



CNAS-CC12

信息安全管理体系认证机构要求
Requirements for bodies providing audit and
certification of information security management
systems
(ISO/IEC 27006:2007)

（征求意见稿）

（本稿完成日期：2007年11月13日）

中国合格评定国家认可委员会

目 录

引 言	4
信息安全管理机构要求	5
1 范围	5
2 规范性引用文件	5
3 术语和定义	5
4 原则	6
5 通用要求	6
5.1 法律与合同事宜	6
5.2 公正性的管理	6
5.3 责任和财力	6
6 结构要求	6
6.1 组织结构和最高管理层	6
6.2 维护公正性的委员会	6
7 资源要求	6
7.1 管理层和人员的能力	6
7.2 参与认证活动的人员	7
7.3 外部审核员和外部技术专家的使用	8
7.4 人员记录	8
7.5 外包	8
8 信息要求	8
8.1 可公开获取的信息	8
8.2 认证文件	9
8.3 获证客户目录	9
8.4 认证资格的引用和标志的使用	9
8.5 保密	9
8.6 认证机构与其客户间的信息交换	9
9 过程要求	9
9.1 通用要求	9
9.2 初次审核与认证	12
9.3 监督活动	14
9.4 再认证	15
9.5 特殊审核	15
9.6 暂停、撤销或缩小认证范围	15
9.7 申诉	15
9.8 投诉	15
9.9 申请组织和客户的记录	15
10 认证机构的管理体系要求	16
10.1 可选方式	16

10.2 方式一：与 GB/T 19001 一致的管理体系要求	16
10.3 方式二：通用的管理体系要求	16
附录 A（资料性附录） 客户组织复杂性和行业特定方面的分析	17
附录 B（资料性附录） 审核员能力范围的示例	19
附录 C（资料性附录） 审核时间	21
附录 D（资料性附录） ISO/IEC 27001 附录 A 控制措施评审指南	25

引 言

CNAS-CC01规定了对管理体系认证机构的认可要求。如果这些机构为按照ISO/IEC 27001:2005对信息安全管理体系（ISMS）实施审核与认证，而希望获得CNAS-CC01认可，则有必要在CNAS-CC01基础上增加相应的要求和指南。本文件提供了这些要求和指南。

本文件的正文采用了CNAS-CC01的结构，并用英文字母“IS”标识在ISMS认证中应用CNAS-CC01时增加的ISMS专用要求和指南。

在本文件中，术语“应”表示相应的条款是强制性的，反映了CNAS-CC01和ISO/IEC 27001的要求。术语“宜”表示相应的条款是对要求的应用指南，希望认证机构予以采纳。

本文件的一个目的是使认可机构更有效地协调一致地使用认证机构认可评审所依据的标准。因此，认证机构与本文件指南的任何差异属于例外情况。认可机构将本着具体情况具体分析的原则对这种差异进行处理，只有认证机构证实了例外情况以某种等效的方式满足ISO/IEC17021和ISO/IEC27001的相关要求和本文件的意图，才会允许这种差异。

注：本文件中，术语“管理体系”和“体系”可互换使用。管理体系的定义见ISO9000:2005。本文件中所述的管理体系不可与其他类型的体系（如信息技术体系）混淆。

信息安全管理体系认证机构要求

1 范围

本文件对信息安全管理体系（以下简称“ISMS”）审核和认证机构规定了要求并提供了指南，以作为对CNAS-CC01:2007和ISO/IEC 27001:2005中相关要求的补充。

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文件的要求。本文件的指南为这些要求提供了进一步的解释。

注：本文件可以作为认可、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

下列文件中的条款通过本文件的引用而成为本文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本文件，然而，鼓励根据本文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本文件。

CNAS-CC01:2007 管理体系认证机构要求

GB/T 19011 质量和（或）环境管理体系审核指南

ISO/IEC 27001:2005 信息技术—安全技术—信息安全管理体系—要求

3 术语和定义

CNAS-CC01:2007和ISO/IEC 27001:2005中给出的术语和定义以及下列术语和定义适用于本文件。

3.1

认证证书 certificate

由认证机构根据其认可条件颁发的，并带有认可标识或声明的一种文件。

3.2

认证机构 certificaion body

按照已发布的ISMS标准和该体系所要求的任何补充性文件，对客户组织的ISMS进行评定和认证的第三方。

3.3

认证文件 certification document

说明客户组织的ISMS符合规定的ISMS标准和该体系所要求的任何补充性文件。

3.4

标志 mark

依法注册的商标或在认可机构或认证机构的规则下颁发的受到保护的标识，显示对机构运行体系具有足够信心，或相关的产品或人员符合规定标准的要求。

3.5

组织 organization

有自身的职能和行政管理、能够确保信息安全得到落实的公司、集团、事务所、企事业单位、机关或团体，或上述单位的部分或组合。

4 原则

CNAS-CC01:2007第4章的原则适用。

5 通用要求

5.1 法律与合同事宜

认证机构应对与认证有关的决定（包括授予、保持、更新、扩大、缩小、暂停和撤销认证）负责，并应保持做出上述决定的权力。

CNAS-CC01:2007条款5.1的要求适用。

5.2 公正性的管理

CNAS-CC01:2007条款5.2的要求适用。另外，以下ISMS专用要求和指南适用。

5.2.1 IS 5.2 利益冲突

认证机构可以执行以下职责，而不被视为咨询或具有潜在的利益冲突：

- a) 认证，包括信息会议、策划会议、文件检查、审核（非 ISMS 内部审核或内部安全复核）和不合格的追踪。
- b) 作为讲师安排和参与培训课程，如果这些课程与信息安全管理、有关的管理体系或审核相关，认证机构宜仅限于提供公众领域可以免费获取的通用的信息和建议，例如：他们不宜提供针对特定公司的、违反下述 c) 的要求的建议；
- c) 在接到请求时，发布认证机构对认证审核标准要求的解释的说明信息，或使其可获得；
- d) 确定认证审核就绪的审核前的活动；但是，这类活动不宜提供违反本条款的建议或意见，并且认证机构宜能够确认这类活动不违反这些要求，及不使用这些活动来证明缩减最终认证审核时间的合理性；
- e) 根据标准或法规实施认可范围以外进行的第二方或第三方审核；
- f) 在认证审核和监督访问过程中增值，例如在审核过程中，当改进机会明显时，通过识别改进的机会而不推荐具体的解决方案来增值。

认证机构应独立于对将要认证的客户组织的ISMS提供ISMS内部审核的机构（包括任何个人）之外。

5.3 责任和财力

CNAS-CC01:2007条款5.3的要求适用。

6 结构要求

6.1 组织结构和最高管理层

CNAS-CC01:2007条款6.1的要求适用。

6.2 维护公正性的委员会

CNAS-CC01:2007条款6.2的要求适用。

7 资源要求

7.1 管理层和人员的能力

CNAS-CC01:2007条款7.1的要求适用。另外，以下ISMS专用要求和指南适用。

7.1.1 IS 7.1 管理层能力

实施 ISMS 认证所需能力的最基本要素是选择、提供和管理其技能和综合能力适合审核活动和相关信息安全问题的人员。

7.1.1.1 能力分析和合同评审

认证机构应确保了解所评审的客户 ISMS 有关的技术和法律发展的知识。

认证机构应根据其运作的全部技术领域，具备对其需提供信息安全管理能力分析的有效体系。

对于每个客户，认证机构在实施合同评审前，应能够证实其对每个相关行业的要求进行了能力分析（针对所评估出需求的技能评定）。然后，认证机构应在能力分析的基础上，与客户组织一起进行合同评审。特别地，认证机构应能够证明其具备完成以下活动的能力：

- a) 对客户组织的活动领域及相关业务风险的理解；
- b) 根据所识别的活动和与信息安全的对资产的威胁、脆弱性和对客户组织的影响来确定认证机构所需的能力；
- c) 确认所需能力的可用性。

7.1.1.2 资源

认证机构的管理应具备必要的过程和资源，以确定每个审核员是否能够胜任在其操作的认证范围所要求的工作。审核员的能力由已验证的背景经历和具体的培训或简历（见附录 B）制定。认证机构应能够与其提供服务的所有客户进行有效地沟通。

7.2 参与认证活动的人员

CNAS-CC01:2007条款7.2的要求适用。另外，以下ISMS专用要求和指南适用。

7.2.1 IS 7.2 认证机构人员的能力

认证机构应具备胜任以下工作的人员：

- a) 选择和验证适合审核的审核组内的 ISMS 审核员的能力；
- b) 对 ISMS 审核员进行简单介绍并安排必要的培训；
- c) 决定授予、保持、撤销、暂停、扩大或缩小认证；
- d) 建立和运行申诉和投诉过程。

7.2.1.1 审核组的培训

认证机构应具备培训审核组的准则，以确保：

- a) 对 ISMS 标准和相关规范性文件的了解；
- b) 对信息安全的理解；
- c) 从业务角度，对风险评估和风险管理的理解；
- d) 对受审活动的技术知识；
- e) 对与 ISMS 相关的法规要求的通用知识；
- f) 管理体系的知识；
- g) 对基于 GB/T 19011 的审核原则的理解；
- h) 对 ISMS 有效性评审和控制措施有效性测量的知识。

这些培训要求适用于审核组的所有成员，除了 d)可以在审核组成员之间分享。

7.2.1.1.1 当为具体认证审核选择指派审核组时，认证机构应确保的各项工作的技能是适宜的。审核组应：

- a) 具备要认证的 ISMS 范围内的特定活动的技术知识，以及适宜时，与这些活动相关的规程及其潜在的信息安全风险的技术知识（非审核员的技术专家可以行使此项职责）；
- b) 充分理解客户组织，以便对其 ISMS 在活动、产品和服务的管理信息安全方面进行可靠的认证审核；
- c) 对适用于客户组织的 ISMS 的法规要求的适当的理解。

7.2.1.1.2 如必要,审核组可以由能够证明在适宜于审核的技术领域具备特定能力的技术专家进行补充。值得注意的是,技术专家不能作为 ISMS 审核员使用,但可为审核员对正在接受审核的管理体系的技术充分性事宜提供建议。认证机构应具备程序:

- a) 依据审核员和技术专家的能力、接受的培训、资格和经历,选择审核员和技术专家;
- b) 在认证审核中,初次对审核员和技术专家的行为进行评审,而后对审核员和技术专家的绩效进行监视。

7.2.1.2 决定过程的管理

管理职责应具备技术能力和根据 ISO/IEC 27001 的要求,对授予、保持、扩大、缩小、撤销和暂停 ISMS 认证决定过程进行管理的能力。

7.2.1.3 ISMS 审核员必备的教育、工作经历、审核员培训和审核经历

7.2.1.3.1 以下准则适用于 ISMS 审核组中的每个审核员。审核员应:

- a) 具备中等教育程度;
- b) 在信息技术方面具备至少 4 年的全职实际工作经历,其中具备至少 2 年与信息安全有关的职位或职责的工作经历;
- c) 成功地完成 5 天的培训,包括 ISMS 审核和审核管理在内的培训范围被认为是适宜的;
- d) 在作为审核员行使职责之前,已获得评审信息安全整个过程的经验。这种经验宜通过参与最少 4 次、总共天数为 20 天认证审核获得,包括文件评审和风险分析,实施评审和审核报告;
- e) 具备时宜的工作经历;
- f) 能够宏观地观察复杂的运行,并理解各单元在更大的客户组织中的职能;
- g) 通过持续的专业发展,保持信息安全和审核知识和技能的更新。

技术专家应遵守准则 a), b), e) 和 f)。

7.2.1.3.2 除了 7.2.1.3.1 中的要求,审核组组长应满足以下要求。这些要求应在指导和监督下进行的审核中得到证明的:

- a) 具备管理认证审核过程的知识和素质;
- b) 至少具有一名实施过 3 次完整 ISMS 认证审核的审核员;
- c) 证明具备口头和书面的有效沟通的能力。

7.3 外部审核员和外部技术专家的使用

CNAS-CC01:2007 条款 7.3 的要求适用。另外,以下 ISMS 专用要求和指南适用。

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

当使用外部审核员或外部技术专家作为审核组成员时,认证机构应确保其能够胜任及遵守本文件适用的规定,并不以直接或通过其雇主参与对 ISMS 或相关管理体系的设计、实施或维护的方式使以公正性受到威胁。

7.3.1.1 技术专家的使用

具有有关影响客户组织的过程和信息安全问题与法律方面的特定知识,但未必满足 7.2 的所有准则的技术专家,可以成为审核组成员。技术专家应在审核员的监督下进行工作。

7.4 人员记录

CNAS-CC01:2007 条款 7.4 的要求适用。

7.5 外包

CNAS-CC01:2007 条款 7.5 的要求适用。

8 信息要求

8.1 可公开获取的信息

CNAS-CC01:2007 条款 8.1 的要求适用。另外,以下 ISMS 专用要求和指南适用。

8.1.1 IS 8.1 授予、保持、扩大、缩小、暂停和撤消认证的程序

认证机构应要求客户组织建立并实施文件化的ISMS，并符合ISO/IEC27001的要求和认证所需其他文件的要求。

认证机构应具备形成文件的程序，以便

- a) 根据 GB/T 19011 和 CNAS-CC01:2007 及其他相关文件的规定，对客户组织 ISMS 进行初次认证审核；
- b) 根据 GB/T 19011 和 CNAS-CC01:2007，对客户组织 ISMS 定期进行监督和再认证审核，**以确保其持续符合相关要求，并验证和记录客户组织及时采取纠正措施以纠正所有不符合的情况。**

8.2 认证文件

CNAS-CC01:2007条款8.2的要求适用。另外，以下ISMS专用要求和指南适用。

8.2.1 IS 8.2 ISMS 的认证文件

认证机构应向ISMS获证的每个客户组织提供认证文件，例如信函或由负责此项职责的人员签署的认证证书。对客户组织和认证覆盖的每个信息系统，这些文件应识别授予的认证范围和ISMS的标准ISO/IEC 27001:2005。另外，证书宜包括适用性声明的特定版本的引用。

8.3 获证客户目录

CNAS-CC01:2007条款8.3的要求适用。

8.4 认证资格的引用和标志的使用

CNAS-CC01:2007条款8.4的要求适用。另外，以下ISMS专用要求和指南适用。

8.4.1 IS 8.4 认证标志的控制

认证机构应对认证标志的所有权、使用权和显示方式进行适当的控制。如果认证机构授权使用标志来表明对ISMS的认证，认证机构宜确保客户组织仅使用由认证机构书面授权的规定标志。认证机构不应授权在产品上使用这一标志，或以表示产品合格的方式使用这一标志。

8.5 保密

CNAS-CC01:2007条款8.5的要求适用。另外，以下ISMS专用要求和指南适用。

8.5.1 IS 8.5 组织记录的获取

在认证审核之前，认证机构应要求客户组织报告是否有一些ISMS的记录由于包含保密性或敏感性的信息不能供审核组进行复核。认证机构应确定ISMS是否在缺少这些记录的情况下得到充分地审核。如果认证机构得出不对已识别的保密性或敏感性的信息进行复核就不能对ISMS进行充分审核这一结论，就应建议客户组织认证审核不能进行，直至获得适当的获取准许。

8.6 认证机构与其客户间的信息交换

CNAS-CC01:2007条款8.6的要求适用。

9 过程要求

9.1 通用要求

CNAS-CC01:2007条款9.1的要求适用。另外，以下ISMS专用要求和指南适用。

9.1.1 IS 9.1.1 ISMS 审核通用要求

9.1.1.1 认证审核准则

客户ISMS接受审核的准则应是ISMS标准ISO/IEC27001中提出的准则和与所实施的职能相关的认证所需的其他文件中的准则。如果要求将解释说明作为这些文件具体在认证方案中的应用，这样的解释说明应由相关及公正的、具备必要的技术能力的委员会或个人给出并由认证机构发布。

9.1.1.2 政策和程序

认证机构的文件应包括实施认证过程的政策和程序，其中包括检查ISMS认证所使用的文件的使用和应用，及审核和认证客户组织的ISMS程序。

9.1.1.3 审核组

应正式任命审核组并为其提供相应的工作文件。审核计划和日期应得到客户组织的同意。明确对审核组的任命，并使客户组织知悉，应要求审核组检查客户组织的结构、政策和程序，来确认这些满足与认证范围相关的所有要求，还应确认程序得到实施及为客户组织的ISMS提供信心。

9.1.2 IS 9.1.2 认证范围

审核组应针对所有适用的认证要求，对包含在限定范围内的客户组织的ISMS进行审核。认证机构应确保客户组织的ISMS的范围和界限，根据其业务特点、组织、所处地理位置、资产和技术得到清晰的限定。认证机构应确认，在ISMS范围内，客户组织说明了ISO/IEC27001:2005的1.2条款所陈述的要求。

认证机构应确保客户组织的信息安全风险评估和风险处理正确地反映其各种活动，并将其限定在ISMS标准ISO/IEC27001所限定的活动之内。认证机构应确认这些在客户组织的ISMS范围和适用性声明中得到反映。

认证机构应确保与不完全属于ISMS范围内的服务和活动的界面在接受认证的ISMS中得到说明，并包括在客户组织的信息安全风险评定中。对这种情况的举例是与其他机构的设备共享（例如：信息技术系统、数据库和通讯系统）。

9.1.3 IS 9.1.3 审核时间

认证机构应允许审核组有充裕的时间进行与初次审核、监督审核或再认证审核相关的所有活动。所分配的时间宜以下列因素为依据：

- a) ISMS 范围的大小（例如：所使用的信息系统的数量、员工的数量）；
- b) ISMS 的复杂程度（例如：信息系统的危险程度、ISMS 的风险状况），见附录 A；
- c) 在 ISMS 范围内进行的业务类型；
- d) 在实施 ISMS 各种不同组成部分（例如：已实施的控制、文件和/或过程控制、纠正/改进措施等）所应用技术的程度和多样性；
- e) 场所的数量；
- f) 先前已证明 ISMS 的绩效；
- g) 在 ISMS 范围内，外包的范围和所使用的第三方协议；
- h) 适于认证的标准和法规。

附录C提供对审核时间的指南。认证机构应准备好用于初次审核、监督审核和再认证审核的时间进行证实并证明其合理性。

9.1.4 IS 9.1.4 多场所

9.1.4.1 在ISMS范围内的多场所抽样决定应比用于质量管理体系的同样决定更加复杂。在客户组织拥有多个场所满足以下a)至c)的准则的情况，认证机构可以考虑使用以抽样为基础的方法进行多场所认证审核：

- a) 所有的场所在相同的 ISMS 下运行，它们被集中管理和审核并提交集中的管理评审；
- b) 所有的场所都包含在客户组织的 ISMS 内部审核方案中；
- c) 所有的场所都包含在客户组织的 ISMS 管理评审方案中。

9.1.4.2 希望使用以抽样为基础的方法的认证机构应具备程序，以确保以下：

- a) 初次的合同评审在最大程度上识别场所的差异，以便确定足够的抽样量。
- b) 由认证机构对具有代表性的场所进行抽样，考虑：
 - 1) 总部和其他场所的内部审核的结果；
 - 2) 管理评审的结果；
 - 3) 场所规模差异；
 - 4) 各场所进行的业务目的的差异；
 - 5) ISMS 的复杂程度；
 - 6) 各场所的信息系统的复杂程度；

- 7) 工作作业的差异;
 - 8) 所进行活动的差异;
 - 9) 与关键的信息系统或处理敏感信息的信息系统的潜在的相互作用;
 - 10) 任何不同的法律要求。
- c) 从客户组织的 ISMS 范围内所有场所中挑选具有代表性的样本。宜于通过判断性选择进行挑选, 以反映上述 b) 中罗列的因素以及某种随机要素。
 - d) 包含在遭受重大风险的 ISMS 里的每个场所由认证机构在认证之前进行审核。
 - e) 根据以上要求, 设计监督审核方案, 并在合理的时间内覆盖客户组织的所有场所或 ISMS 范围内的所有场所。
 - f) 无论是在总部还是其他单一场所, 在观察到不合格的情况, 纠正措施程序适用于包括在认证范围内的总部和所有场所。

下列 IS 9.1.5 表述的审核应说明客户组织总部的活动, 以确保单一的 ISMS 适用于所有场所, 并在运行层面交付集中管理。审核应说明上述所有问题。

9.1.5 IS 9.1.5 审核方法

认证机构应具备要求客户组织证明其确定了 ISMS 内部审核的时间, 方案和程序具备操作性并能够操作的程序。

认证机构的程序不宜预示 ISMS 实施的特殊方式或文件和记录的特殊格式。认证程序应重点确保客户组织的 ISMS 满足 ISO/IEC 27001 标准的要求及客户组织的方针和目标。

如适宜, 审核计划宜识别在审核中使用的网络支持的审核技术。

注: 网络支持的审核技术可包括, 例如电话会议、web 会议、互动式的基于 web 的沟通和远程的电子方式获取 ISMS 文件和访问过程。这种技术的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。

9.1.6 IS 9.1.6 认证审核报告

9.1.6.1 认证机构可以采用适合其需要的报告程序, 但这些程序最低限度应确保:

- a) 在离开客户组织场所前, 在审核组和客户组织管理者之间召开一次会议, 审核组在此场所提供
 - 1) 有关客户组织的 ISMS 是否符合特殊认证要求的书面或口头说明;
 - 2) 客户组织就审核发现及其根据提出问题的机会。
- b) 审核组向客户组织就关于客户组织的安全管理体系符合 ISMS 所有认证要求的审核发现提供审核报告。

9.1.6.2 审核报告宜提供以下信息:

- a) 包括文件评审摘要在内的审核说明;
- b) 客户组织信息安全风险分析的认证审核报告;
- c) 所使用的全部审核时间和分别用于文件评审、风险分析评定、现场评审和审核报告时间的详细说明;
- d) 后续的审核询问、挑选的基本原理和所采用的方法。

9.1.6.3 向认证机构提供的审核发现的审核报告应具备充足的详细情况, 有助于并支持认证决定, 包括:

- a) 审核包含的区域 (例如: 认证要求和接受审核的场所), 包括后续的重大审核跟踪和所使用的审核方法 (见 IS 9.1.5);
- b) 获得的观察, 正面的 (例如: 值得注意的特点) 和负面的 (例如: 潜在的不合格);
- c) 客观证据和不符合所引用的 ISMS 标准 ISO/IEC 27001 和认证所需的其他文件的要求支持的、已识别的任何不符合的详细情况;
- d) 对客户组织 ISMS 符合认证要求并清楚地说明不符合的意见, 适用性声明版本的引用, 及在适用的情况下, 与客户组织先前的认证审核结果的任何有用的对照。

完整的问卷、检查清单、观察、日志或审核员笔记可能构成完整的审核报告的一部分。如果使用这些方法，这些文件应提供给认证机构，作为支持认证决定的证据。在审核过程中，有关被评价样本的信息宜包含在审核报告或其他认证文件中。

报告应考虑客户组织所采用的内部组织和程序的充分性，以便对ISMS建立信心。

除了记录在ISO/IEC 27001:2005条款9.1.10中的要求，报告宜包括：

- 对 ISMS 内部审核和管理评审的信任度；
- 有关 ISMS 的实施和有效性的最重要的正面与负面观察的摘要；
- 关于是否授予客户组织 ISMS 认证的审核组的建议，以及支持该建议的信息。

9.2 初次审核与认证

CNAS-CC01:2007条款9.2的要求适用。另外，以下ISMS专用要求和指南适用。

9.2.1 IS 9.2.1 审核组的能力

除了7.2条款所列的要求之外，以下要求适用于认证评审。对于监督活动，只有与已安排的监督活动有关的要求适用。

以下要求适用于整个审核组。

- a) 在以下每个领域，至少应有一名审核组成员满足认证机构准则，在审核组内部负责：
 - 1) 管理审核组；
 - 2) 应用于 ISMS 的管理体系和过程；
 - 3) 在特定的信息安全领域，具备法律和法规要求方面的知识；
 - 4) 识别信息安全相关的威胁和事件趋势；
 - 5) 识别顾客组织的弱点并理解其发生的可能性，其影响及其减缓和控制；
 - 6) ISMS 的控制措施及其实施的知识；
 - 7) ISMS 的有效性评审和控制措施测量的知识；
 - 8) 有关和/或相关的 ISMS 的标准，行业最佳实践，安全方针和程序；
 - 9) 事件处理方法和业务持续性的知识；
 - 10) 有关有形和无形信息资产和影响分析的知识；
 - 11) 可能与安全相关或其安全性成为问题的当前技术的知识；
 - 12) 风险管理过程和方法的知识。
- b) 审核组应有能力将顾客组织 ISMS 中的安全事件迹象追溯到 ISMS 的相应要素。
- c) 审核组在上述项目上，应具有相当的工作经验和实际应用（这不意味着审核员需要信息安全所有领域的全面的经验，但整个审核组宜对被审核的领域具备充分的认识和经验）。

审核组可以由一名审核员组成，如果其满足上述a)的所有准则。

9.2.1.1 IS 9.2.1.1 审核员能力的证明

审核员应能够证明其具备上述知识和能力，例如：

- a) 认可的、特定的 ISMS 资格；
- b) 注册为审核员；
- c) 被批准的 ISMS 培训课程；
- d) 更新连续的专业发展记录；
- e) 通过见证审核员在实际客户系统的 ISMS 审核过程得到实际证明。

9.2.2 IS 9.2.2 初次审核的一般准备

认证机构应要求客户组织为认证审核的进行做好所有必要的安排，这些包括对以下活动的准备：为了认证审核、再认证审核和解决投诉问题而进行文件检查以及进入所有区域、使用记录（包括内部审核报告和信息安全独立评审报告）和访问人员。

在现场认证审核之前，至少应提供以下信息：

- a) ISMS 和其活动所涵盖的一般信息；

b) ISO/IEC 27001:2005 条款 4.3.1 所要求的 ISMS 文件的复印件, 及必要的相关文件。

9.2.3 IS 9.2.3 初次认证审核

9.2.3.1 IS 9.2.3.1 第一阶段审核

在这个阶段, 认证机构应获取设计 ISMS 的文件, 并包括 ISO/IEC 27001 条款 4.3.1 所要求的文件。

第一阶段审核的目的是, 通过理解以客户组织 ISMS 方针和目标为背景的 ISMS, 特别是客户组织准备审核的状态, 为策划第二阶段的审核提供重点。

第一阶段审核包括, 但不宜仅限于文件评审。认证机构应与客户组织就文件评审的时间和地点达成一致。在所有情况下, 文件评审应在第二阶段审核开始前完成。

第一阶段审核结果应形成书面报告。认证机构应在决定进行第二阶段审核前, 对第一阶段的审核报告进行复核, 以便挑选具有必要能力的第二阶段的审核组成员。

认证机构应让客户组织意识到在第二阶段的审核中, 可以需要其他类型的信息和记录。

9.2.3.2 IS 9.2.3.2 第二阶段审核

9.2.3.2.1 第二阶段审核经常以客户组织的场所进行。认证机构以第一阶段的审核报告中的形成文件的审核发现为基础, 起草实施第二阶段审核的审核计划。第二阶段审核的目标是:

- a) 确认客户组织遵守自身的方针、目标和程序;
- b) 确认 ISMS 符合规范性 ISMS 标准 ISO/IEC 27001 的要求并实现客户组织的方针目标。

9.2.3.2.2 为达到此目标, 审核应重点关注客户组织:

- a) 信息安全有关风险的评估, 及此评定产生的可比较和可重现的结果;
- b) ISO/IEC 27001:2005 条款 4.3.1 所列的文件要求;
- c) 在风险评定和风险处理过程的基础上, 对控制目标和控制的选择;
- d) ISMS 有效性的评审和信息安全控制有效性的测量, 以及根据 ISMS 目标进行报告和复核;
- e) ISMS 内部审核和管理评审;
- f) 信息安全方针的管理职责;
- g) 所选择和实施的控制、适用性声明与风险评定和风险处理过程的结果及 ISMS 方针和目标之间的对应关系;
- h) 控制的实施(见附录 D), 考虑客户组织对控制的有效性的测量[见上述 d)], 确定控制是否得以实施并有效以到达所述的目标;
- i) 方案、过程、程序、记录、内部审核和对 ISMS 有效性的复核, 以确保其追踪至管理决定和 ISMS 的方针和目标。

9.2.3.3 IS 9.2.3.3 ISMS 审核的特定要素

认证机构的责任确定客户组织在制定和保持有关识别、检查和评价信息安全相关资产威胁、弱点和对客户组织影响的程序方面是否一致。认证机构应:

- a) 要求客户组织证明安全相关的威胁的分析与客户组织的运行是相关并充分的;
注: 客户组织负责确定该客户组织据以识别重大信息安全相关风险的准则, 并制定相应的程序。
- b) 确定客户组织识别、检查和评价信息安全相关资产威胁、弱点和影响的程序和应用的的结果是否与客户组织的方针、目标和目的保持一致。

认证机构也应确定用于重要性分析的程序是否健全并正确实施。如果信息安全相关资产威胁、弱点或对客户组织的影响被识别为重要时, 它应纳入 ISMS 管理之中。

9.2.3.3.1 遵守法律和法规

法律法规合规性的保持和评价是客户组织的责任。认证机构应限于检查和抽样, 以对 ISMS 在此方面的运作建立信心。认证机构应验证客户组织具有管理体系, 以达到对适用于信息安全风险和影响的法律法规的遵守。

9.2.3.3.2 ISMS 文件与其他管理体系文件的整合

客户组织可以将ISMS文件与其他管理体系文件（例如：质量、健康与安全，和环境）相结合，只要ISMS能够清楚地识别与其他体系的适宜的界面。

9.2.3.3 结合管理体系审核

认证机构可以提供与ISMS有关的其他管理体系认证，或仅提供ISMS认证。

ISMS审核可以和其他管理体系的审核相结合。这种结合只有在证明审核满足ISMS认证所有要求时才有可能。在审核报告中，对ISMS重要的所有要素应清晰地呈现并易于识别。审核的质量不应受到结合审核的负面影响。

注：GB/T 19011为进行结合管理体系的审核提供指南。

9.2.4 IS 9.2.4 授予初次认证的信息

为提供认证决定的基础，认证机构应要求提供做出认证决定的充分信息的、清晰的报告。

要求审核组在认证审核过程的各个阶段向认证机构提供的报告。结合存档信息，这些报告至少宜包括IS 9.1.6要求的信息。

9.2.5 IS 9.2.5 认证决定

在认证机构中，决定授予/撤销认证的实体（或个人）宜在所有方面具备足以评价审核过程和由审核组提供的相关建议的、相当的知识和经验。

是否授予客户组织ISMS认证的决定是由认证机构以认证过程中收集的信息和其他相关信息为基础做出的。负责做出认证决定的人员不应参与审核。审核决定应以审核组审核报告中审核发现和认证建议，及认证机构获取的任何其他相关信息为基础。

负责做出授予认证决定的实体在正常情况下，不宜推翻审核组的负面建议。如果出现这种情况，认证机构应记录和说明决定推翻建议的依据。

关于认证的决定，CNAS-CC01:2007未提及客户组织至少进行一次完整的ISMS内部审核和客户组织ISMS的管理评审的特定的时间间隔。认证机构可以具体说明时间间隔。无论认证机构是否选择指定最低的频次，认证机构应制定测量方法，以确保客户组织的管理评审和ISMS内部审核过程的有效性。

不对客户组织授予认证，直至具备充分的证据证明管理评审和ISMS内部审核的安排得以实施，且是有效的并将得到保持。

9.3 监督活动

CNAS-CC01:2007条款9.3的要求适用。另外，以下ISMS专用要求和指南适用。

9.3.1 IS 9.3 监督活动

9.3.1.1 监督审核过程应与本文件中表述的有关客户组织ISMS的认证审核的规定保持一致。

监督的目的是为了验证已被批准的ISMS继续实施，考虑由于客户组织的运行变化造成体系的变化并确保对认证要求的持续遵守。监督方案通常宜包括：

- a) 内部 ISMS 审核、管理评审和预防和纠正措施的体系维护要素；
- b) 根据 ISMS 标准 ISO/IEC27001:2005 和其他认证所需的文件的要求，与外部人员的沟通；
- c) 形成文件的体系的变更；
- d) 受这种变更影响的区域；
- e) ISO/IEC27001:2005 中所选择的要素；
- f) 适宜时，其他所选择的领域。

9.3.1.2 认证机构的监督至少要对以下进行复核：

- a) ISMS 在达到客户组织信息安全方针目标方面的有效性；
- b) 定期评价和对相关信息安全法律法规的遵守进行复核的程序运行；
- c) 针对前次审核中已识别的不符合采取的措施。

9.3.1.3 认证机构的监督至少宜包括ISO/IEC 27001:2005中对监督审核的几点要求，另外，宜考虑以下问题：

- a) 认证机构宜使其监督方案适应信息安全问题有关的资产威胁、弱点和对客户组织的影响，并证明方案正确；
- b) 认证机构的监督方案宜由认证机构确定。访问的具体日期可与被认证的客户组织达成协议；
- c) 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有关的方面；
- d) 要求认证机构对认证证书的使用进行监督。

在监督审核过程中，认证机构应向认证机构提交的申诉和投诉记录，在发现任何不符合或无法满足认证要求的情况，客户组织已调查其自身的ISMS和程序，并采取适当的纠正措施。

监督报告应包括，特别是排除先前所揭示的不符合的信息。由监督所产生的包括至少宜包含上述a)的所有要求。

9.4 再认证

CNAS-CC01:2007条款9.4的要求适用。另外，以下ISMS专用要求和指南适用。

9.4.1 IS 9.4 再认证审核

再认证审核程序应与本文件中表述的有关客户组织ISMS的认证审核的规定保持一致。

认证机构应具备清楚的程序，规定保持认证的环境和条件。如果在监督或再认证审核中，发现不符合存在，该不符合在认证机构同意的时间内应得到有效地纠正。如果纠正没有在同意的时间内进行，认证范围应被缩小，或暂停或撤销认证。允许采取纠正措施的时间宜与不符合的严重程度和风险相当，以确保客户组织的产品或服务满足规定要求的。

9.5 特殊审核

CNAS-CC01:2007条款9.5的要求适用。另外，以下ISMS专用要求和指南适用。

9.5.1 IS 9.5 特殊情况

如果已经通过ISMS认证的客户组织对其体系做重大修改或者如果发生影响其认证基础的其他变更，应该按照特别规定进行监督活动。

9.6 暂停、撤销或缩小认证范围

CNAS-CC01:2007条款9.6的要求适用。

9.7 申诉

CNAS-CC01:2007条款9.7的要求适用。

9.8 投诉

CNAS-CC01:2007条款9.8的要求适用。另外，以下ISMS专用要求和指南适用。

9.8.1 IS 9.8 投诉

投诉代表着有关可能的不符合的信息来源。认证机构宜要求获证客户在收到投诉后，确定投诉的原因，适宜时报告投诉原因，包括在客户组织ISMS中的预先确定（预先处理）的因素。

认证机构宜对客户组织使用调查以制定补救/纠正措施感到满意，其中包括以下措施以：

- a) 如法规要求时，通知适当的职权机构；
- b) 恢复符合性；
- c) 防止再发生；
- d) 评价和减小任何负面的安全事件和相关的的影响；
- e) 确保与其他 ISMS 组成部分的令人满意的互动；
- f) 评定所采用的补救/纠正措施的有效性。

认证机构应要求每个获证客户组织在接到请求时，根据ISO/IEC 27001要求提供所有投诉和所采取的纠正措施的记录。

9.9 申请组织和客户的记录

CNAS-CC01:2007条款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

CNAS-CC01:2007条款10.1的要求适用。

10.2 方式一：与 GB/T 19001 一致的管理体系要求

CNAS-CC01:2007条款10.2的要求适用。

10.3 方式二：通用的管理体系要求

CNAS-CC01:2007条款10.3的要求适用。另外，以下ISMS专用要求和指南适用。

10.3.1 IS 10.3 ISMS 实施

建议认证机构按照ISO/IEC 27001要求实施ISMS。

附录 A

(资料性附录)

客户组织复杂性和行业特定方面的分析

A.1 组织的潜在风险

当决定审核的时间和审核员的能力时，需要考虑客户组织的复杂性。本附录旨在提供分析客户组织复杂性的实例。

赋予 ISMS 范围复杂性的类别可用于确定：

- a) ISMS 审核的审核员能力要求（实例见附录 B）；
- b) ISMS 审核的审核时间要求（实例见附录 C）。

表 A.1 列出了决定 ISMS 范围复杂性可能因素的一般情况。对于特定的环境，表 A.1 可能需要加以修改，或者适当地增加一些特殊因素。

如果单独使用复杂性准则（见下表 A.1），可通过使用几个不同的因素，将 ISMS 范围复杂性分为三个类别：“高”、“中”和“低”。可将所有因素的最大类别作为是整体的有效类别，输出结果就是这个类别，即：“高”、“中”或“低”。

表 A.1 ISMS 范围复杂性准则

复杂性因素	类别			重要性
	高	中	低	
员工+签约人员的数量	>=1000	>=200	<200	<ul style="list-style-type: none"> ● ISMS 实施的规模 ● 管理信息系统 ● 生产管理相关的系统 ● 销售/物流/一般服务相关的系统 ● 信息技术/信息服务和相关系统 ● 建筑/造船/设备工程相关的系统
用户数量	>=1,000,000	>=200,000	<200,000	<ul style="list-style-type: none"> ● 财务系统 ● 政府、学校、医学/医院系统
场所数量	>=5	>=2	1	<ul style="list-style-type: none"> ● ISMS 实施的规模 ● 物理与环境安全（ISO/IEC 27001 A.9）
服务器数量	>=100	>=10	<10	<ul style="list-style-type: none"> ● ISMS 实施的规模 ● 物理与环境安全（A.9） ● 访问控制（ISO/IEC 27001 A.11） ● 通信与操作管理（ISO/IEC 27001 A.10）
工作站+PC+笔记本的数量	>=300	>=50	<50	<ul style="list-style-type: none"> ● 访问控制（ISO/IEC 27001 A.11）
应用开发与维护人员的数量	>=100	>=20	<20	<ul style="list-style-type: none"> ● 信息系统的获取、开发和维护（ISO/IEC 27001 A.12）
网络与加密技术	具有加密/数字签名/PKI 要求	具有使用标准加密设施，	无加密/数字签名/PKI 要	<ul style="list-style-type: none"> ● 通信与操作管理（A.10） ● 访问控制（ISO/IEC 27001 A.11）

复杂性因素	类别			重要性
	高	中	低	
	的外部/互联网连接	无数字签名/PKI 要求的外部/互联网连接	求的外部/互联网连接	
法律符合性的重要性	不符合导致起诉的	不符合导致重大的经济处罚或者信誉损害	不符合导致无关紧要的经济处罚或者信誉损害	● 法律和指南 (ISO/IEC 27001 A.15)
行业特定风险的适用性(参见附录 A.2 行业特定的风险和行业特定的法律和规定的示例)	有适用的行业特定的法律和规定	没有适用的行业特定的法律规定,但有重大的行业特定风险	没有适用的行业特定的法律规定,也没有重大的行业特定风险	● ISMS 实施的规模 ● 法律和指南 (ISO/IEC 27001 A.15)

A.2 信息安全风险中的行业特定类别

信息风险可能对于考虑的信息类型或组织的运行部门来说是特殊的。下列示例阐述了风险考虑的不同类别。

应用于所有组织的特殊类别：

- 工资、养老金、健康安全、组织档案、内部和部门间的信息等
- 任何其他个人可确认的信息
- 任何其他商业敏感/关键信息，例如研发信息、设计信息、客户详细信息、财务结果与预测、商业计划、知识产权、制造过程等。

政府敏感/关键信息：

- 公众信息
- 电子政务应用
- 市民持有信息（例如健康、救济金、税金、档案等）
- 政府的供应商和生产商持有的信息，例如 ICT 设计、设施、产品、服务等等。

应用于组织级别的特殊类别：

- 公司治理——列出的公司（可能也有其他大的实体）

应用于业务部门的特殊类别：

- 卫生保健
- 教育
- 航空宇宙
- 电信
- 金融服务
- 慈善和非盈利组织

附 录 B
(资料性附录)
审核员能力范围的示例

B.1 需考虑的一般能力

有很多途径可以证实审核员的知识和经验。例如，使用承认的资格可以证实知识和经验。注册，例如在审核员注册机构或其他任何得倒认可的审核员注册形式下的注册，也可以用来证明需要的知识和经验。最好对审核组要求的能力级别做出规定，使之与组织的行业/技术领域和复杂性因素对应。

B.2 需考虑的特殊能力**B.2.1 ISO/IEC 27001 附录 A 控制措施的知识**

下面描述与 ISMS 审核相关的典型知识。除了下表列出的 ISO/IEC 27001 控制领域外，审核员也应知晓 27000 族标准的其他标准。

信息安全方针政策，业务要求的知识和经验	安全方针
业务过程、实践和组织结构的一般知识和经验	信息安全组织
资产评估、清单、分类和允许使用策略的知识	资产管理
人力资源部所使用的过程与规程的一般知识和经验	人力资源安全
物理和环境安全的知识	物理和环境安全
在信息安全(包括管理测量以及专门技术的适当级别)方面所使用的标准、过程、技术和方法的最新知识和经验，这包括当前一些公共业务实践的知识。	通信和操作管理
	访问控制
	信息系统获取、开发和维护
事件管理的过程和规程的最新知识和经验	信息安全事件管理
关于业务连续性的标准、过程、计划和测试规程的最新知识和经验	业务连续性管理
与 ISMS 有关的业务合同问题、公共法律法规的最新知识	符合性

B.2.2 有关 ISMS 的典型知识

审核员宜具备知识，掌握下列审核和 ISMS 的内容：

- 编制审核方案和计划
- 审核类型和方法
- 审核风险
- 信息安全过程分析
- 持续改进的循环周期 (PDCA)
- 信息安全内部审核

审核员宜具备知识，掌握下列法规的要求：

- 知识产权
- 组织记录的内容、保护和保持
- 数据保护与隐私
- 密码控制措施的规则
- 反恐

- 电子商务
- 电子和数字签名
- 工作场所监督
- 通讯侦听与数据监视（如，电子邮件）
- 计算机滥用
- 电子证据收集
- 渗透测试
- 国际和国家部门的特殊要求（例如银行）

审核员应具备知识，掌握下列管理的要求：

- 信息安全风险的处理
- ICT 外包的安全风险
- 供应链信息安全风险

附 录 C
(资料性附录)
审核时间

C.1 绪论

本附录包含了与 ISO 17021 中 9.1、9.2、9.3 和 9.4 有关的进一步的信息。宜将其与 IS 9.1.2、IS9.1.3、IS9.1.5 和 IS9.1.6 以及 IS9.2.3.1、IS9.2.3.2 和 IS9.2.3.3 结合在一起阅读。本附录为开发根据不同规模和复杂度的客户组织 ISMS 范围确定自身审核时间的规程的认证机构提供了指南。

认证机构需要针对每一个申请者和被认证的 ISMS 识别初次审核、监督审核和复评所花费的审核时间。在制定审核计划阶段使用本附录，可以确保在确定适当审核时间时方法的一致性。同时，本附录给出的指南允许按照审核过程（尤其是 1 阶段审核）中的发现和考虑的 ISMS 范围的复杂性进行调整。

C.2 确定审核时间的程序

经验已经表明 ISMS 的范围、员工的数量（见下面 C.3 中的审核时间表）、规模、特性、复杂性和潜在信息安全风险的严重性（下面将更加详细的解释）将支配所有给定的 ISMS 审核的时间长短。IS9.1.3 和 IS9.2.3.1、IS9.2.3.2 以及 IS9.2.3.3 列出了准则，当确定所需的审核时间长短时宜考虑。需要在认证机构合同评审过程中对这些准则以及其他因素对分配的审核时间的潜在影响予以检查。

需要注意的是，当确定审核时间，宜考虑所有这些因素，附录 C.3 中的审核时间表不能单独使用。下列示例证明了能影响审核时间的因素，并详细描述了 IS9.1.3 给定的因素列表：

- 与 ISMS 范围大小相关的因素（例如使用的信息系统的数量、处理的信息的容量、用户的数量、特权用户的数量、IT 平台的数量、网络的数量及他们的规模）；
- 与 ISMS 复杂性相关的因素（例如信息系统的关健度、ISMS 的风险情况、操作和处理的敏感和关键信息的多少及类型、电子交易的数量及类型、所有开发项目的数量和规模、远程工作的范围、ISMS 文档的范围）；
- 在 ISMS 范围内执行的业务的类型，以及关于这些业务类型的安全、法律法规、合同和业务要求；
- 在 ISMS 各种组件的实施过程中使用的技术的范围和多样性（例如实施的控制措施、文档和/或过程控制、纠正/预防措施、信息系统、IT 系统、网络等等，无论他们是固定的、移动的、无线的、外部的或内部的）；
- ISMS 范围内场所的数量、这些场所的异同、所有的场所都审核还是抽样审核；
- ISMS 先前证明的执行效率；
- ISMS 范围内使用的外包和第三方安排的范围，以及对这些服务的依赖性；
- 可能应用于认证、行业特定要求的标准、法规和规章。

由于 ISMS 的特殊需求增加的要求，ISMS 的认证通常要比质量管理体系或环境管理体系花费更多的时间，例如 ISMS 方针、风险管理、ISMS 控制目标和控制措施。认证机构需要：

- a) 审核客户组织决定其信息安全风险和影响严重性所使用的方法的完备性和一致性；
- b) 确认所设计的系统能达到合规性（所有相关的法规和其他适用于 ISMS 的要求）的体系有能力做到这一点，并且这个体系正在被实施和保持；
- c) 确认正确选择和实施了控制目标和控制措施、测量其有效性，实现“对安全失效的预防和适当的响应”的过程是完备且始终遵守的；
- d) 确认满足客户组织 ISMS 的文档要求；

e) 源于 1 阶段审核所增加的需求。

C.3 审核时间表

C.3.1 审核时间表

下面提供的审核时间表给出了初次审核时间的平均数量（此处及后面的内容中，这个数量包括 1 阶段和 2 阶段审核的时间），经验表明对于给定员工数量的 ISMS 范围来说是适当的。经验还表明一个类似大小的 ISMS 范围，有些需要多一些时间，有些需要少一些时间。

认证时间的变化依赖于因素的数量，包括规模、审核范围、后勤、组织的复杂性和审核准备状态（也见上面的 C.2）。需要在认证机构合同评审过程中对这些准则以及其他因素对分配的审核时间的潜在影响予以检查。因此，审核时间表不能单独使用。

基于所有轮班员工的总数量识别起点，下面的审核时间表提供了用于审核计划的框架。基于被审核的 ISMS 范围的适用因素的重要性以及每一个因素的属性对时间表进行调整，增加或减少权重来修改这些基本数字。本表中用到的术语在下面 C.3.2 中进行了解释。

审核时间表

员工数量	QMS 初次审核时间 (审核人日)	EMS 初次审核时间 (审核人日)	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	2	3	5	见附录 C.2	
11~25	3		7	见附录 C.2	
26~45	4	6	8.5	见附录 C.2	
46~65	5		10	见附录 C.2	
66~85	6		11	见附录 C.2	
86~125	7	8	12	见附录 C.2	
126~175	8		13	见附录 C.2	
176~275	9		14	见附录 C.2	
276~425	10		15	见附录 C.2	
426~625	11	12	16.5	见附录 C.2	
626~875	12		17.5	见附录 C.2	
876~1175	13		18.5	见附录 C.2	
1176~1550	14		19.5	见附录 C.2	
1551~2025	15	18	21	见附录 C.2	
2026~2675	16		22	见附录 C.2	
2676~3450	17		23	见附录 C.2	
3451~4350	18		24	见附录 C.2	
4351~5450	19		25	见附录 C.2	
5451~6800	20		26	见附录 C.2	
6801~8500	21		27	见附录 C.2	
8501~10700	22		28	见附录 C.2	
>10700	延用以上规律		延用以上规律	见附录 C.2	

C.3.2 术语的解释

在审核时间表中涉及的“员工”是指工作活动与 ISMS 范围有关的所有人员。所有轮班员工的总数量是确定审核时间的起点。

员工的有效数量包括非永久性员工（季节性人员、临时工以及转包工），他们在审核时会在场。一

个认证机构宜与被审核的组织协商确定审核的时间，其最好能证明覆盖组织的所有范围。适当时，考虑的环节可包括季、月、日/日期和轮班。

兼职员工宜同专职员工等同处理。这个决定将依赖于与专职员工工作时间的比较。

“审核时间”包括一个审核员或审核组在 1 阶段审核、2 阶段审核和策划（适当时，包括办公室文档评审）阶段所花费的时间；即与组织、人员、记录、文档那个和过程以及报告撰写接触的时间。包括策划和报告的“审核时间”不宜将现场“审核时间”缩小到少于审核时间表 70%的时间。当另外需要时间去实施策划或撰写报告时，减少现场审核时间也是不合理的。审核员往返时间不算入本计算中，需加入表中涉及的审核时间中。

注 1：70%是一个基于 ISMS 审核经验的因素。

如果使用了远程审核技术（例如交互式基于 web 的协作、web 会议、远程会议和/或组织过程的电子确认），这些活动宜在审核计划中加以识别（见 IS9.1.5），可以考虑将其作为现场审核时间的一部分。

如果认证机构审核计划中远程审核活动占据大于 30%的现场审核时间，认证机构要判断审核计划的适当性，并在实施前从认可机构获得特殊的批准。

注 2：现场审核时间是指单独场所的现场审核时间。远程场所的电子审核作为远程审核，即使电子审核在物理上执行于组织的办公场所之内。

表中的“审核时间”是按照“审核人日”来说明的，一个审核人日是全部的正常工作时间。

对于初次认证审核周期，对一个规定组织的监督时间宜与初次审核时间成比例，每年的监督审核时间大约是初次审核时间的 1/3。计划的监督时间宜每次实施评审以说明组织的变化以及系统的成熟度等，至少在复评时应进行评审。

执行复评所花费的全部时间将依赖于 IS9.1.6 和 ISO/IEC 17021 的 9.4 中定义的评审。在复评时花费的时间宜与相同组织的初次认证审核的时间成比例，大约是初次审核的 2/3。复评审核时间按上面进行计算，超过了日常监督时间，但当复评与监督审核一起实施时，复评也将满足监督审核的要求。无论结论是什么，可 IS9.1.2 的指南适用。

一旦按照 ISMS 范围中的显示的员工数量确定了审核的基点，考虑能影响实际审核时间的因素，需要对审核时间做一些调整，以确保对特殊的 ISMS 以及附录 C.2 列出的要求作出有效的审核。

需要增加审核时间的要素可能是：

- 在 ISMS 范围内的复杂的后勤，包括多于一个的建筑物或位置；
- 员工语言超过一种（需要翻译或防止个别审核员单独工作）；
- 法规的高级别；
- ISMS 覆盖了极其复杂的过程或相关的大量或单一活动；
- 过程涉及了硬件、软件、过程和服务的结合；
- 需要观看临时场所的活动来确认永久场所的活动，它的管理体系从属于认证（见下面的注 3）。

允许减少审核时间的因素可能是：

- 没有/低的风险产品/过程；
- 组织的预备知识（例如，如果组织已经通过了同一个认证机构的其他标准认证）；
- 客户的认证准备（例如，已经被另外的第三方机构认证或认可）；
- 仅涉及单一的活动过程（例如，只有服务）；
- 在适当的位置有成熟的管理体系；
- 大部分员工执行相同的简单任务。

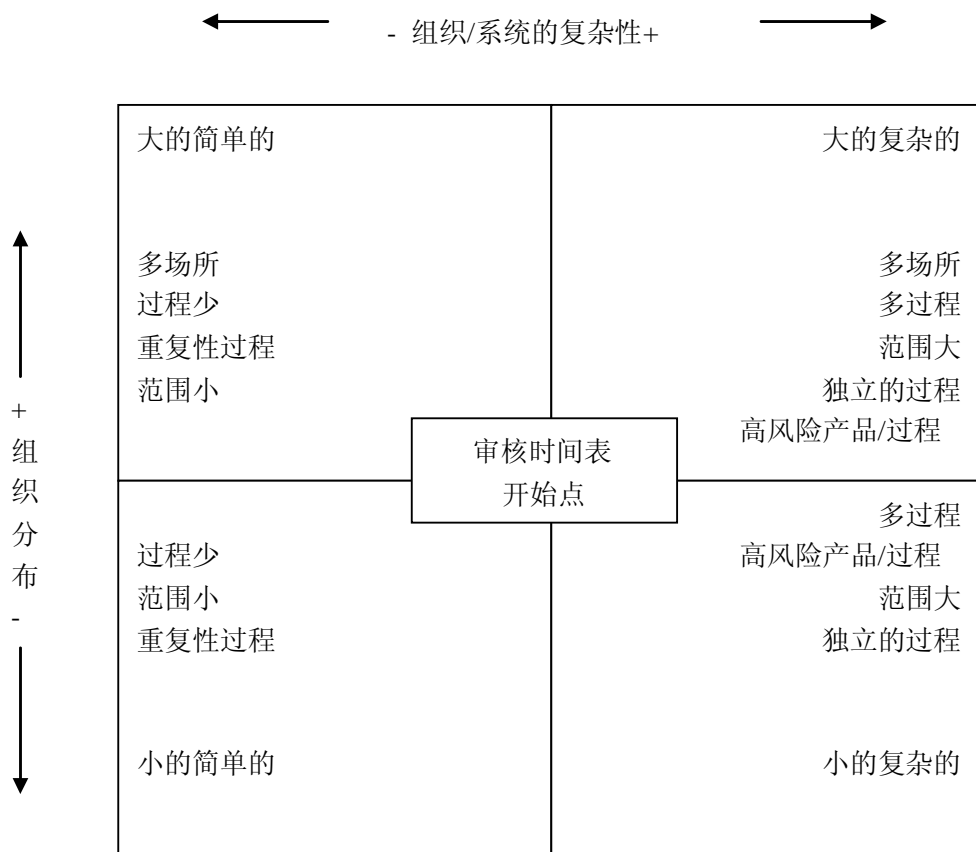
注 3：在认证申请者或被认证组织于临时场所提供他们的产品或服务的情况下，将评价这个场所纳入到认证审核和监督方案中是十分重要的。

一个临时场所是一个不同于认证文档标识场所/位置（其活动在认证的范围内，并按已定义的时间周期实施）的位置。这些场所可以从主要的项目管理场所到资要的服务/安装场所。观看这些场所的需要和抽样的范围宜基于由于系统不符合所引起的在满足需要/期望方面的产品或服务失效风险的评价。

选择的场所的抽样宜体现出组织的能力需要和服务变化，考虑到活动的规模和类型，以及在运行项目的不同阶段。

宜考虑 ISMS 范围、过程、产品/服务的所有属性，由这些因素所作的公正调整证明对于有效的审核来说，审核时间是适当的。增加因素可能被减少因素所影响。在所有的情况下，在审核时间表中对时间的调整，应保持足够的证据和记录来证明其变化的正当性。

下列图形展示了在以上表中的审核时间增加因素和减少因素的潜在交互。



附录 D (资料性附录)

ISO/IEC 27001 附录 A 控制措施评审指南

D.1 目的

本附录为 ISO/IEC 27001 附录 A 列出的控制措施的实施提供了评审指南，并可以指导在初次审核和随后的监督审核中对他们的执行收集审核证据。客户组织在 ISMS 中（按照适用性声明）选择的所有控制措施的实施需要在初次审核的 2 阶段、监督审核或复评中进行评审。

认证机构收集的审核证据必需是充分的，以得出控制措施是否有效的结论。控制措施如何执行将在客户组织声明的规程或策略中或适用性声明中加以规定。很明显，在 ISMS 范围之外的控制措施无需审核。

D.1.1 审核证据

最高质量的审核证据是由审核员通过观察收集的（例如，门上锁了、人员签署保密性协议、存在资产登记并包含观察到的资产、系统设置是充分的等等）。证据可以从观察控制措施的执行结果来收集（例如，由恰当的授权人员为指定人员签署的打印输出的访问权、事件决定的记录、由恰当的授权人员为指定人员签署的处理权、管理或其他会议的备忘录等等）。证据可以是审核员直接测试（或重新执行）的结果（例如试图执行被控制措施所禁止的任务、机器上预防恶意代码的软件是否安装、是否是最新的、授予的访问权（在检查完职权人员之后）等等）。可通过与员工/签约人员的面谈中收集关于过程和控制措施以及决定的证据，无论这些是否是真实恰当的。

D.2 如何使用表 D.1

D.2.1 “组织类控制措施”和“技术类控制措施”列

在各列中的“×”表示：该控制措施是组织类控制措施还是技术类控制措施。某些控制措施既是组织类的又是技术类的，该条目在两列中都有。

组织类控制措施的绩效证据可以通过控制措施执行记录、访谈、观察和物理检查等进行收集。技术类控制措施的执行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，进行收集。

D.2.2 “系统测试”列

“系统测试”意味着系统的直接评审（例如系统设置或配置的评审）。审核员问题可以在系统控制台，或者通过测试工具结果的评价来回答。如果客户组织有基于计算机的工具在使用，这种工具又恰是审核员所熟悉的，那么可以用来支持审核，或者，客户组织（或他们的子承包商）完成的评价结果可以用来作为评审的材料。

对于技术类控制措施的评审，可有两个类别：

- “可能的”：系统测试对评价实施的控制措施是可能的，但往往不是必要的。
- “推荐的”：系统测试通常是必要的。

D.2.3 “目视检查”列

“目视检查”意味着这些控制措施通常需要通过视觉在其特定区域进行检查来评价他们的有效性。这意味着，分别进行纸面文档评审或者访谈是不够的，审核员需要在控制措施实施的特定区域进行验证。

D.2.4 “审核评审指南”列

对于特定控制措施的审核具有指南是有益的，“审核评审指南”列提供了可能的评价控制措施的关注区域，作为审核员的进一步指南。

表 D.1 控制措施分类

ISO/IEC 27001:2005, 附录 1	组织类 控制措施	技术类 控制措施	系统测试	目视检查	审核评审指南
A.5 安全方针					
A.5.1 信息安全方针					
A.5.1.1 信息安全方针文件	×				
A.5.1.2 信息安全方针的评审	×				管理评审备忘录
A.6 信息安全组织					
A.6.1 内部组织					
A.6.1.1 信息安全管理承诺	×				管理会议备忘录
A.6.1.2 信息安全协调	×				管理会议备忘录
A.6.1.3 信息安全职责的分配	×				
A.6.1.4 信息处理设施的授权过程	×				
A.6.1.5 保密性协议	×				从文件的复印件中抽样
A.6.1.6 与政府部门的联系	×				
A.6.1.7 与特殊权益团体的联系	×				
A.6.1.8 信息安全的独立评审	×				阅读报告
A.6.2 外部各方					
A.6.2.1 与外部各方相关风险的识别	×				
A.6.2.2 处理与顾客有关的安全问题	×				
A.6.2.3 处理第三方协议中的安全问题	×				测试一些合同条款
A.7 资产管理					
A.7.1 对资产负责					
A.7.1.1 资产清单	×				识别资产
A.7.1.2 资产责任人	×				
A.7.1.3 资产的允许使用	×				
A.7.2 信息分类					
A.7.2.1 分类指南	×				
A.7.2.2 信息的标记和处理	×				命名：目录，文件，打印报告，记录介质（例如磁带，磁盘，CD）、电子消息和文件传输。
A.8 人力资源安全					
A.8.1 任用之前					
A.8.1.1 角色和职责	×				
A.8.1.2 审查	×				
A.8.1.3 任用的条款和条件	×				
A.8.2 任用中					
A.8.2.1 管理职责	×				
A.8.2.2 信息安全意识、教育和培训	×				询问员工他们是否知道了他们宜知道的特殊事项
A.8.2.3 纪律处理过程	×				
A.8.3 任用的终止或变化					

ISO/IEC 27001:2005, 附录 1	组织类 控制措施	技术类 控制措施	系统测试	目视检查	审核评审指南
A. 8. 3. 1 终止职责	×				
A. 8. 3. 2 资产的归还	×				
A. 8. 3. 3 撤销访问权	×	×	推荐的		
A. 9 物理和环境安全					
A. 9.1 安全区域					
A. 9. 1. 1 物理安全边界	×				
A. 9. 1. 2 物理入口控制	×	×	可能的	×	访问记录的存档
A. 9. 1. 3 办公室、房间和设施的安全保护	×			×	
A. 9. 1. 4 外部威胁和环境威胁的安全防护	×			×	
A. 9. 1. 5 在安全区域工作	×			×	
A. 9. 1. 6 公共访问区和交接区安全	×			×	
A. 9.2 设备安全					
A. 9. 2. 1 设备安置和保护	×	×	可能的	×	
A. 9. 2. 2 支持性设施	×	×	可能的	×	
A. 9. 2. 3 布缆安全	×			×	
A. 9. 2. 4 设备维护	×				
A. 9. 2. 5 组织场所外的设备安全	×	×	可能的		便携式设备加密
A. 9. 2. 6 设备的安全处置或再利用	×	×	可能的	×	
A. 9. 2. 7 资产的移动	×				
A. 10 通信和操作管理					
A. 10.1 操作程序和职责					
A. 10. 1. 1 文档化的操作程序	×				
A. 10. 1. 2 变更管理	×	×	推荐的		
A. 10. 1. 3 责任分割	×				
A. 10. 1. 4 开发、测试和运行设施分离	×	×	可能的		
A. 10.2 第三方服务交付管理					
A. 10. 2. 1 服务交付	×				
A. 10. 2. 2 第三方服务的监视和评审	×	×	可能的		
A. 10. 2. 3 第三方服务的变更管理	×				
A. 10.3 系统规划和验收					
A. 10. 3. 1 容量管理	×	×	可能的		
A. 10. 3. 2 系统验收	×				
A. 10.4 防范恶意和移动代码					
A. 10. 4. 1 控制恶意代码	×	×	推荐的		服务器、PC、网关的抽样
A. 10. 4. 2 控制移动代码	×	×	可能的		
A. 10.5 备份					
A. 10. 5. 1 信息备份	×	×	推荐的		尝试一次恢复
A. 10.6 网络安全管理					
A. 10. 6. 1 网络控制	×	×	可能的		

ISO/IEC 27001:2005, 附录 1	组织类 控制措施	技术类 控制措施	系统测试	目视检查	审核评审指南
A. 10. 6. 2 网络服务的安全	×				SLA 的安全失误
A. 10. 7 介质处置					
A. 10. 7. 1 可移动介质的管理	×	×	可能的		
A. 10. 7. 2 介质的处置	×				
A. 10. 7. 3 信息处理程序	×				
A. 10. 7. 4 系统文件的安全	×	×	可能的	×	
A. 10. 8 信息的交换					
A. 10. 8. 1 信息交换策略和程序	×				
A. 10. 8. 2 交换协议	×				
A. 10. 8. 3 运输中的物理介质	×	×	可能的		加密或物理保护
A. 10. 8. 4 电子消息发送	×	×	可能的		确认抽样的消息符合按略/ 规程
A. 10. 8. 5 业务信息系统	×				
A. 10. 9 电子商务服务					
A. 10. 9. 1 电子商务	×	×	可能的		
A. 10. 9. 2 在线交易	×	×	推荐的		检查: 完整性, 访问授权
A. 10. 9. 3 公共可用信息	×	×	可能的		
A. 10. 10 监视					
A. 10. 10. 1 审计日志	×	×	可能的		在线的或打印的
A. 10. 10. 2 监视系统的使用	×	×	可能的		
A. 10. 10. 3 日志信息的保护	×	×	可能的		
A. 10. 10. 4 管理员和操作员日志	×	×	可能的		
A. 10. 10. 5 故障日志	×				
A. 10. 10. 6 时钟同步		×	可能的		
A. 11 访问控制					
A. 11. 1 访问控制的业务要求					
A. 11. 1. 1 访问控制策略	×				
A. 11. 2 用户访问管理					
A. 11. 2. 1 用户注册	×				对系统有访问权的员工/签 约人员进行抽样检查
A. 11. 2. 2 特权管理	×	×	可能的		员工的内部调动
A. 11. 2. 3 用户口令管理	×				
A. 11. 2. 4 用户访问权的复查	×				
A. 11. 3 用户职责					
A. 11. 3. 1 口令使用	×				检验适当位置的用户指南/ 策略
A. 11. 3. 2 无人值守的用户设备	×				检验适当位置的用户指南/ 策略
A. 11. 3. 3 清空桌面和屏幕策略	×			×	
A. 11. 4 网络访问控制					

ISO/IEC 27001:2005, 附录 1	组织类 控制措施	技术类 控制措施	系统测试	目视检查	审核评审指南
A. 11. 4. 1 使用网络服务的策略	×				
A. 11. 4. 2 外部连接的用户鉴别	×	×	推荐的		
A. 11. 4. 3 网络上的设备标识		×			通常不实施
A. 11. 4. 4 远程诊断和配置端口的保护		×	推荐的		
A. 11. 4. 5 网络隔离	×	×	可能的		网络图: WAN, LAN, VLAN, VPN, 网络对象, 网段, 如 DMZ 区等。
A. 11. 4. 6 网络连接控制	×	×	推荐的		共享网络不常见
A. 11. 4. 7 网络路由控制	×	×	推荐的		防火墙, 路由器/交换机: 规则库, ACL' s, 访问控制策略
A. 11. 5 操作系统访问控制					
A. 11. 5. 1 安全登录程序	×	×	推荐的		
A. 11. 5. 2 用户标识和鉴别	×	×	推荐的		
A. 11. 5. 3 口令管理系统	×	×	推荐的		
A. 11. 5. 4 系统实用工具的使用	×	×	推荐的		
A. 11. 5. 5 对话超时	×	×	可能的	×	
A. 11. 5. 6 联机时间的限制	×	×	可能的	×	
A. 11. 6 应用和信息访问控制					
A. 11. 6. 1 信息访问限制	×	×	推荐的		
A. 11. 6. 2 敏感系统隔离	×	×	可能的		
A. 11. 7 移动计算和远程工作					
A. 11. 7. 1 移动计算和通信	×	×	可能的		
A. 11. 7. 2 远程工作	×	×	可能的		
A. 12 信息系统获取、开发和维护					
A. 12. 1 信息系统的安全需求					
A. 12. 1. 1 安全需求分析和规范	×				
A. 12. 2 应用中的正确处理					
A. 12. 2. 1 输入数据的确认	×	×	推荐的		软件开发指南、软件测试、在实践中存在用户需要该控制措施的业务应用样本的确认
A. 12. 2. 2 内部处理的控制	×	×	可能的		软件开发指南、软件测试、在实践中存在用户需要该控制措施的业务应用样本的确认。
A. 12. 2. 3 消息的完整性		×	可能的		
A. 12. 2. 4 输出数据的确认	×	×	可能的		软件开发指南、软件测试、在实践中存在用户需要该控制措施的业务应用样本

ISO/IEC 27001:2005, 附录 1	组织类 控制措施	技术类 控制措施	系统测试	目视检查	审核评审指南
					的确认
A. 12.3 密码控制					
A. 12.3.1 使用密码控制的策略	×	×	可能的		适当时,也可检查策略的实施
A. 12.3.2 密钥管理	×	×	推荐的		
A. 12.4 系统文件的安全					
A. 12.4.1 运行软件的控制	×	×	可能的		
A. 12.4.2 系统测试数据的保护	×	×	可能的	×	
A. 12.4.3 程序源代码的访问控制	×	×	推荐的		
A. 12.5 开发和支持过程中的安全					
A. 12.5.1 变更控制程序	×				
A. 12.5.2 操作系统变更后,应用的技术评审	×				
A. 12.5.3 软件包变更的限制	×				
A. 12.5.4 信息泄露	×	×	可能的		未知服务
A. 12.5.5 外包软件开发	×				
A. 12.6 技术脆弱性管理					
A. 12.6.1 技术脆弱性的控制	×	×	推荐的		补丁的分发
A. 13 信息安全事件管理					
A. 13.1 报告信息安全事态和弱点					
A. 13.1.1 报告信息安全事态	×				
A. 13.1.2 报告安全弱点	×				
A. 13.2 信息安全事件和改进的管理					
A. 13.2.1 职责和程序	×				
A. 13.2.2 对信息安全事件的总结	×				
A. 13.2.3 证据的收集	×				
A. 14 业务连续性管理					
A. 14.1 业务连续性管理的信息安全方面					
A. 14.1.1 业务连续性管理过程中包含的信息安全	×				
A. 14.1.2 业务连续性和风险评估	×				
A. 14.1.3 制定和实施包含信息安全的连续性计划	×	×	可能的	×	灾难恢复场所检查和灾难恢复场所的距离,要符合风险评估和适用的法律法规要求。
A. 14.1.4 业务连续性计划框架	×				
A. 14.1.5 测试、维护和再评估业务连续性计划	×				
A. 15 符合性					
A. 15.1 符合法律要求					

ISO/IEC 27001:2005, 附录 1	组织类 控制措施	技术类 控制措施	系统测试	目视检查	审核评审指南
A. 15. 1. 1 可用法律的识别	×				
A. 15. 1. 2 知识产权 (IPR)	×				
A. 15. 1. 3 保护组织的记录	×	×	可能的		
A. 15. 1. 4 数据保护和个人信息的隐私	×	×	可能的		
A. 15. 1. 5 防止滥用信息处理设施	×				
A. 15. 1. 6 密码控制措施的规章	×				
A. 15. 2 安全策略和标准以及技术符合性					
A. 15. 2. 1 符合安全策略和标准	×				
A. 15. 2. 2 技术符合性检查	×	×			评估过程和跟踪
A. 15. 3 信息系统审核考虑					
A. 15. 3. 1 信息系统审核控制措施	×				
A. 15. 3. 2 信息系统审核工具的保护	×	×	可能的		