

中华人民共和国国家标准

GB/T 27308—2011

合格评定 信息技术服务管理体系 认证机构要求

Conformity assessment—Requirements for bodies providing audit and
certification of IT service management systems

2011-12-30 发布

2012-03-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

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

10 认证机构的管理体系要求 8

 10.1 可选方式 8

 10.2 方式一：与 GB/T 19001 一致的管理体系要求 9

 10.3 方式二：通用的管理体系要求 9

附录 A（资料性附录） 信息技术服务类别 10

附录 B（资料性附录） 审核时间 12

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国认证认可标准化技术委员会(SAC/TC 261)提出并归口。

本标准起草单位:中国电子技术标准化研究所、中国国家认证认可监督管理委员会、中国合格评定国家认可中心、中国认证认可协会、广东赛宝认证中心、华夏认证中心有限公司、山东标准研究院、上海质量体系审核中心、北京天和正通信息技术有限公司、中国软件评测中心、上海三零卫士信息安全有限公司。

本标准主要起草人:韩硕祥、杨晓光、黄俊梅、庞翔、费扬、付瑞云、赵国祥、王梅、娄丹、朱瑞虹、王正华、娄天峰、张少彤、曾波、张建军。

引 言

GB/T 27021—2007《合格评定 管理体系审核认证机构的要求》提供了对各类管理体系认证机构的通用要求。本标准在 GB/T 27021 通用要求的基础上补充了依据 GB/T 24405.1—2009《信息技术 服务管理 第1部分：规范》开展信息技术服务管理体系(ITSMS)审核和认证的机构的专用要求和指南,并与 GB/T 27021—2007 共同使用。

本标准正文遵循 GB/T 27021—2007 的结构,增加了针对 ITSMS 审核和认证机构的特殊要求和指南。

本标准的意图是规范实施 ITSMS 审核和认证的机构自身的管理运作,并为认可机构协调一致的评审认证机构提供依据。如果认证机构在贯彻本标准的指南性条款时存有异议,认证机构应对此进行说明,并确保满足本标准及 GB/T 27021—2007 的相关条款要求。

合格评定 信息技术服务管理体系 认证机构要求

1 范围

本标准对实施信息技术服务管理体系(以下简称“ITSMS”)审核和认证的认证机构提出要求并提供指南,以作为对 GB/T 27021—2007 要求的补充。

本标准适用于对实施 ITSMS 审核和认证的认证机构的认可提供支持。

任何提供 ITSMS 认证的机构需要在能力和可靠性方面证实其满足本标准的要求。本标准的指南性条款为这些要求提供了进一步的说明。

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 19011 质量和(或)环境管理体系审核指南(ISO 19011,IDT)

GB/T 24405.1—2009 信息技术 服务管理 第1部分:规范(ISO/IEC 20000-1:2005,IDT)

GB/T 27021—2007 合格评定 管理体系审核认证机构的要求(ISO/IEC 17021:2006,IDT)

3 术语和定义

下列术语和定义适用于本文件。

3.1

认证机构 certification body

按照正式发布的 ITSMS 标准及其所要求的任何补充性文件,对组织的 ITSMS 进行审核和认证的第三方机构。

3.2

认证文件 certification document

表明组织的 ITSMS 符合特定的 ITSMS 标准及其所要求的任何补充性文件的一类文件。

3.3

组织 organization

公司、集团、事务所、工厂、政府机构、科研机构、学校等,或者其部分或组合,无论其是否是法人,还是公有或私有的,均具有其自身的职能和管理,并能够确保实施其信息技术服务。

4 原则

本条款应用 GB/T 27021—2007 中第4章的原则。

5 通用要求

5.1 法律与合同事宜

见 GB/T 27021—2007 中 5.1 的要求。

5.2 公正性的管理

见 GB/T 27021—2007 中 5.2 的要求。

5.3 责任和财力

见 GB/T 27021—2007 中 5.3 的要求。

6 结构要求

6.1 组织结构和最高管理层

见 GB/T 27021—2007 中 6.1 的要求。

6.2 维护公正性的委员会

见 GB/T 27021—2007 中 6.2 的要求。

7 资源要求

7.1 管理层和人员的能力

见 GB/T 27021—2007 中 7.1 的要求。

7.1.1 管理层能力

为实施 ITSMS 认证,管理层的基本能力是选择、提供和管理那些具备与受审核的活动和有关的信息技术服务事宜相适应的技能和综合能力的人员。

7.1.2 能力分析

认证机构应确保相关人员理解组织信息技术服务类别(参见附录 A)有关的技术和法律、法规以及其他相关要求。

认证机构应具备有效的能力分析系统,以便在其运作所涉及的全部技术领域就需要具备的信息技术服务管理方面的能力进行分析。

对于每个组织,认证机构应在能力分析的基础上实施申请评审。认证机构应证实具备如下能力:

- a) 依据附录 A 提供的信息技术服务分类准则,确定组织的业务类别;
- b) 明确组织的业务活动范围;
- c) 与 a)中确定出的组织的业务类别相对应,识别组织业务活动范围内的信息技术服务管理过程;
- d) 根据组织的业务类别和已识别的相关活动,确定认证机构应具备的能力;
- e) 确认认证机构是否具备所需要的能力。

7.2 参与认证活动的人员

见 GB/T 27021—2007 中 7.2 的所有要求。

7.2.1 认证管理人员

认证管理人员的能力至少应包括如下内容：

- a) 选择审核员并验证他们的能力；
- b) 给 ITSMS 审核员提供简要的指导并安排必要的培训；
- c) 作出授予、保持、更新、扩大、缩小、暂停或撤销认证决定；
- d) 建立和实施投诉、申诉和争议程序。

7.2.2 审核员和技术专家

7.2.2.1 审核员应具备如下条件：

- a) 大学本科(含)以上学历；
- b) 至少 4 年与信息技术相关的全职工作经历,其中至少 2 年与信息技术服务相关的工作经历；
- c) 完成累计 40 小时信息技术服务管理标准和认证审核知识的培训；
- d) 承担审核员职责之前,已获得评审 ITSMS 的相关经验。这种经验宜通过参与最少 4 次、总天数为 20 天的审核获得,其中至少 1 次是完整的 ITSMS 审核；
- e) c)和 d)所指相关经验应在近三年内获得；
- f) 具备 GB/T 19011 标准中要求的个人素质；
- g) 不断提升自身信息技术服务管理和审核方面的知识和能力。

技术专家应符合上述 a)、b)和 f)。

7.2.2.2 认证机构应为培训和选择审核组成员建立准则,以确保审核员：

- a) 理解 ITSMS 标准和其他相关规范性文件；
- b) 理解信息技术服务管理过程和相关知识；
- c) 理解服务改进计划的执行和管理；
- d) 具有与受审核的活动相关的技术知识；
- e) 具有与组织的信息技术服务类别(参见附录 A)相适应的法律、法规及其他技术要求的知识；
- f) 理解基于 GB/T 19011 的审核原则、程序和技术。

除了上述 d)可以在审核组成员之间共享外,其余均适用于审核组的所有成员。

作为审核组组长除了符合以上要求外,还应符合如下要求,并应通过在指导和监督下进行的审核中得到证实：

- a) 具备管理认证审核过程的知识和素质；
- b) 已经至少作为审核员实施过 3 次完整 ITSMS 审核。

7.2.2.3 审核员应能够证实其具备上述知识和能力,如通过：

- a) 经承认的信息技术服务管理方面的相关资质；
- b) 经注册的审核员资格；
- c) 经批准的信息技术服务管理课程培训；
- d) 持续提升自身知识和能力的记录；
- e) 经现场见证的审核能力证明；
- f) 定期的个人评价记录。

7.2.3 决定过程的管理人员的能力

管理层应具备对授予、保持、扩大、缩小、暂停或撤销 ITSMS 认证的決定过程进行管理所需的技术能力。

7.3 外部审核员和外部技术专家的使用

见 GB/T 27021—2007 中 7.3 的要求。

7.4 人员记录

见 GB/T 27021—2007 中 7.4 的要求。

7.5 外包

见 GB/T 27021—2007 中 7.5 的要求。

8 信息要求

8.1 可公开获取的信息

见 GB/T 27021—2007 中 8.1 的要求。

8.2 认证文件

见 GB/T 27021—2007 中 8.2 的要求。

8.3 获证客户目录

见 GB/T 27021—2007 中 8.3 的要求。

8.4 获证资格的引用和标志的使用

见 GB/T 27021—2007 中 8.4 的要求。

8.5 保密

见 GB/T 27021—2007 中 8.5 的要求。

认证机构应识别法律、法规对保密方面的要求,并在与组织签订的认证协议中明确双方及其相关人员的责任和义务。

在认证审核之前,认证机构应要求组织说明是否存在不能提供给审核组的包含保密性或敏感性信息的 ITSMS 记录。认证机构应确定是否能在缺少这些记录的情况下对 ITSMS 进行充分的审核。如果认证机构认为不对已识别的保密性或敏感性的信息进行审核就不能保证 ITSMS 审核的充分性,则应告知组织只有在获得适当的访问许可时才能进行认证审核。

8.6 认证机构与其组织间的信息交换

见用 GB/T 27021—2007 中 8.6 的要求。

9 过程要求

9.1 通用要求

9.1.1 审核方案

见 GB/T 27021—2007 中 9.1.1~9.1.3 的要求。

9.1.2 认证审核准则

组织的 ITSMS 接受审核的准则应是 GB/T 24405.1—2009 所给出的要求和其实施业务相关的认证所需其他文件中的要求。如果需要对上述文件在特定认证方案中的应用作出解释,这种解释应由公正的和具备必要技术能力的相关委员会或人员给出,并由认证机构正式发布。

9.1.3 政策和程序

认证机构的管理体系文件应包括实施认证过程的政策和程序,其中包括对用于各类 ITSMS 认证的那些文件的使用和应用情况的检查,也包括对用于审核和认证组织 ITSMS 程序的检查。

9.1.4 审核组的能力

当为特定认证审核选择指派审核组时,认证机构应确保审核组实施各项工作的技能是适宜的。除了本标准 7.2 中的要求之外,以下要求适用于认证审核。对于监督活动,仅仅与已安排的监督活动有关的要求适用。

- a) 在以下每个方面,至少有一名审核组成员满足认证机构能力准则并在审核组内承担相应责任:
 - 1) 管理审核组;
 - 2) 适用于 ITSMS 的管理体系和过程;
 - 3) ITSMS 过程及其实施的相关知识;
 - 4) ITSMS 有效性评审和测量的相关知识;
 - 5) ITSMS 标准,行业最佳实践和程序的相关知识;
 - 6) 事件处理方法的相关知识;
 - 7) 当前服务管理涉及的相关技术;
 - 8) 风险管理过程和方法的相关知识。
- b) 审核组应具备将组织的服务级别协议(SLA)的各个方面对应到 ITSMS 中相应条款进行评审的能力。
- c) 审核组应具有服务管理过程相适应的工作经验和能力。(这不意味着每一个审核员必须具备服务管理所有领域的经验和能力,但是审核组整体上应具备受审核的 ITSMS 范围内所覆盖的经验和能力。)

9.1.5 审核时间

参见 GB/T 27021—2007 中 9.1.4 的要求。

本标准附录 B 对审核时间提供指南,认证机构应能证明或说明在初次审核、监督审核和再认证审核中所用时间的合理性。

9.1.6 多场所

见 GB/T 27021—2007 中 9.1.5 的要求。

9.1.6.1 当组织拥有满足以下条件的多个场所时,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) 所有的场所进行的相同活动,在同一 ITSMS 下运行,并接受统一的管理、内部审核和管理评审;
- b) 所有的场所都包含在组织的 ITSMS 内部审核方案中;
- c) 所有的场所都包含在组织的 ITSMS 管理评审方案中。

9.1.6.2 认证机构在使用基于抽样的方法时,应具备程序以确保:

- a) 在初次的合同评审中,最大程度地识别场所之间的差异,以便确定适宜的抽样水平。
- b) 结合以下因素抽取具有代表性的场所:
 - 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) 场所规模的差异;
 - 4) 场所业务目的的差异;
 - 5) ITSMS 的复杂程度;
 - 6) 工作方式的差异;
 - 7) 所实施活动的差异;
 - 8) 任何不同的法律、法规要求。
- c) 从组织的 ITSMS 范围内的所有场所中选择具有代表性的样本,该选择宜基于上述 b) 中所列因素以及随机因素所作出的判断。
- d) 根据上述要求,设计监督审核方案时考虑组织 ITSMS 认证范围内有代表性的场所业务范围。
- e) 无论是在总部还是在某单一场所发现不符合,纠正措施的实施适用于包括在认证范围内的总部和所有场所(适用时)。

审核应关注组织为确保其 ITSMS 以一致的方式,在所有场所得得到有效运行。

9.1.7 审核组任务及成员确认

见 GB/T 27021—2007 中 9.1.6~9.1.8 的要求。

9.1.8 现场审核方法

见 GB/T 27021—2007 中 9.1.9 的要求。

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,例如,电话会议、网络会议、基于网络的互动式沟通和远程电子访问 ITSMS 文件和(或) ITSMS 过程等方式。关注这些技术将有助于提高审核的有效性和效率,并支持审核过程的完整性。

9.1.9 认证审核报告

见 GB/T 27021—2007 中 9.1.10 的要求。

9.1.9.1 认证机构可以采用适合其需要的报告程序,但这些程序至少应确保:

- a) 在离开组织场所前,在审核组和组织管理者之间召开一次会议,并提供:
 - 1) 关于组织 ITSMS 与特定认证要求的符合性方面的书面或口头说明;
 - 2) 组织就审核发现及其根据提出疑问的机会。
- b) 审核组向认证机构提供关于审核发现的审核报告,这些审核发现是针对组织的 ITSMS 与所有认证要求的符合性。

9.1.9.2 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) 审核覆盖的区域(例如,认证要求和接受审核的场所),也包括所采用的主要审核路线和所使用的审核方法(见本标准的 9.1.8);
- b) 审核结果(包括正面的和负面的);
- c) 已识别的任何不符合的详细情况,包括支持它们的客观证据和这些不符合所涉及的审核准则的要求;
- d) 对 ITSMS 内部审核和管理评审的信任程度的评价。

9.1.10 不符合处理及认证决定

见 GB/T 27021—2007 中 9.1.11~9.1.15 的要求。

9.2 初次审核与认证

9.2.1 申请和申请评审

见 GB/T 27021—2007 中 9.2.1~9.2.2 的要求。

认证机构应要求组织确定其 ITSMS 的范围。认证机构应确保组织的 ITSMS 范围恰当地反映其服务活动(参见附录 A),并确保组织没有将其活动中应包含的体系运行要素排除在认证范围之外。

适宜时,组织应在递交认证申请时指明不完全包含在 ITSMS 范围内的服务活动。例如,与其他组织共同提供信息技术服务的情况。

9.2.2 初次认证审核

信息技术管理体系的初次认证审核应分两个阶段实施:第一阶段和第二阶段。

9.2.2.1 第一阶段审核

见 GB/T 27021—2007 中 9.2.3.1 的要求。

在该审核阶段,认证机构应能够获取 ITSMS 的相关文件,其中包括 GB/T 24405.1—2009 中 3.2 所要求的文件。

组织可以把 ITSMS 与其他管理体系(如:质量、信息安全、职业健康安全、环境)的文件合并在一起,但应明确 ITSMS 与其他管理体系的接口。

9.2.2.2 第二阶段审核

见 GB/T 27021—2007 中 9.2.3.2 的要求。

认证机构宜关注组织是否充分识别了基于组织业务活动的信息技术服务管理过程,并证实与组织的运作是适宜的。

9.2.2.2.1 组织过程的运作控制

认证机构宜要求组织证实其对信息技术服务管理过程的分析和组织运作实施了适当的控制措施,应包括:

- a) 服务交付过程(服务级别管理,服务报告,服务连续性和可用性管理,信息技术服务的预算和核算,能力管理,信息安全管理);
- b) 关系过程(业务关系管理,供方管理);
- c) 处理过程(事件管理,问题管理);
- d) 控制过程(配置管理,变更管理);
- e) 发布过程(发布管理)。

9.2.2.2.2 管理体系结合审核

认证机构可以仅提供 ITSMS 认证服务,或结合 ITSMS 认证提供其他管理体系认证服务。

ITSMS 审核可以和其他管理体系的审核相结合。这种结合只有在证实审核满足 ITSMS 认证所有要求时才有可能。审核的质量不应由于结合审核受到负面影响。

注: GB/T 19011 为实施管理体系的结合审核提供指南。

9.2.3 初次认证的审核结论

见 GB/T 27021—2007 中 9.2.4 的要求。

9.2.4 授予初次认证的信息

见 GB/T 27021—2007 中 9.2.5.1 和 9.2.5.2 的要求。

负责作出认证决定的人员不应参与审核。

通常情况下,负责作出认证决定的人员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作出推翻建议的决定的依据。

9.3 监督活动

见 GB/T 27021—2007 中 9.3 的要求。

对于 ITSMS 比较复杂和经常变更的组织,每年一次审核可能不适宜,认证机构应能证明考虑过这些事宜。

9.4 再认证

见 GB/T 27021—2007 中 9.4 的要求。

如果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实施有效的纠正措施。如果纠正措施没有在同意的时间内完成,认证范围应被缩小,或暂停、撤销认证证书。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适宜,以确保组织的服务满足规定要求。

9.5 特殊审核

见 GB/T 27021—2007 中 9.5 的要求。

如果已经通过 ITSMS 认证的组织对其管理体系做重大修改,或者发生影响其认证基础的其他变更,认证机构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

见 GB/T 27021—2007 中 9.6 的要求。

9.7 申诉

见 GB/T 27021—2007 中 9.7 的要求。

9.8 投诉

见 GB/T 27021—2007 中 9.8 的要求。

9.9 申请组织和组织的记录

见 GB/T 27021—2007 中 9.9 的要求。

10 认证机构的管理体系要求

10.1 可选方式

见 GB/T 27021—2007 中 10.1 的要求。

10.2 方式一：与 GB/T 19001 一致的管理体系要求

见 GB/T 27021—2007 中 10.2 的要求。

10.3 方式二：通用的管理体系要求

见 GB/T 27021—2007 中 10.3 的要求。

附 录 A
(资料性附录)
信息技术服务类别

认证机构宜参照表 A.1,开展如下活动:

- a) 确定认证机构开展认证的范围;
- b) 针对特定的行业类别和种类,识别审核员所必需的技术资格;
- c) 选择有适宜资格的审核组。

表 A.1 信息技术服务类别

大类	中类	内 容	备 注
01 (规划与设计服务)	01.01	信息系统咨询规划	根据客户的实际业务需求,为其提供信息系统的资讯和规划服务。
	01.02	信息系统硬件设计、开发服务	对信息系统硬件的架构、选型和实施策略进行设计,并实施开发。
	01.03	信息系统软件设计、开发服务	信息系统软件的需求分析、设计、开发等服务。
	01.04	信息技术咨询服务	协助需方提升和优化信息化管理活动的咨询服务,如 IT 治理,IT 服务管理等咨询服务。
02 (集成服务)	02.01	设备系统集成服务	指以搭建需方的信息化管理支持平台为目的,将设备及其嵌入式软件进行集成设计、安装调试的服务。如网络系统集成服务、智能建筑系统集成服务、安全防护系统集成服务等。
	02.02	软件系统集成服务	将各个分离的软件、功能和信息等集成到相互关联的、统一和协调的平台之中的服务。如界面集成、数据集成、应用集成等。
03 (测试与监理服务)	03.01	信息系统测试服务	提供检验信息系统是否与设计目标相吻合,相关功能是否达到基本要求的服务。
	03.02	软件产品测试服务	提供检验软件产品是否与设计目标相吻合,相关功能是否达到基本要求的服务。
	03.03	信息系统工程监理	为需方提供监理服务,对监理对象进行监督和理顺,以保证工程项目的建设达到需方预期的目标。
	03.04	软件工程监理服务	对软件开发生命全周期中活动实施监理服务。
	03.05	其他测试与监理服务	
04 (运行维护服务)	04.01	基础设施运行维护服务	指对保证信息系统正常运行所必需的电力、空调、消防、安防、网络等基础环境的运维。如机房电力、消防、安防、网络等系统的运维。
	04.02	硬件运行维护服务	硬件设施的状态监控、故障处理、性能优化等。如网络设备、服务器设备、安全设备、存储备份设备、音视频设备、终端设备、办公设备及其他相关设备的运维。

表 A.1 (续)

大类	中类	内 容	备 注
04 (运行维护服务)	04.03	软件运行维护服务	应用软件(含操作系统、中间件、网管、防病毒等)和定制化软件(数据交换、开发平台、安全类、内容管理、工作流、报表等)的改正性、适应性维护和局部功能调整或优化,以及常规的技术支持。
	04.04	其他信息技术运行维护服务	
05 (安全服务)	05.01	风险评估	评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性,并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。
	05.02	安全运维	通过专业的服务,解决网络和信息系統日常运行中的安全问题,包括系统安全加固、日常安全监控、定期安全审计、安全通告、补丁更新以及安全技术支持等。
	05.03	应急处理	为降低安全事件给客户造成的损失和影响,在处置网络与安全事件时提供一系列的措施和行动。
	05.04	灾难恢复	将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态,并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态的活动和流程。
	05.05	其他安全服务	
06 (业务流程服务)	06.01	电子商务支持服务	为电子商务活动提供各种支撑和管理服务。如CA安全认证服务、支付结算服务、公共电子商务服务等。
	06.02	软件运营服务	需方根据需求通过互联网订购和使用供方提供的应用软件系统的部分或全部功能的服务。如在线存储、在线杀毒等。
	06.03	数据处理	将图片、文字、影像、语音等信息内容运用数字化技术进行加工处理并整合运用的服务。
	06.04	呼叫中心/服务台服务	为客户提供客户投诉、客户服务咨询、产品推荐热线与市场调查、电话销售等服务。
	06.05	其他业务流程服务	

附 录 B
(资料性附录)
审 核 时 间

本附录为认证机构制定有关确定审核时间的程序提供了指南。

认证机构需要针对每一申请认证的 ITSMS,识别初次审核、监督审核和再认证审核所花费的审核时间。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(尤其是第一阶段审核)中的发现和考虑的 ITSMS 范围进行调整。经验表明,ITSMS 的范围、所涉及雇员的数量、规模、特性、复杂性对任何一个特定审核所需的时间有决定性影响。在认证机构的申请评审过程中,需要检查这些因素对审核时间的确定所产生的潜在影响。

需要注意的是,在确定审核时间时,宜考虑所有因素而不能孤立地使用本审核时间表。下列情况说明可能影响审核时间的因素:

- 与 ITSMS 范围的规模有关的因素(例如,信息系统的数量、处理的信息量、用户的数量、特权用户的数量、IT 平台的数量、网络的数量及它们的规模);
- 与 ITSMS 的复杂程度有关的因素(例如,SLA 的要求、组织对信息系统的依赖程度、所操作和处理的敏感和关键信息的多少及类型、所有开发项目的数量和规模、ITSMS 文件化的程度);
- 在 ITSMS 范围内开展的服务类型,以及关于这些服务类型的安全、法律、法规、合同和业务要求;
- 在 ITSMS 各部分的实施过程中,所应用的技术的水平和多样性[例如,已使用工具、文件和(或)过程控制、纠正和(或)预防措施、信息系统、网络等,而无论它们是固定的、移动的、无线的、外部的或内部的];
- 在 ITSMS 范围内场所的数量,这些场所的异同程度如何,是否所有的场所都被审核还是抽样;
- 经证实的以往 ITSMS 绩效;
- 在 ITSMS 范围内,所使用的外包和第三方安排的程度,以及对这些服务的依赖程度;
- 适用于认证的标准、法律和法规,以及任何可能适用的行业特定要求。

表 B.1 给出了初次审核时间的平均数量(这个数量包括第一阶段和第二阶段审核的时间),同时还应根据受审核组织特定的因素调整审核时间。

表 B.1 审核时间表

员工数量 人	ITSMS 初次审核时间 审核人日
1~25	4
26~45	5
46~65	6
66~85	7
86~125	8
126~175	9
176~275	10
276~425	11
426~625	12

表 B.1(续)

员工数量 人	ITSMS 初次审核时间 审核人日
626~875	13
876~1 175	14
1 176~1 550	15
1 551~2 025	16
2 026~2 675	17
2 676~3 450	18
3 451~4 350	19
4 351~5 450	20
5 451~6 800	21
6 801~8 500	22
8 501~10 700	23
>10 700	沿用以上规律

表 B.1 中涉及的“员工”是指工作活动与 ITSMS 范围有关的所有人员。所有轮班员工的数量是确定审核时间的起点。

“审核时间”包括审核组在第一阶段审核、第二阶段审核和策划(适当时,包括非现场文件评审)阶段所使用的时间,其中包括接触组织、人员、记录、文件和过程所用的时间,以及编制审核报告所用的时间。现场审核的时间不宜低于总审核时间的 80%,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 80%的时间。实施策划或撰写报告需要增加时间时,不应因此减少现场审核时间。审核时间不包括审核员的旅途时间。

注 1: 80%是一个基于 ITSMS 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、电话会议和(或)组织过程的电子验证],这些活动宜在审核计划中加以识别(见本标准 9.1.8),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,认证机构宜确定审核计划的适当性,并在实施前得到认可机构的特殊批准。

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被视为远程审核,即使电子审核在组织的物理场所进行。

表 B.1 中的“审核时间”是按照“审核人日”来说明的,一个审核人日是完整的正常工作时间(8 h)。

对于初次认证审核周期,对一个组织的监督时间宜与初次审核时间成比例,每年的监督审核时间大约是初次审核时间的三分之一。认证机构宜适时地核查其所策划的监督审核时间,以考虑组织的变更及管理体的成熟度等,至少宜在再认证审核时进行该核查。

再认证审核的审核全部时间取决于 GB/T 27021—2007 的 9.4.1.2 中所确定活动的结果,同时宜与同一组织的初次认证审核所用的时间成比例,大约是初次认证审核时间的三分之二。再认证审核时间遵照上述并超出例行的监督审核时间,但当再认证审核与计划的例行监督审核一起实施时,再认证审

核也应满足监督审核的要求。

对于明确了雇员数量的典型 ITSMS 范围,一旦确定了所需审核时间的常规基点后,除了本标准 9.1.5 中所列事项外,还需考虑进行一些调整,以便解决一些差异,这些差异可能影响到为实施一个有效的 ITSMS 审核所需的实际审核时间。

需要增加审核时间的因素,例如(但不限于):

- 多于一个工作场所;
- 员工使用不同的语言(需要翻译或影响审核员独立工作);
- 法律法规对其有较高的要求;
- 服务覆盖的过程非常复杂或有较多的特殊活动;
- 管理体系不成熟。

允许减少审核时间的因素,例如(但不限于):

- 相对员工人数而言,办公现场很小;
- 管理体系成熟;
- 从事同种、简单的工作的员工的比例高。

临时场所是认证文件所注明的场所和(或)位置以外的位置,其活动在认证范围内,并在规定的时间周期内实施。此类场所范围可从大项目管理场所到较小的服务或安装场所。是否需要访问这些场所及对其抽样范围的决定宜基于由于系统不符合所引起的未能满足需要或期望的服务的风险评价。所选择的场所样本宜考虑到活动的规模和类型,体现出组织的能力需求和服务变化的范围,以及项目进展的不同阶段。

宜考虑 ITSMS 范围、过程和服务的所有属性,并公平地对有效审核所需增加或减少审核时间的合理因素进行调整。增加时间的因素可被减少时间的因素冲抵。在任何情况下,对审核时间表中所提供时间的调整,应保持足够的证据和记录来证实其变化的合理性。

图 B.1 展示了在表 B.1 中的审核时间的增加因素和减少因素的潜在交互作用。

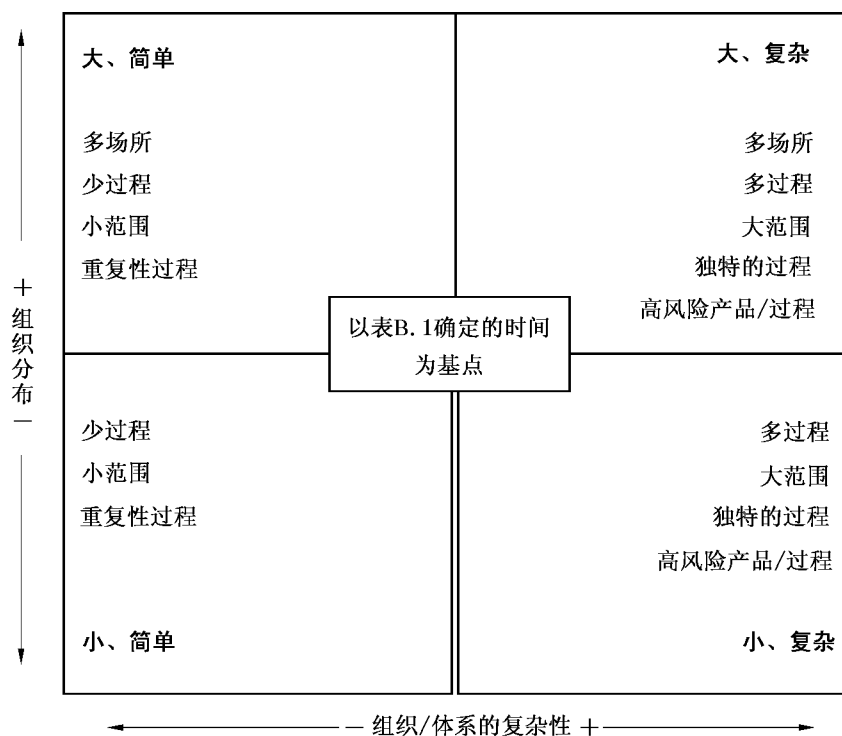


图 B.1 审核时间调整示意图