

ICS 35.040
L 80



中华人民共和国国家标准

GB/T 25067—2010/ISO/IEC 27006:2007

GB/T 25067—2010/ISO/IEC 27006:2007

信息技术 安全技术 信息安全管理体系审核认证机构的要求

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

(ISO/IEC 27006:2007, IDT)

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认证机构的要求
GB/T 25067—2010/ISO/IEC 27006:2007

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 2.25 字数 56 千字
2010年11月第一版 2010年11月第一次印刷

*

书号: 155066·1-40481 定价 33.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68533533



GB/T 25067-2010

2010-09-02 发布

2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

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	2
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	5
8.3 获证客户组织名录	5
8.4 认证的引用和标志的使用	5
8.5 保密性	5
8.6 认证机构与其客户组织间的信息交换	5
9 过程要求	5
9.1 通用要求	5
9.2 初次审核与认证	8
9.3 监督活动	10
9.4 再认证	11
9.5 特殊审核	11
9.6 暂停、撤销或缩小认证范围	11
9.7 申诉	11
9.8 投诉	11
9.9 申请组织和客户组织的记录	12
10 认证机构的管理体系要求	12
10.1 可选方式	12

10.2 方式一:按照 GB/T 19001—2008 的管理体系要求 12

10.3 方式二:通用的管理体系要求 12

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 13

附录 B (资料性附录) 审核员能力的示例 15

附录 C (资料性附录) 审核时间 17

附录 D (资料性附录) 对已实施的 GB/T 22080—2008 附录 A 的控制措施的评审指南 21

表 D.1 (续)

GB/T 22080—2008,附录 A 控制措施	组织类 控制措施	技术类 控制措施	系统测试	目视 检查	认证审核中的 评审指南
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 职责和规程	×				
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					管理评审记录
A.14.1.1 在业务连续性管理过程中包含信息安全	×				
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					
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 数据保护和个人隐私的隐私	×	×	可能的		
A.15.1.5 防止滥用信息处理设施	×				
A.15.1.6 密码控制措施的规则	×				
A.15.2 符合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 技术符合性核查	×	×			评估过程和跟踪
A.15.3 信息系统审计考虑					
A.15.3.1 信息系统审计控制措施	×				
A.15.3.2 信息系统审计工具的保护	×	×	可能的		