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

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

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

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。

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

1　范围

本标准规定了信息系统安全审计产品的技术要求和测试评价方法，技术要求包括安全功能要求、自身安全功能要求和安全保证要求，并提出了信息系统安全审计产品的分级要求。

本标准适用于信息系统安全审计产品的设计、开发、测试和评价。

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 17859　1999　计算机信息系统　安全保护等级划分准则

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB 17859—1999 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

事件　incident

试图改变目标状态，并造成或可能造成损害的行为的发生。

3.2

安全审计　security audit

对事件进行记录和分析，并针对特定事件采取相应比较的动作。

3.3

信息系统安全审计产品　information system security audit product

对信息系统的事件进行记录和分析，并针对特定事件采取相应比较动作的产品。

3.4

审计记录　audit recordation

审计产品记录审计目标事件得到的信息。

3.5

审计日志　audit log

审计产品记录自身事件得到的信息。

3.6

审计中心　audit center

审计产品中记录、分析、处理审计代理发送的事件的功能部件。

3.7

审计代理　audit agent

审计产品中采集事件并发送给审计中心的功能部件。

4 缩略语

下列缩略语适用于本文件。

CPU:中央处理器 (Central Processing Unit)

DoS:拒绝服务 (Denial of Service)

FTP:文件传输协议 (File Transfer Protocol)

HTML:超文本置标语言 (Hyper Text Markup Language)

HTTP:超文本传输协议 (Hypertext Transfer Protocol)

IM:即时通讯 (Instant Messenger)

IP:因特网协议 (Internet Protocol)

IT:信息技术 (Information Technology)

PDF:可移植文档格式 (Portable Document Format)

POP3:邮局协议第三版 (Post Office Protocol 3)

SMTP:简单邮件传输协议 (Simple Mail Transfer Protocol)

SNMP:简单网络管理协议 (Simple Network Management Protocol)

SQL:结构化查询语言 (Structured Query Language)

TCP:传输控制协议 (Transmission Control Protocol)

TELNET:远程登录 (Telecommunication Network)

UDP:用户数据报协议 (User Datagram Protocol)

URL:统一资源定位符 (Universal Resource Locator)

5 产品等级划分

5.1 等级划分说明

根据信息系统安全审计产品应提供的安全功能要求、自身安全功能要求和安全保证要求的强弱,将产品分为基本级和增强级。基本级规定了产品应提供的基本安全功能要求;自身安全功能要求依据GB 17859—1999 第二级:系统审计保护级相关要求。增强级规定了产品除具备基本级要求以外还应增强的安全功能要求;自身安全功能要求依据 GB 17859—1999 第三级:安全标记保护级相关要求。

信息系统安全审计产品的等级划分如表 1、表 2 和表 3 所示。对产品的等级评定是依据这三个表格的综合评定得出的,基本级产品应满足表 1、表 2、表 3 中所标明的基本级应满足的所有项目;增强级产品应满足表 1、表 2、表 3 中所标明的增强级应满足的所有项目。

5.2 等级划分表

5.2.1 安全功能要求等级划分

信息系统安全审计产品安全功能要求等级划分如表 1 所示。

表 1　安全功能要求等级划分表

安全功能要求			基本级	增强级
数据采集			*	*
审计分析	事件审计	主机事件审计	*	*
		网络事件审计	*	**
		数据库事件审计	*	**
		应用系统事件审计	*	*
	统计分析	统计	*	* *
		关联分析	—	*
		潜在危害分析		*
		异常事件分析		*
		扩展分析接口		*
审计结果	审计记录		*	*
	统计报表		*	*
	审计查阅		*	*
管理控制	图形界面		*	*
	事件分级		*	*
	事件告警		—	*
注："*"表示要求该功能；"**"表示要求该功能并有增强要求；" "表示不要求该功能。本标准中将基本级和增强级的技术要求和测试评价方法分别进行描述，其中"加粗字体"表示增强级较基本级增加的内容。				

5.2.2　自身安全功能要求等级划分

信息系统安全审计产品自身安全功能要求等级划分如表 2 所示。

表 2　自身安全功能要求等级划分表

自身安全要求		基本级	增强级
用户与鉴别	唯一性标识	*	*
	属性定义	*	*
	用户角色	—	*
	基本鉴别	*	*
	多重鉴别机制	—	*
	超时锁定或注销	—	*
	鉴别失败处理	*	*
	鉴别数据保护	*	*

表 2（续）

自身安全要求		基本级	增强级
数据传输安全	远程管理保密	*	*
	数据传输保密	—	*
	数据传输完整性	—	*
	安全状态监测	—	*
	审计代理安全	—	*
	分布式部署	—	*
	时间同步	*	*
数据存储安全	存储介质	*	*
	数据库支持	*	*
	备份与恢复	—	*
	数据删除	—	*
	存储空间耗尽处理	*	**
	数据存储完整性	*	*
审计日志		*	**

注：“*”表示要求该功能；“**”表示要求该功能并有增强要求；“—”表示不要求该功能。本标准中将基本级和增强级的技术要求和测试评价方法分别进行描述，其中“加粗字体”表示增强级较基本级增加的内容。

5.2.3 安全保证要求等级划分

信息系统安全审计产品安全保证要求等级划分如表 3 所示。

表 3 安全保证要求等级划分表

安全保证要求			基本级	增强级
配置管理	配置管理能力	版本号	*	*
		配置项		*
		授权控制	—	*
	配置管理覆盖		—	*
交付与运行	交付程序		—	*
	安装、生成和启动程序		*	*
开发	非形式化功能规范		*	*
	高层设计	描述性高层设计	—	*
		安全加强的高层设计	—	*
	非形式化对应性证实		*	*
指导性文档	管理员指南		*	*
	用户指南		*	*

表 3（续）

安全保证要求			基本级	增强级
生命周期支持				*
测试	测试覆盖	覆盖证据	*	*
		覆盖分析	—	*
	测试深度		—	*
	功能测试		—	*
	独立测试	一致性	*	*
		抽样		*
脆弱性分析保证	指南审查			*
脆弱性分析保证	产品安全功能强度评估		—	*
	开发者脆弱性分析		—	*
注：“*”表示要求该功能；“—”表示不要求该功能。本标准中将基本级和增强级的技术要求和测试评价方法分别进行描述，其中“加粗字体”表示增强级较基本级增加的内容。				

6 技术要求

6.1 基本级技术要求

6.1.1 安全功能要求

6.1.1.1 数据采集

信息系统安全审计产品应至少能够根据审计目标设置数据采集策略。

6.1.1.2 审计分析

6.1.1.2.1 事件审计

####### 6.1.1.2.1.1 主机事件审计

主机审计型信息系统安全审计产品应至少能够审计以下事件中的两种：

a) 主机启动和关闭；
b) 操作系统日志；
c) 网络连接；
d) 软硬件配置变更；
e) 外围设备使用；
f) 文件使用；
g) 其他事件。

####### 6.1.1.2.1.2 网络事件审计

网络审计型信息系统安全审计产品应能够审计以下事件：

a) FTP 通讯；

b) HTTP 通讯；
c) SMTP/POP3 通讯；
d) TELNET 通讯；
e) 其他网络协议或应用通讯。

6.1.1.2.1.3 数据库事件审计

数据库审计型信息系统安全审计产品应能够审计以下事件：
a) 数据库用户操作，包括用户登录鉴别、切换用户、用户授权等；
b) 数据库数据操作，包括数据的增加、删除、修改、查询等；
c) 数据库结构操作，包括新建、删除数据库或数据表等。

6.1.1.2.1.4 应用系统事件审计

应用系统审计型信息系统安全审计产品应至少能够审计以下事件中的两种：
a) 用户登录、注销；
b) 用户访问应用系统提供的服务；
c) 用户管理应用系统；
d) 应用系统出现系统资源超负荷或服务瘫痪等异常；
e) 应用系统遭到 DoS、SQL 注入、跨站脚本等攻击；
f) 其他应用系统事件。

6.1.1.2.2 统计

信息系统安全审计产品应能够以目标标识和事件类型等条件统计审计事件。

6.1.1.3 审计结果

6.1.1.3.1 审计记录

信息系统安全审计产品应能够把事件审计结果生成审计记录，内容要求如下：
a) 主机事件审计记录包括：日期时间、主机标识、事件主体、事件客体、事件描述等。
b) 网络事件审计记录除日期时间、源 IP、目的 IP 外，还包括：
   1) FTP、TELNET 通讯的用户名、操作命令等；
   2) HTTP 通讯的目标 URL 等；
   3) SMTP/POP3 通讯的发件邮箱、收件邮箱、邮件主题等；
   4) 其他网络协议或应用通讯的名称等。
c) 数据库事件审计记录包括：日期时间、客户端标识、数据库标识、操作命令等。
d) 应用系统事件审计记录包括：日期时间、应用系统标识、事件主体、事件客体、事件描述等。

6.1.1.3.2 统计报表

信息系统安全审计产品应能够把统计结果生成报表，并满足以下要求：
a) 报表包括文字和图像信息；
b) 报表可导出，至少支持 HTML、PDF、WORD、EXCEL 等文件格式中的一种。

6.1.1.3.3 审计查阅

信息系统安全审计产品应提供审计结果查阅功能，并满足以下要求：

a) 仅授权用户能访问审计结果；
b) 提供审计结果查看工具；
c) 提供按一定的条件查询、组合查询和排序审计记录的功能。

6.1.1.4 管理控制

6.1.1.4.1 图形界面

信息系统安全审计产品应为用户提供配置管理的图形界面。

6.1.1.4.2 事件分级

信息系统安全审计产品应能够设置事件分级策略以区分事件的安全级别，审计记录应包含事件分级信息。

6.1.2 自身安全功能要求

6.1.2.1 用户与鉴别

6.1.2.1.1 唯一性标识

信息系统安全审计产品应保证任何用户都具有全局唯一的标识。

6.1.2.1.2 属性定义

信息系统安全审计产品应为每个用户规定与之相关的安全属性，包括：用户标识、鉴别信息、权限等。

6.1.2.1.3 基本鉴别

信息系统安全审计产品应保证任何用户在执行产品的安全功能前都要进行身份鉴别。若其采用网络远程方式管理，还应对管理地址进行识别。

6.1.2.1.4 鉴别失败处理

信息系统安全审计产品应提供鉴别失败处理功能。用户连续鉴别失败达到最大失败次数后，阻止用户进一步的鉴别请求。最大失败次数仅由授权用户设定。

6.1.2.1.5 鉴别数据保护

信息系统安全审计产品应保证用户鉴别数据以非明文形式存储，不被未授权查看或修改。

6.1.2.2 数据传输安全

6.1.2.2.1 远程管理保密

信息系统安全审计产品若采用网络远程方式管理，应保证管理数据保密传输。

6.1.2.2.2 时间同步

信息系统安全审计产品若由多个组件组成，应提供各组件与审计中心或时钟服务器时间同步的功能。

6.1.2.3 数据存储安全

6.1.2.3.1 存储介质

信息系统安全审计产品应将审计记录和自身审计日志存储于掉电非易失性存储介质中。

6.1.2.3.2 数据库支持

信息系统安全审计产品应将审计记录与自身审计日志存储于数据库中。

6.1.2.3.3 存储空间耗尽处理

信息系统安全审计产品应提供数据存储空间耗尽处理功能，当剩余存储空间低于阈值时进行告警。

6.1.2.3.4 数据存储完整性

信息系统安全审计产品不应提供对数据进行添加、修改、删除的功能或接口，防止审计记录和自身审计日志被篡改。

6.1.2.4 审计日志

信息系统安全审计产品应能够生成自身审计日志，包括以下事件：

a) 身份鉴别，包括成功和失败；
b) 因鉴别失败次数超过了阈值而采取的禁止进一步尝试的措施；
c) 用户的增加、删除、修改；
d) 审计策略的增加、删除、修改；
e) 时间同步；
f) 存储空间达到阈值报警；
g) 其他事件。

自身审计日志内容应包括：日期时间、事件主体、事件客体、事件描述等。

6.1.3 安全保证要求

6.1.3.1 版本号

开发者应为产品的不同版本提供唯一的标识。

6.1.3.2 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

6.1.3.3 开发

6.1.3.3.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；
b) 是内在一致的；
c) 描述所有外部接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
d) 完备地表示产品安全功能。

6.1.3.3.2 非形式化对应性证实

开发者应在产品安全功能表示的所有相邻对之间提供对应性分析。

对于产品安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能在较具体的安全功能表示中得到正确且完备地细化。

6.1.3.4 指导性文档

6.1.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；

b) 怎样安全地管理产品；

c) 在安全处理环境中应被控制的功能和权限；

d) 所有对与产品的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；

g) 所有与管理员有关的 IT 环境安全要求。

6.1.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取但受安全处理环境所控制的所有功能和权限；

d) 产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

6.1.3.5 测试

6.1.3.5.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

6.1.3.5.2 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

6.2 增强级技术要求

6.2.1 安全功能要求

6.2.1.1 数据采集

信息系统安全审计产品应至少能够根据审计目标设置数据采集策略。

6.2.1.2 审计分析

6.2.1.2.1 事件审计

6.2.1.2.1.1 主机事件审计

主机审计型信息系统安全审计产品应至少能够审计以下事件中的两种：

a) 主机启动和关闭；
b) 操作系统日志；
c) 网络连接；
d) 软硬件配置变更；
e) 外围设备使用；
f) 文件使用；
g) 其他事件。

6.2.1.2.1.2 网络事件审计

网络审计型信息系统安全审计产品应能够审计以下事件：

a) 网络协议或应用审计，包括：
   1) FTP 通讯；
   2) HTTP 通讯；
   3) SMTP/POP3 通讯；
   4) TELNET 通讯；
   5) 其他网络协议或应用通讯。
b) 网络攻击审计，至少包括以下一种：
   1) DoS 攻击；
   2) 端口扫描攻击；
   3) 其他网络攻击。

6.2.1.2.1.3 数据库事件审计

数据库审计型信息系统安全审计产品应能够审计以下事件：

a) 数据库用户操作，包括用户登录鉴别、切换用户、用户授权等；
b) 数据库数据操作，包括数据的增加、删除、修改、查询等；
c) 数据库结构操作，包括新建、删除数据库或数据表等；
d) 数据库操作结果，包括数据库返回内容、操作成功或失败等。

6.2.1.2.1.4 应用系统事件审计

应用系统审计型信息系统安全审计产品应至少能够审计以下事件中的两种：

a) 用户登录、注销；
b) 用户访问应用系统提供的服务；
c) 用户管理应用系统；
d) 应用系统出现系统资源超负荷或服务瘫痪等异常；
e) 应用系统遭到 DoS、SQL 注入、跨站脚本等攻击；
f) 其他应用系统事件。

6.2.1.2.2 统计分析

6.2.1.2.2.1 统计

信息系统安全审计产品应提供统计功能，要求如下：

a) 事件统计：以目标标识和事件类型等条件统计审计事件；

b) 流量统计：网络审计型产品至少统计 TCP 协议、UDP 协议、网络应用等流量中的一种。

6.2.1.2.2.2 关联分析

信息系统安全审计产品应能够对相互关联的事件进行综合分析。

6.2.1.2.2.3 潜在危害分析

信息系统安全审计产品应提供潜在危害分析功能，设置某一事件累积发生的次数或频率超过阈值的情况为潜在危害事件。

6.2.1.2.2.4 异常事件分析

信息系统安全审计产品应至少能够分析以下异常事件中的一种：

a) 用户活动异常；

b) 系统资源滥用或耗尽；

c) 网络应用服务超负荷；

d) 网络通讯连接数剧增；

e) 其他异常事件。

6.2.1.2.2.5 扩展分析接口

信息系统安全审计产品应提供扩展分析接口，用户可通过该接口利用扩展事件分析模块分析自身无法分析的事件。

6.2.1.3 审计结果

6.2.1.3.1 审计记录

信息系统安全审计产品应能够把事件审计结果生成审计记录，内容要求如下：

a) 主机事件审计记录包括：日期时间、主机标识、事件主体、事件客体、事件描述等。

b) 网络事件审计记录除日期时间、源 IP、目的 IP 外，还包括：

1) FTP、TELNET 通讯的用户名、操作命令等；

2) HTTP 通讯的目标 URL 等；

3) SMTP/POP3 通讯的发件邮箱、收件邮箱、邮件主题等；

4) 网络攻击的类型等；

5) 其他网络协议或应用通讯的名称等。

c) 数据库事件审计记录包括：日期时间、客户端标识、数据库标识、操作命令、操作结果等。

d) 应用系统事件审计记录包括：日期时间、应用系统标识、事件主体、事件客体、事件描述等。

6.2.1.3.2 统计报表

信息系统安全审计产品应能够把统计结果生成报表，并满足以下要求：

a) 报表包括文字和图像信息；

b) 报表可导出，至少支持 HTML、PDF、WORD、EXCEL 等文件格式中的一种。

6.2.1.3.3 审计查阅

信息系统安全审计产品应提供审计结果查阅功能，并满足以下要求：

a) 仅授权用户能访问审计结果；

b) 提供审计结果查看工具；

c) 提供按一定的条件查询、组合查询和排序审计记录的功能。

6.2.1.4 管理控制

6.2.1.4.1 图形界面

信息系统安全审计产品应为用户提供配置管理的图形界面。

6.2.1.4.2 事件分级

信息系统安全审计产品应能够设置事件分级策略以区分事件的安全级别，审计记录应包含事件分级信息。

6.2.1.4.3 事件告警

信息系统安全审计产品应提供事件报警功能，并满足以下要求：

a) 至少支持屏幕报警、邮件告警、SNMP trap 告警、声光电告警、短信告警等方式中的一种；

b) 能够对高频发生的相同告警事件进行合并告警，避免出现告警风暴；

c) 能够记录告警事件，内容包括日期时间、告警事件描述、告警发生次数等。

6.2.2 自身安全功能要求

6.2.2.1 用户与鉴别

6.2.2.1.1 唯一性标识

信息系统安全审计产品应保证任何用户都具有全局唯一的标识。

6.2.2.1.2 属性定义

信息系统安全审计产品应为每个用户规定与之相关的安全属性，包括用户标识、鉴别信息、权限等。

6.2.2.1.3 用户角色

信息系统安全审计产品应设置多个用户角色并规定与之相关的权限，同时保证任何角色都具有全局唯一的标识。

6.2.2.1.4 基本鉴别

信息系统安全审计产品应保证任何用户在执行产品的安全功能前都要进行身份鉴别。若其采用网络远程方式管理，还应对管理地址进行识别。

6.2.2.1.5 多重鉴别机制

信息系统安全审计产品应向用户提供除口令以外的其他身份鉴别机制，至少包括以下一种：

a) 电子签名或证书鉴别；

b) 智能IC卡鉴别；
c) 指纹鉴别；
d) 虹膜鉴别；
e) 其他鉴别机制。

6.2.2.1.6 超时锁定或注销

信息系统安全审计产品应提供用户登录超时锁定或注销功能，终止超过最大超时时间仍没有任何操作用户的管理会话，需要再次进行身份鉴别才能继续管理操作。最大超时时间仅由授权用户设定。

6.2.2.1.7 鉴别失败处理

信息系统安全审计产品应提供鉴别失败处理功能。用户连续鉴别失败达到最大失败次数后，阻止用户进一步的鉴别请求。最大失败次数仅由授权用户设定。

6.2.2.1.8 鉴别数据保护

信息系统安全审计产品应保证用户鉴别数据以非明文形式存储，不被未授权查看或修改。

6.2.2.2 数据传输安全

6.2.2.2.1 远程管理保密

信息系统安全审计产品若采用网络远程方式管理，应保证管理数据保密传输。

6.2.2.2.2 数据传输保密

信息系统安全审计产品若由多个组件组成，应保证控制命令、采集数据等在组件间保密传输。

6.2.2.2.3 数据传输完整性

信息系统安全审计产品若由多个组件组成，应提供一定的技术手段防止组件间传输的数据被篡改。

6.2.2.2.4 安全状态监测

信息系统安全审计产品应能够监测组件状态，包括：
a) 能监测自身CPU、内存、存储空间等状态；
b) 产品若由多个组件组成，审计中心能够监测各组件的运行状态。

6.2.2.2.5 审计代理安全

信息系统安全审计产品若包括软件审计代理组件，软件审计代理应能够保护自身安全，包括：
a) 进程具备自动加载措施，在审计目标操作系统启动时自动加载，并防止被取消自动加载；
b) 进程具备保护措施，防止被强制终止；
c) 程序具备防卸载措施，卸载时至少提供口令保护；
d) 程序具备完整性检查措施，防止程序文件被篡改。

6.2.2.2.6 分布式部署

信息系统安全审计产品应支持多级分布式部署模式，并满足以下要求：
a) 能够设置集中审计中心和审计分中心；
b) 某一审计分中心异常不影响集中审计中心和其他审计分中心正常运行；

c) 集中审计中心能够对审计分中心下发数据采集策略；
d) 集中审计中心能够收集审计分中心上传的审计记录，记录中包括审计分中心标识；
e) 集中审计中心能够对上传的各审计分中心采集的数据进行集中统计分析。

6.2.2.2.7 时间同步

信息系统安全审计产品若由多个组件组成，应提供各组件与审计中心或时钟服务器时间同步的功能。

6.2.2.3 数据存储安全

6.2.2.3.1 存储介质

信息系统安全审计产品应将审计记录和自身审计日志存储于掉电非易失性存储介质中。

6.2.2.3.2 数据库支持

信息系统安全审计产品应将审计记录与自身审计日志存储于数据库中。

6.2.2.3.3 备份与恢复

信息系统安全审计产品应提供审计记录的备份恢复功能，并满足以下要求：
a) 能够对指定时间段的数据进行备份；
b) 备份出的数据文件采取保护措施，防止被未授权查看；
c) 能够根据备份文件恢复数据。

6.2.2.3.4 数据删除

信息系统安全审计产品应提供审计记录和自身审计日志的删除功能，并满足以下要求：
a) 不应提供有选择性地手动删除审计记录和自身审计日志的功能；
b) 能够设置审计记录和自身审计日志的保存时限，自动删除超过保存时限的数据；
c) 若产品为软件，卸载时能够删除审计记录和自身审计日志或提醒用户删除。

6.2.2.3.5 存储空间耗尽处理

信息系统安全审计产品应提供数据存储空间耗尽处理功能，当剩余存储空间低于阈值时进行告警。在存储空间耗尽前，能够采用自动转储等方式将数据备份到其他存储空间。

6.2.2.3.6 数据存储完整性

信息系统安全审计产品不应提供对数据进行添加、修改、删除的功能或接口，防止审计记录和自身审计日志被篡改。

6.2.2.4 审计日志

信息系统安全审计产品应能够生成自身审计日志，包括以下事件：
a) 身份鉴别，包括成功和失败；
b) 因鉴别失败次数超过了阈值而采取的禁止进一步尝试的措施；
c) 用户的增加、删除、修改；
d) 审计策略的增加、删除、修改；
e) 时间同步；

f) 软件审计代理的卸载；

g) 超过保存时限的审计记录和自身审计日志的自动删除；

h) 审计日志和审计记录的备份与恢复；

i) 存储空间达到阈值报警；

j) 其他事件。

自身审计日志内容应包括日期时间、事件主体、事件客体、事件描述等。

6.2.3 安全保证要求

6.2.3.1 配置管理

6.2.3.1.1 配置管理能力

6.2.3.1.1.1 版本号

开发者应为产品的不同版本提供唯一的标识。

6.2.3.1.1.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效维护的证据。

6.2.3.1.1.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

6.2.3.1.2 配置管理覆盖

配置管理范围至少应包括产品交付与运行文档、开发文档、指导性文档、生命周期支持文档、测试文档、脆弱性分析文档和配置管理文档，从而确保它们的修改是在一个正确授权的可控方式下进行的。

配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

6.2.3.2 交付与运行

6.2.3.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

6.2.3.2.2 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

6.2.3.3 开发

6.2.3.3.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；

b) 是内在一致的；
c) 描述所有外部接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
d) 完备地表示产品安全功能。

6.2.3.3.2 高层设计

6.2.3.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：
a) 表示是非形式化的；
b) 是内在一致的；
c) 按子系统描述安全功能的结构；
d) 描述每个安全功能子系统所提供的安全功能性；
e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 标识安全功能子系统的所有接口；
g) 标识安全功能子系统的哪些接口是外部可见的。

6.2.3.3.2.2 安全加强的高层设计

开发者提供的安全加强的高层设计应满足以下要求：
a) 描述产品的功能子系统所有接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
b) 把产品分成安全策略实施和其他子系统来描述。

6.2.3.3.3 非形式化对应性证实

开发者应在产品安全功能表示的所有相邻对之间提供对应性分析。

对于产品安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能在较具体的安全功能表示中得到正确且完备地细化。

6.2.3.4 指导性文档

6.2.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：
a) 管理员可使用的管理功能和接口；
b) 怎样安全地管理产品；
c) 在安全处理环境中应被控制的功能和权限；
d) 所有对与产品的安全操作有关的用户行为的假设；
e) 所有受管理员控制的安全参数，如果可能，指明安全值；
f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
g) 所有与管理员有关的 IT 环境安全要求。

6.2.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取但受安全处理环境所控制的所有功能和权限；

d) 产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

6.2.3.5 生命周期支持

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并应提供在产品的开发和维护过程中执行安全措施的证据。

6.2.3.6 测试

6.2.3.6.1 测试覆盖

6.2.3.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

6.2.3.6.1.2 覆盖分析

开发者应提供测试覆盖的分析。

测试覆盖分析应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。

6.2.3.6.2 测试深度

开发者应提供测试深度的分析。

测试深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

6.2.3.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，标识要测试的安全功能，并描述测试的目标；

b) 测试过程，标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对于其他测试结果的顺序依赖性；

c) 预期的测试结果，表明测试成功后的预期输出；

d) 实际测试结果，表明每个被测试的安全功能按照规定进行运作。

6.2.3.6.4 独立测试

6.2.3.6.4.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

6.2.3.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

6.2.3.7 脆弱性分析保证

6.2.3.7.1 指南审查

开发者应提供指导性文档，指导性文档应满足以下要求：

a) 标识所有可能的产品运行模式(包括失败或操作失误后的运行)、它们的后果以及对于保持安全运行的意义；
b) 是完备的、清晰的、一致的、合理的；
c) 列出关于预期使用环境的所有假设；
d) 列出对外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求。

6.2.3.7.2 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度的度量。

6.2.3.7.3 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

7 测试评价方法

7.1 基本级测试评价方法

7.1.1 安全功能测试评价方法

7.1.1.1 数据采集

信息系统安全审计产品的数据采集功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 根据审计目标设置产品的采集策略；
   2) 在该审计目标进行可审计事件操作；
   3) 查看产品对以上事件的审计记录。
b) 预期结果：产品能够根据审计目标设置数据采集策略。

7.1.1.2 审计分析

7.1.1.2.1 事件审计

7.1.1.2.1.1 主机事件审计

信息系统安全审计产品的主机事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；
2) 启动和关闭目标主机；
3) 在目标主机进行操作系统操作，生成操作系统日志；
4) 在目标主机进行网络连接操作；
5) 更改目标主机的软硬件配置；
6) 使用目标主机的外围设备；
7) 在目标主机进行文件的添加、修改、删除等操作；
8) 在目标主机进行其他可审计事件操作；
9) 查看产品对以上主机事件的审计记录。

b) 预期结果：主机审计型产品至少能够审计以上两种主机事件。

7.1.1.2.1.2 网络事件审计

信息系统安全审计产品的网络事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；
2) 在目标主机或网络登录某个 FTP 服务器并做文件操作；
3) 在目标主机或网络访问某个 HTTP 网页；
4) 在目标主机或网络通过 SMTP/POP3 发收邮件；
5) 在目标主机或网络登录某个 TELNET 服务器并做远程操作；
6) 在目标主机或网络进行其他网络协议或应用通讯操作；
7) 查看产品对以上网络协议或应用事件的审计记。

b) 预期结果：网络审计型产品能够审计以上网络协议或应用事件。

7.1.1.2.1.3 数据库事件审计

信息系统安全审计产品的数据库事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；
2) 在目标数据库服务器进行用户登录鉴别、切换用户、用户授权等数据库用户操作；
3) 在目标数据库服务器进行数据的增加、删除、修改、查询等数据库数据操作；
4) 在目标数据库服务器进行新建、删除数据库或数据表等数据库结构操作；
5) 查看产品对以上数据库操作的审计记录。

b) 预期结果：数据库审计型产品能够审计以上数据库操作事件。

7.1.1.2.1.4 应用系统事件审计

信息系统安全审计产品的应用系统事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；
2) 登录、注销目标应用系统；
3) 访问目标应用系统提供的服务；
4) 管理目标应用系统；
5) 在目标应用系统模拟系统资源超负荷或服务瘫痪等异常；
6) 采用 DoS、SQL 注入、跨站脚本等方式攻击目标应用系统；

7) 在目标应用系统进行其他可审计事件操作；

8) 查看产品对以上应用系统事件的审计记录。

b) 预期结果：应用系统审计型产品至少能够审计以上两种应用系统事件。

7.1.1.2.2 统计

信息系统安全审计产品的统计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；

2) 在多个审计目标进行可审计事件操作；

3) 在审计目标进行多种类型可审计事件操作；

4) 分别查看产品以目标标识和事件类型等条件统计审计事件的结果；

5) 重复以上事件操作；

6) 查看以上统计结果的变化。

b) 预期结果：产品能够以目标标识和事件类型等条件统计审计事件。

7.1.1.3 审计结果

7.1.1.3.1 审计记录

信息系统安全审计产品的审计记录功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 查看主机事件审计记录的日期时间、主机标识、事件主体、事件客体、事件描述等信息；

2) 查看网络事件审计记录的日期时间、源 IP、目的 IP 等信息，此外查看 FTP、TELNET 通讯的用户名、操作命令等信息，HTTP 通讯的目标 URL 等信息，SMTP/POP3 通讯的发件邮箱、收件邮箱、邮件主题等信息，其他网络协议或应用通讯的名称等信息；

3) 查看数据库事件审计记录的日期时间、客户端标识、数据库标识、操作命令等信息；

4) 查看应用系统事件审计记的日期时间、应用系统标识、事件主体、事件客体、事件描述等信息。

b) 预期结果：产品能够把事件审计结果生成审计记录，相应审计记录内容包括以上信息。

7.1.1.3.2 统计报表

信息系统安全审计产品的统计报表功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 查看产品的统计结果并生成报表；

2) 查看报表的文字和图像信息；

3) 以 HTML、PDF、WORD、EXCEL 等格式导出报表并查看导出的报表。

b) 预期结果：

1) 产品能够把统计结果生成报表；

2) 统计报表包括文字和图像信息；

3) 报表可导出，至少支持 HTML、PDF、WORD、EXCEL 等文件格式中的一种。

7.1.1.3.3 审计查阅

信息系统安全审计产品的审计查阅功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 分别尝试以非授权用户和授权用户查看产品的审计结果；
2) 以一定的条件对审计记录进行查询、组合查询和排序。

b) 预期结果：
1) 仅授权用户能够访问产品的审计结果；
2) 提供审计结果查看工具；
3) 提供按一定的条件查询、组合查询和排序审计记录的功能。

7.1.1.4 管理控制

7.1.1.4.1 图形界面

信息系统安全审计产品的图形界面功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 登录产品图形界面并设置产品的采集策略；
2) 在审计目标进行可审计事件操作；
3) 在产品图形界面进行审计结果查看等操作。

b) 预期结果：产品能够为用户提供配置管理的图形界面。

7.1.1.4.2 事件分级

信息系统安全审计产品的事件分级功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 设置产品的采集策略和事件分级策略；
2) 在审计目标进行不同级别审计事件操作；
3) 查看产品不同级别的审计记录。

b) 预期结果：
1) 产品能够设置事件分级策略；
2) 审计记录包含事件分级信息。

7.1.2 自身安全测试评价方法

7.1.2.1 用户与鉴别

7.1.2.1.1 唯一性标识

信息系统安全审计产品的唯一性标识功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 查看产品的用户信息；
2) 尝试新建一个相同用户标识的用户。

b) 预期结果：产品不能建立相同用户标识的用户，任何用户标识全局唯一。

7.1.2.1.2 属性定义

信息系统安全审计产品的属性定义功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 查看产品用户的用户标识、鉴别信息、权限等信息；
2) 以用户标识、鉴别信息、权限等信息新建用户。

b) 预期结果：产品能够为每个用户规定与之相关的安全属性，包括用户标识、鉴别信息、权限等。

7.1.2.1.3 基本鉴别

信息系统安全审计产品的基本鉴别功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 尝试在未鉴别的情况下使用产品功能；
   2) 尝试以非授权用户鉴别并使用产品功能；
   3) 设置产品的远程管理地址限制功能；
   4) 分别以授权和非授权的地址尝试鉴别并登录产品。
b) 预期结果：
   1) 任何用户在执行产品的安全功能前都要进行身份鉴别；
   2) 能够对网络远程管理地址进行识别。

7.1.2.1.4 鉴别失败处理

信息系统安全审计产品的鉴别失败处理功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 设置产品的最大鉴别失败次数；
   2) 以错误的鉴别信息尝试鉴别，重复操作达到最大鉴别失败次数；
   3) 该用户以正确的鉴别信息尝试鉴别；
   4) 以非授权用户尝试设置最大失败次数。
b) 预期结果：
   1) 产品提供鉴别失败处理功能；
   2) 最大失败次数仅由授权用户设定。

7.1.2.1.5 鉴别数据保护

信息系统安全审计产品的鉴别数据保护功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 登录后台数据库查看产品的用户鉴别数据；
   2) 分别以非授权和授权用户尝试查看或修改用户鉴别数据。
b) 预期结果：
   1) 产品的用户鉴别数据以非明文形式存储；
   2) 用户鉴别数据不被未授权查看或修改。

7.1.2.2 数据传输安全

7.1.2.2.1 远程管理保密

信息系统安全审计产品的远程管理保密功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 鉴别登录产品并进行配置管理操作；
   2) 截获鉴别和管理的通讯数据并查看数据内容。
b) 预期结果：产品远程管理数据保密。

7.1.2.2.2 时间同步

信息系统安全审计产品的时间同步功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 在审计中心对各组件下发与审计中心或时钟服务器时间同步的命令；

2) 各组件设置与审计中心或时钟服务器时间同步的策略；

3) 在各组件查看同步后的时间。

b) 预期结果：产品能够同步各组件与审计中心或时钟服务器的时间。

7.1.2.3 数据存储安全

7.1.2.3.1 数据存储介质

信息系统安全审计产品的数据存储介质功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 在产品进行各种配置管理操作，生成自身审计日志；

2) 在审计目标进行可审计事件操作，生成审计记录；

3) 关闭产品电源后重新启动；

4) 查看审计记录和自身审计日志。

b) 预期结果：产品将审计记录和自身审计日志存储于掉电非易失性存储介质中。

7.1.2.3.2 数据库支持

信息系统安全审计产品的数据库支持功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 登录产品后台数据库；

2) 查看数据库类型版本、审计记录和自身审计日志。

b) 预期结果：产品将审计记录与自身审计日志存储于数据库中。

7.1.2.3.3 存储空间耗尽处理

信息系统安全审计产品的存储空间耗尽处理功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品存储空间报警阈值；

2) 在审计目标进行大量可审计事件操作或直接拷贝大文件填充存储空间直至达到报警阈值；

3) 查看报警。

b) 预期结果：产品在剩余存储空间低于阈值时能够进行告警。

7.1.2.3.4 数据完整性

信息系统安全审计产品的数据完整性功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 以授权用户尝试对数据进行添加、修改和删除；

2) 以非授权用户尝试对数据进行添加、修改和删除。

b) 预期结果：产品不提供对数据进行添加、修改、删除的功能或接口。

7.1.2.4 审计日志

信息系统安全审计产品的审计日志功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 以错误的鉴别信息连续鉴别失败达到最大鉴别失败次数；
2) 以正确的身份鉴别信息进行鉴别；
3) 进行用户和角色的增加、删除、修改操作；
4) 进行审计策略的增加、删除、修改操作；
5) 进行时间同步操作；
6) 设置存储空间报警阈值，填充存储空间直至存储空间达到阈值报警；
7) 进行其他操作；
8) 查看以上操作的审计日志，查看审计日志的日期时间、事件主体、事件客体、事件描述等信息。

b) 预期结果：
1) 产品能够审计以上事件；
2) 审计日志包括日期时间、事件主体、事件客体、事件描述等信息。

7.1.3 安全保证测试评价方法

7.1.3.1 版本号

信息系统安全审计产品的版本号的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者提供的配置管理支持文件是否包含以下内容：版本号，要求开发者所使用的版本号与所表示的产品样本完全对应，没有歧义。

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，开发者提供唯一版本号。

7.1.3.2 安装、生成和启动程序

信息系统安全审计产品的安装、生成和启动程序的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者是否提供了文档说明系统的安装、生成、启动和使用的过程，用户是否通过此文档了解安装、生成、启动和使用过程。

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，评价者审查内容应说明系统的安装、生成、启动和使用的过程符合测试评价方法要求。

7.1.3.3 开发

7.1.3.3.1 非形式化功能规范

信息系统安全审计产品的非形式化功能规范的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者所提供的信息是否满足如下要求：

1) 功能设计使用非形式化风格来描述产品安全功能与其外部接口；
2) 功能设计是内在一致的；
3) 功能设计描述使用所有外部产品安全功能接口的目的与方法，适当的时候，提供结果影响例外情况和出错信息的细节；
4) 功能设计完整地表示产品安全功能。

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，评价者审查内容至少包括测试评价方法中的四个方面。开发者提供的内容精确和完整。

7.1.3.3.2 非形式化对应性证实

信息系统安全审计产品的非形式化对应性证实的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者是否在产品安全功能表示的所有相邻对之间提供对应性分析。其中，系统各种安全功能表示（如系统功能设计、高层设计、低层设计、实现表示）之间的对应性是所提供的抽象产品安全功能表示要求的精确而完整的示例。产品安全功能在功能设计中进行细化，并且较为抽象的产品安全功能表示的所有相关安全功能部分，在较具体的产品安全功能表示中进行细化。

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，评价者审查内容至少包括功能设计、高层设计、底层设计、实现表示这四项。开发者提供的内容精确和完整，并互相对应。

7.1.3.4 指导性文档

7.1.3.4.1 管理员指南

信息系统安全审计产品的管理员指南的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者是否提供了供授权管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

1) 产品可以使用的管理功能和接口；
2) 怎样安全地管理产品；
3) 在安全处理环境中应进行控制的功能和权限；
4) 所有对与产品的安全操作有关的用户行为的假设；
5) 所有受管理员控制的安全参数，如果可能，指明安全值；
6) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；
7) 所有与授权管理员有关的 IT 环境的安全要求。

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，评价者审查内容至少包括测试评价方法中的七方面。开发者提供的管理员指南完整。

7.1.3.4.2 用户指南

信息系统安全审计产品的用户指南的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

1) 产品的非管理用户可使用的安全功能和接口；
2) 产品提供给用户的安全功能和接口的用法；
3) 用户可获取但受安全处理环境控制的所有功能和权限；
4) 产品安全操作中用户所应承担的职责；
5) 与用户有关的 IT 环境的所有安全要求。

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，评价者审查内容至少包括测试评价方法中的五方面。开发者提供的用户指南完整。

7.1.3.5 测试

7.1.3.5.1 覆盖证据

信息系统安全审计产品的覆盖证据的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者提供的测试覆盖证据，在测试覆盖证据中是否表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

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，开发者提供的测试覆盖证据表明

测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

7.1.3.5.2 一致性

信息系统安全审计产品的一致性的测试评价方法和预期结果如下：

a) 测试评价方法：评价者评价开发者提供的测试产品，提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

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，开发者提供适合测试的产品，提供的测试集合、执行的测试及其结果与其自测系统功能时使用的测试集合、执行的测试及其结果相一致。

7.2 增强级测试评价方法

7.2.1 安全功能测试评价方法

7.2.1.1 数据采集

信息系统安全审计产品的数据采集功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 根据审计目标设置产品的采集策略；
2) 在该审计目标进行可审计事件操作；
3) 查看产品对以上事件的审计记录。

b) 预期结果：产品能够根据审计目标设置数据采集策略。

7.2.1.2 审计分析

7.2.1.2.1 事件审计

7.2.1.2.1.1 主机事件审计

信息系统安全审计产品的主机事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；
2) 启动和关闭目标主机；
3) 在目标主机进行操作系统操作，生成操作系统日志；
4) 在目标主机进行网络连接操作；
5) 更改目标主机的软硬件配置；
6) 使用目标主机的外围设备；
7) 在目标主机进行文件的添加、修改、删除等操作；
8) 在目标主机进行其他可审计事件操作；
9) 查看产品对以上主机事件的审计记录。

b) 预期结果：主机审计型产品至少能够审计以上两种主机事件。

7.2.1.2.1.2 网络事件审计

信息系统安全审计产品的网络事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 网络协议或应用审计：

设置产品的采集策略；

——在目标主机或网络登录某个 FTP 服务器并做文件操作；
——在目标主机或网络访问某个 HTTP 网页；
——在目标主机或网络通过 SMTP/POP3 发收邮件；
——在目标主机或网络登录某个 TELNET 服务器并做远程操作；
——在目标主机或网络进行其他网络协议或应用通讯操作；
——查看产品对以上网络协议或应用事件的审计记。

2) 网络攻击审计：
——设置产品的采集策略；
——通过 DoS 攻击工具对目标主机或网络进行攻击；
——通过端口扫描工具对目标主机或网络进行攻击；
——应用其他攻击工具对目标主机或网络进行攻击；
——查看产品对以上网络攻击事件的审计记录。

b) 预期结果：
1) 网络审计型产品能够审计以上网络协议或应用事件；
2) 网络审计型产品至少能够审计以上一种网络攻击事件。

7.2.1.2.1.3 数据库事件审计

信息系统安全审计产品的数据库事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 设置产品的采集策略；
2) 在目标数据库服务器进行用户登录鉴别、切换用户、用户授权等数据库用户操作；
3) 在目标数据库服务器进行数据的增加、删除、修改、查询等数据库数据操作；
4) 在目标数据库服务器进行新建、删除数据库或数据表等数据库结构操作；
5) 查看产品对以上数据库操作事件的审计记录，查看以上数据库操作结果记录。

b) 预期结果：数据库审计型产品能够审计以上数据库操作事件和操作结果。

7.2.1.2.1.4 应用系统事件审计

信息系统安全审计产品的应用系统事件审计功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 设置产品的采集策略；
2) 登录、注销目标应用系统；
3) 访问目标应用系统提供的服务；
4) 管理目标应用系统；
5) 在目标应用系统模拟系统资源超负荷或服务瘫痪等异常；
6) 采用 DoS、SQL 注入、跨站脚本等方式攻击目标应用系统；
7) 在目标应用系统进行其他可审计事件操作；
8) 查看产品对以上应用系统事件的审计记录。

b) 预期结果：应用系统审计型产品至少能够审计以上两种应用系统事件。

7.2.1.2.2 统计分析

7.2.1.2.2.1 统计

信息系统安全审计产品的统计功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 事件统计：

——设置产品的采集策略；

——在多个审计目标进行可审计事件操作；

——在审计目标进行多种类型可审计事件操作；

——分别查看产品以目标标识和事件类型等条件统计审计事件的结果；

——重复以上事件操作；

——查看以上统计结果的变化。

2) 流量统计：

——设置网络审计型产品的采集策略；

——在目标主机或网络进行大流量 TCP 协议网络事件操作；

——在目标主机或网络进行大流量 UDP 协议网络事件操作；

——在目标主机或网络进行大流量网络应用事件操作；

——在目标主机或网络进行大流量其他网络事件操作；

——查看产品统计 TCP 协议流量、UDP 协议流量、网络应用流量、其他网络流量的结果；

——重复以上网络事件操作；

——查看以上统计结果的变化。

b) 预期结果：

1) 产品能够以目标标识和事件类型等条件统计审计事件；

2) 网络审计型产品至少能够统计以上流量中的一种。

7.2.1.2.2.2 关联分析

信息系统安全审计产品的关联分析功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；

2) 在审计目标进行相互关联的事件操作；

3) 查看对以上相互关联事件进行综合分析的结果。

b) 预期结果：产品能够对相互关联的事件进行综合分析。

7.2.1.2.2.3 潜在危害分析

信息系统安全审计产品的潜在危害分析功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；

2) 定义某一事件为潜在危害事件，并设置此事件发生的次数或频率阈值；

3) 在审计目标重复进行该潜在危害事件操作，直至其次数或频率超过阈值；

4) 查看产品对该潜在危害事件分析的结果。

b) 预期结果：产品能够分析潜在危害事件。

7.2.1.2.2.4 异常事件分析

信息系统安全审计产品的异常事件分析功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；

2) 在审计目标进行异常活动的操作；

3) 在审计目标进行耗费系统资源的操作，导致审计目标系统资源滥用或耗尽；
4) 在审计目标进行耗费应用服务的操作，导致审计目标网络应用超负荷；
5) 在审计目标进行大量网络通讯连接操作，导致网络通讯连接数剧增；
6) 在审计目标进行其他异常事件；
7) 查看产品对以上异常事件分析的结果。

b) 预期结果：产品至少能够分析以上一种异常事件。

7.2.1.2.2.5 扩展分析接口

信息系统安全审计产品的扩展分析接口功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 设置产品的采集策略；
2) 在审计目标进行产品无法分析的事件操作；
3) 查看产品对以上事件分析的结果；
4) 在审计分析接口中增加以对上事件的审计分析模块；
5) 在审计目标重复以上事件操作；
6) 查看产品对以上事件分析的结果。

b) 预期结果：产品能够提供扩展分析接口。

7.2.1.3 审计结果

7.2.1.3.1 审计记录

信息系统安全审计产品的审计记录功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 查看主机事件审计记录的日期时间、主机标识、事件主体、事件客体、事件描述等信息；
2) 查看网络事件审计记录的日期时间、源 IP、目的 IP 等信息，此外查看 FTP、TELNET 通讯的用户名、操作命令等信息，HTTP 通讯的目标 URL 等信息，SMTP/POP3 通讯的发件邮箱、收件邮箱、邮件主题等信息，网络攻击的类型等信息，其他网络协议或应用通讯的名等信息；
3) 查看数据库事件审计记录的日期时间、客户端标识、数据库标识、操作命令、操作结果等信息；
4) 查看应用系统事件审计记的日期时间、应用系统标识、事件主体、事件客体、事件描述等信息。

b) 预期结果：产品能够把事件审计结果生成审计记录，相应审计记录内容包括以上信息。

7.2.1.3.2 统计报表

信息系统安全审计产品的统计报表功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 查看产品的统计结果并生成报表；
2) 查看报表的文字和图像信息；
3) 以 HTML、PDF、WORD、EXCEL 等格式导出报表并查看导出的报表。

b) 预期结果：
1) 产品能够把统计结果生成报表；
2) 统计报表包括文字和图像信息；

3） 报表可导出，至少支持 HTML、PDF、WORD、EXCEL 等文件格式中的一种。

7.2.1.3.3 审计查阅

信息系统安全审计产品的审计查阅功能的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 分别尝试以非授权用户和授权用户查看产品的审计结果；

2） 以一定的条件对审计记录进行查询、组合查询和排序。

b） 预期结果：

1） 仅授权用户能够访问产品的审计结果；

2） 提供审计结果查看工具；

3） 提供按一定的条件查询、组合查询和排序审计记录的功能。

7.2.1.4 管理控制

7.2.1.4.1 图形界面

信息系统安全审计产品的图形界面功能的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 登录产品图形界面并设置产品的采集策略；

2） 在审计目标进行可审计事件操作；

3） 在产品图形界面进行审计结果查看等操作。

b） 预期结果：产品能够为用户提供配置管理的图形界面。

7.2.1.4.2 事件分级

信息系统安全审计产品的事件分级功能的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 设置产品的采集策略和事件分级策略；

2） 在审计目标进行不同级别审计事件操作；

3） 查看产品不同级别的审计记录。

b） 预期结果：

1） 产品能够设置事件分级策略；

2） 审计记录包含事件分级信息。

7.2.1.4.3 事件告警

信息系统安全审计产品的事件告警功能的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 设置产品的采集策略和告警事件；

2） 以屏幕报警、邮件告警、SNMP trap 告警、声光电告警、短信告警等方式设置告警方式；

3） 在审计目标进行告警事件操作；

4） 查看告警并查看报警记录中的日期时间、告警事件描述、告警发生次数等信息；

5） 在审计目标短时间内进行大量相同的告警事件操作；

6） 查看告警并查看报警记录中的日期时间、告警事件描述、告警发生次数等信息。

b） 预期结果：

1） 产品能够设置事件报警策略；

2） 至少支持屏幕报警、邮件告警、SNMP trap 告警、声光电告警、短信告警等方式中的一种；
3） 能够对高频发生的相同告警事件进行合并告警；
4） 能够记录告警事件，内容包括日期时间、告警事件描述、告警发生次数等。

7.2.2 自身安全测试评价方法

7.2.2.1 用户与鉴别

7.2.2.1.1 唯一性标识

信息系统安全审计产品的唯一性标识功能的测试评价方法和预期结果如下：

a） 测试评价方法：
1） 查看产品的用户信息；
2） 尝试新建一个相同用户标识的用户。

b） 预期结果：产品不能建立相同用户标识的用户，任何用户都具有全局唯一的标识。

7.2.2.1.2 属性定义

信息系统安全审计产品的属性定义功能的测试评价方法和预期结果如下：

a） 测试评价方法：
1） 查看产品用户的用户标识、鉴别信息、权限等信息；
2） 以用户标识、鉴别信息、权限等信息新建用户。

b） 预期结果：产品能够为每个用户规定与之相关的安全属性，包括用户标识、鉴别信息、权限等。

7.2.2.1.3 用户角色

信息系统安全审计产品的用户角色功能的测试评价方法和预期结果如下：

a） 测试评价方法：
1） 查看产品的角色信息；
2） 尝试新建一个相同角色标识的角色；
3） 建立两个不同的角色，赋予不同的权限；
4） 建立两个不同的用户，分别赋予以上两种角色；
5） 分别以这两个用户登录产品，查看其权限。

b） 预期结果：
1） 产品能够设置多个用户角色并规定与之相关的权限；
2） 任何角色都具有全局唯一的标识。

7.2.2.1.4 基本鉴别

信息系统安全审计产品的基本鉴别功能的测试评价方法和预期结果如下：

a） 测试评价方法：
1） 尝试在未鉴别的情况下使用产品功能；
2） 尝试以非授权用户鉴别并使用产品功能；
3） 设置产品的远程管理地址限制功能；
4） 分别以授权和非授权的地址尝试鉴别并登录产品。

b） 预期结果：
1） 任何用户在执行产品的安全功能前都要进行身份鉴别；
2） 能够对网络远程管理地址进行识别。

7.2.2.1.5 多重鉴别机制

信息系统安全审计产品的多重鉴别机制的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 启用产品的多重鉴别机制；
   2) 配置电子签名或证书、IC卡、指纹、虹膜等鉴别机制；
   3) 以口令和以上其他鉴别方式组合鉴别登录产品。
b) 预期结果：产品能够向用户提供除口令以外的其他身份鉴别机制，至少包括以上一种。

7.2.2.1.6 超时锁定或注销

信息系统安全审计产品的超时锁定或注销功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 设置产品的最大超时时间；
   2) 不做任何操作直至超过最大超时时间；
   3) 尝试继续管理操作，重新鉴别后尝试继续管理操作；
   4) 尝试以非授权用户设置最大超时时间。
b) 预期结果：
   1) 产品能够提供用户登录超时锁定或注销功能；
   2) 最大超时时间仅由授权用户设定。

7.2.2.1.7 鉴别失败处理

信息系统安全审计产品的鉴别失败处理功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 设置产品的最大鉴别失败次数；
   2) 以错误的鉴别信息尝试鉴别，重复操作达到最大鉴别失败次数；
   3) 该用户以正确的鉴别信息尝试鉴别；
   4) 以非授权用户尝试设置最大失败次数。
b) 预期结果：
   1) 产品提供鉴别失败处理功能；
   2) 最大失败次数仅由授权用户设定。

7.2.2.1.8 鉴别数据保护

信息系统安全审计产品的鉴别数据保护功能的测试评价方法和预期结果如下：

a) 测试评价方法：
   1) 登录后台数据库查看产品的用户鉴别数据；
   2) 分别以非授权和授权用户尝试查看或修改用户鉴别数据。
b) 预期结果：
   1) 产品的用户鉴别数据以非明文形式存储；
   2) 用户鉴别数据不被未授权查看或修改。

7.2.2.2 数据传输安全

7.2.2.2.1 远程管理保密

信息系统安全审计产品的远程管理保密功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 鉴别登录产品并进行配置管理操作；

2) 截获鉴别和管理的通讯数据并查看数据内容。

b) 预期结果：产品网络远程管理数据保密。

7.2.2.2.2 数据传输保密

信息系统安全审计产品的数据传输保密功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；

2) 在审计目标进行可审计事件操作；

3) 截获组件间传输的控制命令、采集数据等数据并查看数据内容。

b) 预期结果：产品组件间传输的控制命令、采集数据等保密。

7.2.2.2.3 数据传输完整性

信息系统安全审计产品的数据传输完整性功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品的采集策略；

2) 在审计目标进行可审计事件操作；

3) 截获组件间传输的控制命令、采集数据等数据并查看数据内容；

4) 尝试篡改数据并重放数据。

b) 预期结果：产品能够提供一定的技术手段防止远程传输的数据被篡改。

7.2.2.2.4 安全状态监测

信息系统安全审计产品的安全状态监测功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 查看产品自身的 CPU、内存、存储空间等状态；

2) 在审计目标进行大量可审计事件操作，使产品 CPU、内存、存储空间等发生变化；

3) 重新查看产品自身的 CPU、内存、存储空间等状态；

4) 在审计中心查看各组件的运行状态；

5) 在各组件进行导致运行状态变化的操作；

6) 重新在审计中心查看各组件的运行状态。

b) 预期结果：

1) 产品能够监测自身 CPU、内存、存储空间等状态；

2) 审计中心能够监测各组件的运行状态。

7.2.2.2.5 审计代理安全

信息系统安全审计产品的审计代理安全功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 启动审计目标操作系统，查看代理状态；
2) 在审计目标尝试取消代理的启动时自动加载功能；
3) 尝试强制终止审计代理进程；
4) 尝试不验证口令直接卸载审计代理，尝试验证口令后卸载审计代理；
5) 尝试篡改审计代理的程序文件。

b) 预期结果：
1) 产品代理进程具备自动加载措施，并防止被取消自动加载；
2) 代理进程具备保护措施，防止被强制终止；
3) 代理程序具备防卸载措施，卸载时至少提供口令保护；
4) 代理程序具备完整性检查措施，防止程序文件被篡改。

7.2.2.2.6 分布式部署

信息系统安全审计产品的分布式部署功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 设置至少一个集中审计中心和两个审计分中心；
2) 关闭一个审计分中心，查看集中审计中心和另一个审计分中心工作状态；
3) 从集中审计中心向审计分中心下发数据采集策略；
4) 在审计分中心查看下发的数据采集策略；
5) 在集中审计中心查看审计分中心上传的审计记录，并查看审计记录中的审计分中心标识；
6) 在审计中心对各审计分中心上传的数据进行集中统计分析。

b) 预期结果：
1) 产品能够设置集中审计中心和审计分中心；
2) 某一审计分中心异常不影响集中审计中心和其他审计分中心正常运行；
3) 集中审计中心能够对审计分中心下发数据采集策略；
4) 集中审计中心能够收集审计分中心上传的审计记录，记录中包括审计分中心标识；
5) 集中审计中心能够对上传的各审计分中心采集的数据进行集中统计分析。

7.2.2.2.7 时间同步

信息系统安全审计产品的时间同步功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 在审计中心对各组件下发与审计中心或时钟服务器时间同步的命令；
2) 各组件设置与审计中心或时钟服务器时间同步的策略；
3) 在各组件查看同步后的时间。

b) 预期结果：产品能够同步各组件与审计中心或时钟服务器的时间。

7.2.2.3 数据存储安全

7.2.2.3.1 数据存储介质

信息系统安全审计产品的数据存储介质功能的测试评价方法和预期结果如下：

a) 测试评价方法：
1) 在产品进行各种配置管理操作，生成自身审计日志；
2) 在审计目标进行可审计事件操作，生成审计记录；
3) 关闭产品电源后重新启动；

4) 查看审计记录和自身审计日志。

b) 预期结果：产品将审计记录和自身审计日志存储于掉电非易失性存储介质中。

7.2.2.3.2 数据库支持

信息系统安全审计产品的数据库支持功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 登录产品后台数据库；

2) 查看数据库类型版本、审计记录和自身审计日志。

b) 预期结果：产品将审计记录与自身审计日志存储于数据库中。

7.2.2.3.3 数据备份与恢复

信息系统安全审计产品的数据备份与恢复功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 选择某个时间范围内的审计记录进行备份；

2) 尝试以非授权用户查看该备份文件；

3) 删除已备份的审计记录，用备份文件恢复数据；

4) 查看恢复的审计记录。

b) 预期结果：

1) 产品能够对指定时间段的数据进行备份；

2) 备份出的数据文件采取保护措施，能够防止被未授权查看；

3) 能够根据备份文件恢复数据。

7.2.2.3.4 数据删除

信息系统安全审计产品的数据删除功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 尝试手动删除某一条或某种条件的审计记录或自身审计日志；

2) 设置审计记录和自身审计日志的保存时限并删除超过保存时限数据的策略；

3) 在数据超过保存时限后，查看审计记录和自身审计日志；

4) 卸载产品，查看提醒用户删除审计记录和审计日志的提示；

5) 登录后台数据库查看卸载后的审计记录和自身审计日志。

b) 预期结果：

1) 产品不提供有选择性地手动删除审计记录和自身审计日志的功能；

2) 能够设置审计记录和自身审计日志的保存时限，自动删除超过保存时限的数据；

3) 软件产品卸载时能够删除审计记录和自身审计日志或提醒用户删除。

7.2.2.3.5 存储空间耗尽处理

信息系统安全审计产品的存储空间耗尽处理功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 设置产品存储空间报警阈值，设置转储策略；

2) 在审计目标进行大量可审计事件操作或直接拷贝大文件填充存储空间直至达到报警阈值；

3) 查看报警；

4) 查看转储服务器上转储的数据。

b) 预期结果：

1) 产品在剩余存储空间低于阈值时能够进行告警；

2) 在存储空间耗尽前，能够采用自动转储等方式将数据备份到其他存储空间。

7.2.2.3.6 数据完整性

信息系统安全审计产品的数据完整性功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 以授权用户尝试对数据进行添加、修改和删除；

2) 以非授权用户尝试对数据进行添加、修改和删除。

b) 预期结果：产品不提供对数据进行添加、修改、删除的功能或接口。

7.2.2.4 审计日志

信息系统安全审计产品的审计日志功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 以错误的鉴别信息连续鉴别失败达到最大鉴别失败次数；

2) 以正确的身份鉴别信息进行鉴别；

3) 进行用户和角色的增加、删除、修改操作；

4) 进行审计策略的增加、删除、修改操作；

5) 进行时间同步操作；

6) 卸载审计代理；

7) 设置审计记录和自身审计日志的保存时限，生成超过保存时限的审计记录和自身审计日志自动删除事件；

8) 备份和恢复审计记录；

9) 设置存储空间报警阈值，填充存储空间直至存储空间达到阈值报警；

10) 进行其他操作；

11) 查看以上操作的审计日志，查看审计日志的日期时间、事件主体、事件客体、事件描述等信息。

b) 预期结果：

1) 产品能够审计以上事件；

2) 审计日志包括日期时间、事件主体、事件客体、事件描述等信息。

7.2.3 安全保证测试评价方法

7.2.3.1 配置管理

7.2.3.1.1 配置管理能力

7.2.3.1.1.1 版本号

信息系统安全审计产品的版本号的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者提供的配置管理支持文件是否包含以下内容：版本号，要求开发者所使用的版本号与所表示的产品样本完全对应，没有歧义。

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，开发者提供唯一版本号。

7.2.3.1.1.2 配置项

信息系统安全审计产品的配置项的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者提供的信息是否满足如下要求：

1) 配置管理系统对所有的配置项做出唯一的标识；

2) 配置管理文档包括配置清单、配置管理计划，配置清单用来描述组成系统的配置项；

3) 配置管理文档还描述对配置项给出唯一标识的方法。

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，评价者审查内容至少包括测试评价方法中的三方面。

7.2.3.1.1.3 授权控制

信息系统安全审计产品的授权控制的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者提供的信息是否满足如下要求：

1) 配置管理系统保证只有经过授权才能修改配置项；

2) 在配置管理计划中，描述配置管理系统是如何使用的。实施的配置管理与配置管理计划相一致；

3) 配置管理文档还提供所有的配置项得到有效地维护的证据。

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，评价者审查内容至少包括测试评价方法中的三方面。开发者提供的配置管理内容完整。

7.2.3.1.2 配置管理覆盖

信息系统安全审计产品的配置管理覆盖的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者提供的配置管理支持文件是否包含以下内容：

1) 产品配置管理范围，将系统的交付与运行文档、开发文档、指导性文档、生命周期支持文档、测试文档、脆弱性分析文档和配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此：

——开发者所提供的配置管理文档展示配置管理系统至少跟踪上述配置管理之下的内容；

——文档描述配置管理系统是如何跟踪这些配置项的；

——文档还提供足够的信息表明达到所有要求。

2) 问题跟踪配置管理范围，除产品配置管理范围描述的内容外，特别强调对安全缺陷的跟踪。

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，评价者审查产品受控于配置管理。

7.2.3.2 交付与运行

7.2.3.2.1 交付程序

信息系统安全审计产品的交付程序的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者是否使用一定的交付程序交付系统，并使用文档描述交付过程，并且评价者审查开发者交付的文档是否包含以下内容：在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

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，开发者提供完整的文档描述所有交付的过程(文档和程序交付)。

7.2.3.2.2 安装、生成和启动程序

信息系统安全审计产品的安装、生成和启动程序的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者是否提供了文档说明系统的安装、生成、启动和使用的过程，用户是否通过此文档了解安装、生成、启动和使用过程。

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，评价者审查内容应说明系统的安装、生成、启动和使用的过程符合测试评价方法要求。

7.2.3.3 开发

7.2.3.3.1 非形式化功能规范

信息系统安全审计产品的非形式化功能规范的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者所提供的信息是否满足如下要求：

1) 功能设计使用非形式化风格来描述产品安全功能与其外部接口；

2) 功能设计是内在一致的；

3) 功能设计描述使用所有外部产品安全功能接口的目的与方法，适当的时候，提供结果影响例外情况和出错信息的细节；

4) 功能设计完整地表示产品安全功能。

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，评价者审查内容至少包括测试评价方法中的四个方面。开发者提供的内容精确和完整。

7.2.3.3.2 高层设计

7.2.3.3.2.1 描述性高层设计

信息系统安全审计产品的描述性高层设计的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者所提供的信息是否满足如下要求：

1) 表示是非形式化的；

2) 是内在一致的；

3) 按子系统描述安全功能的结构；

4) 描述每个安全功能子系统所提供的安全功能性；

5) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；

6) 标识安全功能子系统的所有接口；

7) 标识安全功能子系统的哪些接口是外部可见的。

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，评价者审查内容至少包括测试评价方法中的七个方面。开发者提供的高层设计内容精确和完整。

7.2.3.3.2.2 安全加强的高层设计

信息系统安全审计产品的安全加强的高层设计的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者所提供的安全加强高层设计是否满足如下要求：

1) 描述系统的功能子系统所有接口的用途与使用方法，适当时提供效果、例外情况和错误消息的

细节；

2) 把系统分成安全策略实施和其他子系统来描述。

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，评价者审查内容至少包括测试评价方法中的两个方面。

7.2.3.3.3 非形式化对应性证实

信息系统安全审计产品的非形式化对应性证实的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者是否在产品安全功能表示的所有相邻对之间提供对应性分析。其中，系统各种安全功能表示（如系统功能设计、高层设计、低层设计、实现表示）之间的对应性是所提供的抽象产品安全功能表示要求的精确而完整的示例。产品安全功能在功能设计中进行细化，并且较为抽象的产品安全功能表示的所有相关安全功能部分，在较具体的产品安全功能表示中进行细化。

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，评价者审查内容至少包括功能设计、高层设计、低层设计、实现表示这四项。开发者提供的内容精确和完整，并互相对应。

7.2.3.4 指导性文档

7.2.3.4.1 管理员指南

信息系统安全审计产品的管理员指南的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者是否提供了供授权管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

1) 产品可以使用的管理功能和接口；

2) 怎样安全地管理产品；

3) 在安全处理环境中应进行控制的功能和权限；

4) 所有对与产品的安全操作有关的用户行为的假设；

5) 所有受管理员控制的安全参数，如果可能，指明安全值；

6) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

7) 所有与授权管理员有关的 IT 环境的安全要求。

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，评价者审查内容至少包括测试评价方法中的七方面。开发者提供的管理员指南完整。

7.2.3.4.2 用户指南

信息系统安全审计产品的用户指南的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

1) 产品的非管理用户可使用的安全功能和接口；

2) 产品提供给用户的安全功能和接口的用法；

3) 用户可获取但受安全处理环境控制的所有功能和权限；

4) 产品安全操作中用户所应承担的职责；

5) 与用户有关的 IT 环境的所有安全要求。

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，评价者审查内容至少包括测试评

价方法中的五方面。开发者提供的用户指南完整。

7.2.3.5 生命周期支持

信息系统安全审计产品的生命周期支持的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者所提供的开发安全文档是否满足如下要求：描述在系统的开发环境中，为保护系统设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并提供在系统的开发和维护过程中执行安全措施的证据。

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，开发者提供的开发安全文档完整。

7.2.3.6 测试

7.2.3.6.1 测试覆盖

7.2.3.6.1.1 覆盖证据

信息系统安全审计产品的覆盖证据的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者提供的测试覆盖证据，在测试覆盖证据中是否表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

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，开发者提供的测试覆盖证据表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

7.2.3.6.1.2 覆盖分析

信息系统安全审计产品的覆盖分析的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者提供的测试覆盖分析，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的，评价测试文档中所标识的测试是否完整。

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，开发者提供的测试文档中所标识的测试与安全功能设计中所描述的安全功能对应，并且标识的测试覆盖所有安全功能。

7.2.3.6.2 测试深度

信息系统安全审计产品的测试深度的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者提供的测试深度分析，是否表明了测试文档中所标识的对安全功能的测试，足以证实该产品的功能和高层设计是一致的。

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，评价者测试和审查与安全功能相对应的测试，这些测试保证测试出的安全功能符合高层设计的要求。

7.2.3.6.3 功能测试

信息系统安全审计产品的功能测试的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者所提供的测试文档，是否包括如下内容：

1) 测试计划、测试过程、预期的测试结果和实际测试结果；
2) 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；
3) 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况(这些概况包括对其他测试结果的顺序依赖性)；
4) 评价预期的测试结果是否表明测试成功后的预期输出；
5) 评价实际测试结果是否表明每个被测试的安全功能按照规定进行运作。

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，评价者审查内容至少包括测试评

价方法中的五方面。开发者提供的测试文档内容完整。

7.2.3.6.4 独立测试

7.2.3.6.4.1 一致性

信息系统安全审计产品的一致性的测试评价方法和预期结果如下：

a) 测试评价方法：评价者评价开发者提供的测试产品，提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

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，开发者提供适合测试的产品，提供的测试集合、执行的测试及其结果与其自测系统功能时使用的测试集合、执行的测试及其结果相一致。

7.2.3.6.4.2 抽样

信息系统安全审计产品的抽样的测试评价方法和预期结果如下：

a) 测试评价方法：评价者评价开发者是否提供一组相当的资源，用于安全功能的抽样测试。

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，开发者和测试执行者提供一组相当的资源，用于安全功能的抽样测试。

7.2.3.7 脆弱性分析保证

7.2.3.7.1 指南审查

信息系统安全审计产品的指南审查的测试评价方法和预期结果如下：

a) 测试评价方法：评价者应审查开发者提供的文档，是否满足了以下要求：

1) 评价文档是否确定了对产品的所有可能的操作方式(包括失败和操作失误后的操作)，是否确定了它们的后果，以及是否确定了对于保持安全操作的意义；

2) 评价文档是否完整、清晰、一致、合理；

3) 评价文档是否列出了所有目标环境的假设；

4) 评价文档是否列出了所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。

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，评价者审查内容至少包括测试评价方法中的四方面。开发者提供的文档内容完整。

7.2.3.7.2 系统安全功能强度评估

信息系统安全审计产品的系统安全功能强度评估的测试评价方法和预期结果如下：

a) 测试评价方法：评价者审查开发者提供的指导性文档，是否对所标识的每个具有安全功能强度声明的安全机制进行了安全功能强度分析，是否说明了安全机制达到或超过定义的最低强度级别或特定功能强度的度量。

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，开发者对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度的度量。

7.2.3.7.3 开发者脆弱性分析

信息系统安全审计产品的开发者脆弱性分析的测试评价方法和预期结果如下：

a) 测试评价方法：

评价者应审查开发者提供的脆弱性分析文档，是否满足了以下要求：

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。

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)

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

GB/T 20945-2013

打印日期:2014年7月28日 F055