ICS 35.040
L 80

中华人民共和国国家标准

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)

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

GB/T 25067—2010/ISO/IEC 27006:2007

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

GB/T 25067-2010

目　　次

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		