲抵。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。

B.3.5 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 B.1 中审核时间的减少，不应超过 30%。

应确定偏离审核时间表的适当理由，并形成文件。

B.3.6 现场审核时间

策划和编制报告一起所用的时间，通常不宜使总的现场“审核时间”减少到表 B.1 中“总审核时间”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。审核员旅途时间未计在内，这应在表中所给出的审核时间的基础上另外增加。

注：70%是基于 ISMS 审核经验所得出的系数。

B.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。宜时常评审所策划的监督审核时间，以考虑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控制），应增加监督审核的时间。

B.5 再认证审核的审核时间

用于再认证审核的全部时间，应取决于 9.4.3 和 GB/T 27021.1—2017 中 9.6.3 所规定的、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。

B.6 多场所的审核时间

应针对每个场所计算每个场所（包括总部）的审核人天数。

可以考虑因部分审核与总部或分场所无关而减少审核时间。认证机构应记录这类减少的合理理由。

附 录 C
（资料性附录）
审核时间计算方法

C.1 总则

本附录为推导出审核时间计算公式提供了进一步的指南。C.2 给出了一个对因数进行分类的示例，它可用作审核时间计算的基础。C.3 提供了一个审核时间计算的示例。

C.2 审核时间计算因数的分类

如 B.3.4 中 a)～h)所列举的，表 C.1 给出了对主要的审核时间计算因数进行分类的示例。认证机构可以使用该分类来制定一个符合 9.1.4.1 的审核时间计算方案。

表 C.1 审核时间计算因数的分类

	对工作量的影响		
	减少工作量	正常工作量	增加工作量
附录 B 中因数 （见 B.3.4）			
a) 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若干敏感/保密信息； ● 若干关键资产； ● 2 个～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 范围内所开展的业务的类型	● 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（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 C.1（续）

	对工作量的影响		
	减少工作量	正常工作量	增加工作量
附录 B 中因数（见 B.3.4）			
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；或 • 对外包协议进行了明确的规定、良好的管理与监视； • 外包方获得了 ISMS 认证； • 可获得相关的独立担保报告	• 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；或 • 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) 信息系统开发的程度	• 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，有若干针对重大业务目的的、正在实施中的项目
g) 场所的数量和灾难恢复场所的数量	• 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) 对于监督或再认证审核：符合 GB/T 27021.1—2017 中 8.5.3、与 ISMS 相关的变更的数量和程度	• 自上次再认证审核后未发生变化	• ISMS 的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 的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

C.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 B.3 中的因数来计算审核时间。该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 C.2 中每个类别的适宜分值，并对结果求和；

第二步：确定与 IT 环境相关的因数：识别表 C.3 中每个类别的适宜分值，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 C.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 B.1）所确定审核人天数乘以第三步中得出的系数。当利用多场所抽样时，要根据执行多场所抽样计划所需的工作量增加所计算出的审核人天。

这个结果是最终的审核人天数。

表 C.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[a]; 2)　组织的客户处于关键业务领域[a]; 3)　组织处于关键业务领域[a]
过程与任务	1)　标准过程,涉及标准的且重复的任务;大量在组织控制下工作的人员从事相同的任务;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 是新的且没有建立
[a] 关键业务领域是可以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、形象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 C.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 C.4　因数对审核时间的影响

业务复杂性	IT 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 B.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 C.2，可以得出与业务和组织相关的因子为 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 C.3，可以得出与 IT 环境相关的因子为 1＋3＋1＝5。利用表 C.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 C.2，与业务和组织相关的因子将变为：1＋1＋1＝3。根据表 C.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。

附 录 D
（资料性附录）
对已实现的 GB/T 22080—2016 附录 A 的控制的评审指南

D.1 目的

在初次认证审核的第二阶段以及监督或再认证活动[见 9.3.1.2.2 g)]中，需要评审客户确定其 ISMS 所需的控制（根据适用性声明）的实现情况。

认证机构所收集的审核证据，需足以得出控制是否有效的结论。例如，在客户的规程或策略中，可以对期望如何实施一项控制做出规定。

D.1.1 审核证据

通过审核员的观察（例如，要求上锁的门已经锁了、人员确实签署了保密协议、有资产登记且资产登记包含所看到的资产、系统设置是适当的等），可以收集到最好的审核证据。从观察控制的实施结果[例如，由恰当的授权人员为指定人员签署的访问权文件、处理事件的记录、由恰当的授权人员签署的处理权限文件、管理（或其他）会议的纪要等等]，可以收集到证据。证据可以是审核员对控制进行直接测试（或重新实施）的结果，例如：尝试执行被控制所禁止的任务、确定机器上是否安装了反恶意代码的软件且其是否是最新的、确定已授予的访问权（在检查完授权之后）等等。通过与在组织控制下工作的人员和（或）合同方就过程和控制进行面谈，确定其所说的是否真实正确，可以收集审核证据。

D.2 如何使用表 D.1

D.2.1 总则

表 D.1 为在初次认证审核和后续审核中评审 GB/T 22080—2016 附录 A 所列出的控制的实现，以及收集与控制的绩效相关的审核证据提供了指南。表 D.1 没有为评审 GB/T 22080—2016 附录 A 之外的控制提供指南。

D.2.2 “组织类控制”列与“技术类控制”列

各列中的“×”表示对应的控制是组织类控制或技术类控制。如果某些控制既是组织类的又是技术类的，则两列中均予以标识。

组织类控制的绩效证据，可以通过核查控制的实施记录、访谈、观察和物理检查来收集。技术类控制的绩效证据，可以通过系统测试（见下面），或者通过使用专门的审核/报告工具来收集。

D.2.3 “系统测试”列

“系统测试”是指对信息系统的直接评审（例如，评审系统的设置或配置）。对于审核员的提问，可以在系统控制台回答，也可以通过评价测试工具的结果来回答。如果客户使用了一个审核员熟悉的、基于计算机的工具，那么可以使用该工具来支持审核，或者评审由客户（或其分包方）所实施的评价的结果。

表 D.1 包含了两类对技术类控制的评审：

- “可能的”：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”：在 ISMS 审核中，系统测试通常是必需的。

注：在本附录中，除非另有所指，“系统”是指“信息系统”。

D.2.4 “目视检验”列

“目视检验”是指通常需要通过在现场进行目视检验来评价控制的有效性。这意味着,通过评审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现场对控制进行验证。

D.2.5 “审核的评审指南”列

作为对审核员的进一步指南,“审核的评审指南”列为评价控制提供了可能的关注点。

表 D.1 控制的分类

GB/T 22080—2016 附录 A 的控制	组织类控制	技术类控制	系统测试	目视检验	审核的评审指南
A.5 信息安全策略					
A.5.1 信息安全管理指导					
A.5.1.1 信息安全策略	×				
A.5.1.2 信息安全策略的评审	×				
A.6 信息安全组织					
A.6.1 内部组织					
A.6.1.1 信息安全的角色和责任	×				
A.6.1.2 职责分离	×				
A.6.1.3 与职能机构的联系	×				
A.6.1.4 与特定相关方的联系	×				
A.6.1.5 项目管理中的信息安全	×				
A.6.2 移动设备和远程工作					
A.6.2.1 移动设备策略	×	×	可能的		适当时,还检查策略的实施
A.6.2.2 远程工作	×	×	可能的		适当时,还检查策略的实施
A.7 人力资源安全					
A.7.1 任用前					
A.7.1.1 审查	×				
A.7.1.2 任用条款及条件	×				
A.7.2 任用中					
A.7.2.1 管理责任	×				
A.7.2.2 信息安全意识、教育和培训	×				询问员工是否知道他宜知道的特定事项
A.7.2.3 违规处理过程	×				
A.7.3 任用的终止和变更					
A.7.3.1 任用终止或变更的责任	×				
A.8 资产管理					
A.8.1 有关资产的责任					

表 D.1（续）

GB/T 22080—2016 附录 A 的控制	组织类控制	技术类控制	系统测试	目视检验	审核的评审指南
A.8.1.1 资产清单	×				识别资产
A.8.1.2 资产的所属关系	×				
A.8.1.3 资产的可接受使用	×				
A.8.1.4 资产归还	×				
A.8.2 信息分级					
A.8.2.1 信息的分级	×				适当时，还检查策略的实施
A.8.2.2 信息的标记	×				命名：目录、文件、印好的报告、记录介质（例如，磁带、磁盘和CD）、电子消息和文件传输
A.8.2.3 资产的处理	×				
A.8.3 介质处理					
A.8.3.1 移动介质的管理	×	×	可能的		
A.8.3.2 介质的处置	×			×	处置过程
A.8.3.3 物理介质的转移	×				物理防护
A.9 访问控制					
A.9.1 访问控制的业务要求					
A.9.1.1 访问控制策略	×				适当时，还检查策略的实施
A.9.1.2 网络和网络服务的访问	×				适当时，还检查策略的实施
A.9.2 用户访问管理					
A.9.2.1 用户注册和注销	×				
A.9.2.2 用户访问供给	×	×	可能的		抽取有系统访问授权的、在组织控制下工作的人员/合同方
A.9.2.3 特许访问权管理	×	×	可能的		员工的内部调动
A.9.2.4 用户的秘密鉴别信息管理	×				
A.9.2.5 用户访问权的评审	×				
A.9.2.6 访问权的移除或调整	×				
A.9.3 用户责任					
A.9.3.1 秘密鉴别信息的使用	×				验证用户指南/策略的适宜性
A.9.4 系统和应用访问控制					
A.9.4.1 信息访问限制	×	×	推荐的		
A.9.4.2 安全登录规程	×	×	推荐的		
A.9.4.3 口令管理系统	×	×	推荐的		
A.9.4.4 特权实用程序的使用	×	×	推荐的		

表 D.1（续）

GB/T 22080—2016 附录 A 的控制	组织类控制	技术类控制	系统测试	目视检验	审核的评审指南
A.9.4.5 程序源代码的访问控制	×	×	推荐的		
A.10 密码					
A.10.1 密码控制					
A.10.1.1 密码控制的使用策略	×				适当时，还检查策略的实施
A.10.1.2 密钥管理	×	×	推荐的		适当时，还检查策略的实施
A.11 物理和环境安全					
A.11.1 安全区域					
A.11.1.1 物理安全边界	×				
A.11.1.2 物理入口控制	×	×	可能的	×	访问记录的存档
A.11.1.3 办公室、房间和设施的安全保护	×			×	
A.11.1.4 外部和环境威胁的安全防护	×			×	
A.11.1.5 在安全区域工作	×			×	
A.11.1.6 交接区	×			×	
A.11.2 设备					
A.11.2.1 设备安置和保护	×			×	
A.11.2.2 支持性设施	×	×	可能的	×	
A.11.2.3 布缆安全	×			×	
A.11.2.4 设备维护	×				
A.11.2.5 资产的移动	×				资产的带出记录
A.11.2.6 组织场所外的设备与资产安全	×	×	可能的		便携式设备加密
A.11.2.7 设备的安全处置或再利用	×	×	可能的	×	磁盘擦除，磁盘加密
A.11.2.8 无人值守的用户设备	×			×	适当时，还检查策略的实施
A.11.2.9 清理桌面和屏幕策略	×				适当时，还检查策略的实施
A.12 运行安全					
A.12.1 运行规程和责任					
A.12.1.1 文件化的操作规程	×				
A.12.1.2 变更管理	×	×	推荐的		
A.12.1.3 容量管理	×	×	可能的		
A.12.1.4 开发、测试和运行环境的分离	×	×	可能的		
A.12.2 恶意软件防范					
A.12.2.1 恶意软件的控制	×	×	推荐的		用于控制恶意软件的软件，其配置和覆盖范围的完整性
A.12.3 备份					

表 D.1（续）

GB/T 22080—2016 附录 A 的控制	组织类控制	技术类控制	系统测试	目视检验	审核的评审指南
A.12.3.1 信息备份	×	×	推荐的		评审策略，恢复测试
A.12.4 日志和监视					
A.12.4.1 事态日志	×	×	可能的		基于风险选择记入日志的事态
A.12.4.2 日志信息的保护	×	×	可能的		
A.12.4.3 管理员和操作员日志	×	×	可能的		
A.12.4.4 时钟同步		×	可能的		
A.12.5 运行软件控制					
A.12.5.1 运行系统软件的安装	×	×	可能的		
A.12.6 技术方面的脆弱性管理					
A.12.6.1 技术方面脆弱性的管理	×	×	推荐的		基于风险的、对运行系统/数据库和应用的补丁管理与加固
A.12.6.2 软件安装限制	×	×	可能的		
A.12.7 信息系统审计的考虑					
A.12.7.1 信息系统审计控制	×				
A.13 通信安全					
A.13.1 网络安全管理					
A.13.1.1 网络控制	×	×	可能的		网络管理
A.13.1.2 网络服务的安全	×	×	推荐的		SLAs，网络服务的信息安全要求（例如，VPN，网络路由与连接的控制，网络设备的配置）
A.13.1.3 网络中的隔离	×	×	可能的		网络拓扑图，网段（例如，VLAN）和网络隔离（例如，DMZ）
A.13.2 信息传输					
A.13.2.1 信息传输策略和规程	×				
A.13.2.2 信息传输协议	×				
A.13.2.3 电子消息发送	×	×	可能的		确认所抽取的消息符合策略/规程
A.13.2.4 保密或不泄露协议	×				合同评审
A.14 系统获取、开发和维护					
A.14.1 信息系统的安全要求					
A.14.1.1 信息安全要求分析和说明	×				
A.14.1.2 公共网络上应用服务的安全保护	×	×	推荐的		基于风险的应用服务设计
A.14.1.3 应用服务事务的保护	×	×	推荐的		保密性、完整性，不可抵赖性
A.14.2 开发和支持过程中的安全					

表 D.1（续）

GB/T 22080—2016 附录 A 的控制	组织类控制	技术类控制	系统测试	目视检验	审核的评审指南
A.14.2.1 安全的开发策略	×				适当时，还检查策略的实施
A.14.2.2 系统变更控制规程	×	×	推荐的		
A.14.2.3 运行平台变更后对应用的技术评审	×				
A.14.2.4 软件包变更的限制	×				
A.14.2.5 系统安全工程原则	×				
A.14.2.6 安全的开发环境	×	×	可能的		
A.14.2.7 外包开发	×				
A.14.2.8 系统安全测试	×				
A.14.2.9 系统验收测试	×	×	可能的		
A.14.3 测试数据					
A.14.3.1 测试数据的保护	×	×	可能的	×	
A.15 供应商关系					
A.15.1 供应商关系中的信息安全					
A.15.1.1 供应商关系的信息安全策略	×				适当时，还检查策略的实施
A.15.1.2 在供应商协议中强调安全	×				测试某些合同条件
A.15.1.3 信息与通信技术供应链	×				测试某些合同条件
A.15.2 供应商服务交付管理					
A.15.2.1 供应商服务的监视和评审	×				
A.15.2.2 供应商服务的变更管理	×				
A.16 信息安全事件管理					
A.16.1 信息安全事件的管理和改进					
A.16.1.1 责任和规程	×				
A.16.1.2 报告信息安全事态	×				
A.16.1.3 报告信息安全弱点	×				
A.16.1.4 信息安全事态的评估和决策	×				
A.16.1.5 信息安全事件的响应	×				
A.16.1.6 从信息安全事件中学习	×				
A.16.1.7 证据的收集	×				
A.17 业务连续性管理的信息安全方面					
A.17.1 信息安全的连续性					管理评审的纪要
A.17.1.1 规划信息安全连续性	×				
A.17.1.2 实现信息安全连续性	×				
A.17.1.3 验证、评审和评价信息安全连续性	×				

表 D.1（续）

GB/T 22080—2016 附录 A 的控制	组织类控制	技术类控制	系统测试	目视检验	审核的评审指南
A.17.2 冗余					
A.17.2.1 信息处理设施的可用性	×	×	可能的		
A.18 符合性					
A.18.1 符合法律和合同要求					
A.18.1.1 适用的法律和合同要求的识别	×		推荐的		
A.18.1.2 知识产权	×				
A.18.1.3 记录的保护	×	×	推荐的		
A.18.1.4 隐私和个人可识别信息保护	×				适当时,还检查策略的实施
A.18.1.5 密码控制规则	×				
A.18.2 信息安全评审					
A.18.2.1 信息安全的独立评审	×				浏览报告
A.18.2.2 符合安全策略和标准	×				
A.18.2.3 技术符合性评审	×	×			

附 录 NA
（资料性附录）
GB/T 25067—2020 与 GB/T 25067—2016 的条款对照关系

本标准与 2016 版的条款对照关系列于表 NA.1。

表 NA.1 GB/T 25067—2020 与 GB/T 25067—2016 的条款对照关系表

GB/T 25067—2020 章条号	对应 GB/T 25067—2016 章条号	主要变化说明
1 范围	1 范围	
2 规范性引用文件	2 规范性引用文件	1) 删除了 ISO 19011，新增了 ISO/IEC 27000； 2) 更新了 GB/T 22080 和 GB/T 27021.1 的版本
3 术语和定义	3 术语和定义	1) 所引用标准由 ISO/IEC 27000 代替 GB/T 22080—2008； 2) 删除了“证书”“认证机构”“标志”“组织”4 个术语，仅保留了术语“认证文件”
4 原则	4 原则	
5 通用要求	5 通用要求	
5.1 法律与合同事宜	5.1 法律和合同事宜	
5.2 公正性的管理	5.2 公正性的管理	在 5.2.1 中：1)删除了原“a)认证，包括信息沟通会议、……和不符合的跟踪；”；2)新增“认证机构不应为客户寻求认证的 ISMS 提供内部信息安全评审。”
5.3 责任和财力	5.3 责任与财力	
6 结构要求	6 结构要求	
7 资源要求	7 资源要求	
7.1 人员能力		
7.1.1 IS 7.1.1 总体考虑	7.1.1.1 能力分析和合同评审第 1 段	1) 第 2 段为新增； 2) 删除了原 7.1.1.1“认证机构应具有一个有效的能力分析系统，……进行分析。”
7.1.2 IS 7.1.2 能力准则的确定	● 7.2.1.1 审核组的培训/9.2.1 IS 9.2.1 审核组的能力 b)和 c)； ● 7.2.1.3.2 a)和 c)	1) 7.1.2.1.1 来自原 7.2.1.1 审核组的培训、原9.2.1 IS 9.2.1 审核组的能力的 b)和 c)； 2) 7.1.2.2 来自原 7.2.1.3.2 的 a)和 c)； 3) 除了 7.1.2.1.1 和 7.1.2.2 外，其余条款为新增条款，是对 GB/T 27021.1—2017 中表 A.1 的细化
7.2 参与认证活动的人员		
7.2.1 IS 7.2 证实审核员的知识和经验	● 9.2.1.1 IS 9.2.1.1 审核员能力的证实； ● 7.2.1.3.1 ISMS 审核员的必备条件； ● 7.2.1.3.2 ISMS 审核组长的条件 b)	7.2.1.1 a)由原“具备中等教育程度”调整为“具备相当于大学教育水平的专业教育或培训”

表 NA.1（续）

GB/T 25067—2020 章条号	对应 GB/T 25067—2016 章条号	主要变化说明
7.3 外部审核员和外部技术专家的使用		删除了原 7.3.1 IS 7.3 使用外部审核员或外部技术专家作为审核组的一部分
7.3.1 IS 7.3 使用外部审核员或外部技术专家作为审核组的一部分	7.3.1.1 技术专家的使用	
7.4 人员记录	7.4 人员记录	
7.5 外包	7.5 外包	
8 信息要求		
8.1 公开信息	8.1 可公开获取的信息	删除了原 8.1.1 IS 8.1 授予、维护……撤销认证的规程
8.2 认证文件		
8.2.1 IS 8.2 ISMS 认证文件	8.2.1 IS 8.2 ISMS 的认证文件	增加了“认证文件也可以包括对所用的特定行业标准的标识”
8.3 认证的引用和标志的使用	8.4 认证的引用和标志的使用	删除了原 8.4.1 IS 8.4 认证标志的控制
8.4 保密	8.5 保密性	
8.4.1 IS 8.4 组织记录的获取	8.5.1 IS 8.5 组织记录的访问	
8.5 认证机构与其客户间的信息交换	8.6 认证机构与其客户间的信息交换	
9 过程要求		
9.1 认证前的活动		
9.1.1 申请	8.1.1 IS 8.1 授予、维护、扩大、缩小、暂停和撤销认证的规程，第一段	
9.1.2 申请评审	9.2 初次审核和认证	
9.1.3 审核方案	● 9.1.5 IS 9.1.5 审核方法，第 2 段； ● 9.2.2 IS 9.2.2 初次审核的一般准备； ● 9.2.5 IS 9.2.5 认证决定，第 4 段； ● 9.1.2 IS 9.1.2 认证范围； ● 9.1.1.1 认证审核准则	1) 9.1.3.1 为新增条款； 2) 9.1.3.2 来自原 9.1.5 IS 9.1.5 审核方法的第 2 段； 3) 9.1.3.3 来自原 9.2.2 IS 9.2.2 初次审核的一般准备； 4) 9.1.3.4 来自原 9.2.5 IS 9.2.5 认证决定的第 4 段； 5) 9.1.3.5 来自原 9.1.2 IS 9.1.2 认证范围； 6) 9.1.3.6 来自原 9.1.1.1 认证审核准则，但删除了“如果需要对上述文件……，并由认证机构正式发布。”

表 NA.1（续）

GB/T 25067—2020 章条号	对应 GB/T 25067—2016 章条号	主要变化说明
9.1.4 确定审核时间	9.1.3 IS 9.1.3 审核时间	新增了对附录 B 和附录 C 的引用
9.1.5 多场所的抽样	9.1.4 IS 9.1.4 多场所	
9.1.6 多管理体系标准	● 9.2.3.3.2 ISMS 文件与其他管理体系文件的整合； ● 9.2.3.3.3 管理体系结合审核	1) 9.1.6.1 来自原 9.2.3.3.2 ISMS 文件与其他管理体系文件的整合； 2) 9.1.6.2 来自原 9.2.3.3.3 管理体系结合审核
9.2 策划审核		
9.2.1 确定审核目的、范围和准则		9.2.1.1，新增条款
9.2.2 选择和指派审核组	● 9.1.1.3 审核组； ● 7.2.1.1.1 为特定审核选派审核组	1) 9.2.2.1 来自原 9.1.1.3 审核组，但删除了有关审核组任务的要求； 2) 9.2.2.2 来自原 7.2.1.1.1
9.2.3 审核计划	● 9.1.5 IS 9.1.5 审核方法，第 3 段和注解； ● 附录 C C.3.2，第二段	1) 9.2.3.1 为新增条款； 2) 9.2.3.2 来自原 9.1.5 IS 9.1.5 审核方法学，第 3 段及其注解； 3) 9.2.3.3 来自原附录 C 中 C.3.2 的第二段
9.3 初次认证		
9.3.1 IS 9.3.1 初次认证审核	● 9.2.3.1 IS 9.2.3.1 第一阶段审核； ● 9.2.3.2 IS 9.2.3.2 第二阶段审核	
9.4 实施审核		
9.4.1 IS 9.4 总则	8.1.1 IS 8.1 授予、维护、扩大、缩小、暂停和撤销认证的规程，第 2 段～第 4 段	
9.4.2 IS 9.4 ISMS 审核的特定要素	9.2.3.3 IS 9.2.3.3 ISMS 审核的特定要素	
9.4.3 IS 9.4 审核报告	9.1.6 IS 9.1.6 认证审核报告	
9.5 认证决定		
9.5.1 IS 9.5 认证决定	9.2.5 IS 9.2.5 认证决定，第 2 段、第 3 段、第 5 段	
9.6 保持认证		
9.6.1 总则		
9.6.2 监督活动	9.3.1 IS 9.3 监督活动	删除了原 9.3.1 中与 GB/T 27021.1—2017 重复的内容，如监督审核方案由认证机构确定、监督要审查认证证书的使用等内容

表 NA.1（续）

GB/T 25067—2020 章条号	对应 GB/T 25067—2016 章条号	主要变化说明
9.6.3 再认证	9.4.1 IS 再认证审核	删除了原 9.4.1 中认证机构应对维护认证的环境和条件做出规定的规程、再认证不符合应在机构同意的时间内得到有效纠正等与 GB/T 27021.1—2017 重复的内容
9.6.4 特殊审核	9.5.1 IS 9.5 特殊情况	
9.6.5 暂停、撤销或缩小认证范围	9.6 暂停、撤销或缩小认证范围	
9.7 申诉	9.7 申诉	
9.8 投诉	9.8 投诉	
9.8.1 IS 9.8 投诉	9.8.1 IS 9.8 投诉	删除了原 9.8.1 中根据投诉调查结果制定补救或纠正措施等与 GB/T 27021.1—2017 重复的内容
9.9 客户的记录	9.9 申请者和客户记录	
10 认证机构的管理体系要求	10 认证机构的管理体系要求	
10.1 可选方式	10.3.1 IS 10.3 ISMS 实现	
10.2 方式 A：通用的管理体系要求	10.3 方式二：通用的管理体系要求	
10.3 方式 B：与 GB/T 19001 一致的管理体系要求	10.2 方式一：按照 GB/T 19001 的管理体系要求	
附录 A(资料性附录) ISMS 审核与认证的知识与技能	附录 B(资料性附录) 审核员能力的示例	1) A.1 概述为新增； 2) 删除了原 B.2.1 有关 GB/T 22080—2008 的附录 A 控制的知识
附录 B(规范性附录) 审核时间	附录 C(资料性附录) 审核时间	新增了审核时间计算原则，给出了审核时间的最大减少量
附录 C(资料性附录) 审核时间计算方法		新增附录
附录 D(资料性附录) 对已实现的 GB/T 22080—2016 附录 A 的控制的评审指南	附录 D(资料性附录) 对已实现的 GB/T 22080—2008 附录 A 的控制的评审指南	按照 GB/T 22080—2016 附录 A，更新了表 D.1
附录 NA(资料性附录) GB/T 25067—2020 与 GB/T 25067—2016 的条款对照关系	附录 NA(资料性附录) GB/T 25067—2016 与 GB/T 25067—2010 的主要技术差异	

参 考 文 献

[1] GB/T 19001—2016 质量管理体系 要求(ISO 9001:2015,IDT)

[2] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南(ISO/IEC 27002:2013,IDT)

[3] ISO 19011 Guidelines for auditing management systems

[4] ISO/IEC 27007 Information technology—Security techniques—Guidelines for information security management systems auditing

中 华 人 民 共 和 国
国 家 标 准
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
GB/T 25067—2020/ISO/IEC 27006:2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2020年4月第一版
*
书号:155066·1-64797

GB/T 25067-2020