

ICS 35.040  
L 80



# 中华人民共和国国家标准

GB/T 20945—2013  
代替 GB/T 20945—2007

GB/T 20945—2013

## 信息安全技术 信息系统安全审计产品 技术要求和测试评价方法

Information security technology—Technical requirements,  
testing and evaluation approaches for information system security audit product

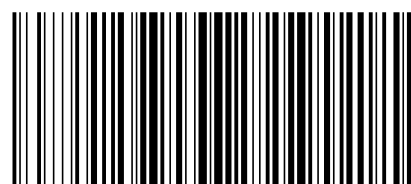
中华人民共和国  
国家标准  
信息安全技术 信息系统安全审计产品  
技术要求和测试评价方法  
GB/T 20945—2013

\*  
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.net.cn  
总编室:(010)64275323 发行中心:(010)51780235  
读者服务部:(010)68523946  
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 3 字数 86 千字  
2014年6月第一版 2014年6月第一次印刷

\*  
书号: 155066·1-49159 定价 42.00 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)68510107



GB/T 20945-2013

2013-12-31 发布

2014-07-15 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 ..... I

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 2

5 产品等级划分 ..... 2

  5.1 等级划分说明 ..... 2

  5.2 等级划分表 ..... 2

6 技术要求 ..... 5

  6.1 基本级技术要求 ..... 5

  6.2 增强级技术要求 ..... 9

7 测试评价方法 ..... 18

  7.1 基本级测试评价方法 ..... 18

  7.2 增强级测试评价方法 ..... 26

参考文献 ..... 43

## 参 考 文 献

[1] GB/T 18336.2—2008 信息技术 信息技术安全性评估准则 第 2 部分:安全功能要求 (ISO/IEC 15408-2:2005, IDT)

[2] GB/T 18336.3—2008 信息技术 信息技术安全性评估准则 第 3 部分:安全保证要求 (ISO/IEC 15408-3:2005, IDT)

---

- 1) 评价文档是否从用户可能破坏安全策略的明显途径出发,对系统的各种功能进行了分析;
  - 2) 对被确定的脆弱性,评价开发者是否明确记录了采取的措施;
  - 3) 对每一条脆弱性,评价是否能够显示在使用系统的环境中该脆弱性不能被利用。
- b) 预期结果:审查记录以及最后结果符合测试评价方法要求,开发者提供的脆弱性分析文档完整。

## 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 20945—2007《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》,本标准与 GB/T 20945—2007 的主要差异如下:

- 修改了“审计事件生成”功能(见 2007 版的 5.1.1);
- 修改了“统计分析”功能;
- 删除了“联动”(见 2007 版的 5.1.4.3)功能;
- 删除了“缺省策略”和“策略模板”和“策略定制”功能(见 2007 版的 5.1.7.2、5.1.7.3 和 5.1.7.4);
- 删除了“升级”功能;
- 删除了“监管要求”功能(见 2007 版的 5.6);
- 增加了“数据备份与恢复”功能;
- 删除了“性能要求”(见 2007 版的第 7 章)。

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。

本文件某些内容可能涉及专利,本文件的发布机构不承担识别这些专利的责任。

本标准起草单位:公安部计算机信息系统安全产品质量监督检验中心、深信服科技有限公司、蓝盾信息安全技术股份有限公司、厦门市美亚柏科信息股份有限公司。

本标准主要起草人:王志佳、沈亮、顾健、顾玮、邹春明、顾建新、赵云、胡维娜。