4) 应测试验证相关系统或组件的配置信息或安全策略是否有效。

d) 单元判定：如果 1)～4)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.3.3 测评单元(L4-ABS1-14)

该测评单元包括以下要求：

a) 测评指标：应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

b) 测评对象：抗 APT 攻击系统、网络回溯系统和威胁情报检测系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否部署相关系统或组件对新型网络攻击进行检测和分析；

2) 应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.3.4 测评单元(L4-ABS1-15)

该测评单元包括以下要求：

a) 测评指标：当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查相关系统或组件的记录是否包括攻击源 IP、攻击类型、攻击目标、攻击时间等相关内容；

2) 应测试验证相关系统或组件的报警策略是否有效。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.4 恶意代码和垃圾邮件防范

9.1.3.4.1 测评单元(L4-ABS1-16)

该测评单元包括以下要求：

a) 测评指标：应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

b) 测评对象：防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查在关键网络节点处是否部署防恶意代码产品等技术措施；

2) 应核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新；

3) 应测试验证相关系统或组件的安全策略是否有效。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.4.2 测评单元(L4-ABS1-17)

该测评单元包括以下要求：

a) 测评指标：应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

b) 测评对象：防垃圾邮件网关等提供防垃圾邮件功能的系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查在关键网络节点处是否部署了防垃圾邮件产品等技术措施；

2) 应核查防垃圾邮件产品运行是否正常，防垃圾邮件规则库是否已经更新到最新；

3) 应测试验证相关系统或组件的安全策略是否有效。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.5 安全审计

9.1.3.5.1 测评单元(L4-ABS1-18)

该测评单元包括以下要求：

a) 测评指标：应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) 测评对象：综合安全审计系统等。

c) 测评实施包括以下内容：

1) 应核查是否部署了综合安全审计系统或类似功能的系统平台；

2) 应核查安全审计范围是否覆盖到每个用户；

3) 应核查是否对重要的用户行为和重要安全事件进行了审计。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.5.2 测评单元(L4-ABS1-19)

该测评单元包括以下要求：

a) 测评指标：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

b) 测评对象：综合安全审计系统等。

c) 测评实施：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.5.3 测评单元(L4-ABS1-20)

该测评单元包括以下要求：

a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

b) 测评对象：综合安全审计系等。

c) 测评实施包括以下内容：

1) 应核查是否采取了技术措施能够对审计记录进行保护；

2） 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.6 可信验证

9.1.3.6.1 测评单元（L4-ABS1-21）

该测评单元包括以下要求：

a） 测评指标：可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

b） 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。

c） 测评实施包括以下内容：

1） 应核查是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证；

2） 应核查是否在应用程序的所有执行环节进行动态可信验证；

3） 应测试验证当检测到边界设备的可信性受到破坏后是否进行报警；

4） 应测试验证结果是否以审计记录的形式送至安全管理中心；

5） 应核查是否能够进行动态关联感知。

d） 单元判定：如果 1）～5）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4 安全计算环境

9.1.4.1 身份鉴别

9.1.4.1.1 测评单元（L4-CES1-01）

该测评单元包括以下要求：

a） 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c） 测评实施包括以下内容：

1） 应核查用户在登录时是否采用了身份鉴别措施；

2） 应核查用户列表确认用户身份标识是否具有唯一性；

3） 应核查用户配置信息或测试验证是否不存在空口令用户；

4） 应核查用户鉴别信息是否具有复杂度要求并定期更换。

d） 单元判定：如果 1）～4）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.1.2 测评单元（L4-CES1-02）

该测评单元包括以下要求：

a) 测评指标：应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

b) 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否配置并启用了登录失败处理功能；

2) 应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账户锁定等；

3) 应核查是否配置并启用了登录连接超时及自动退出功能。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.1.3 测评单元（L4-CES1-03）

该测评单元包括以下要求：

a) 测评指标：当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

b) 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施：应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.1.4 测评单元（L4-CES1-04）

该测评单元包括以下要求：

a) 测评指标：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

b) 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别；

2) 应核查其中一种鉴别技术是否使用密码技术来实现。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2 访问控制

9.1.4.2.1 测评单元(L4-CES1-05)

该测评单元包括以下要求：

a) 测评指标：应对登录的用户分配账户和权限。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否为用户分配了账户和权限及相关设置情况；

2) 应核查是否已禁用或限制匿名、默认账户的访问权限。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.2 测评单元(L4-CES1-06)

该测评单元包括以下要求：

a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否已经重命名默认账户或默认账户已被删除；

2) 应核查是否已修改默认账户的默认口令。

d) 单元判定：如果 1)或 2)为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.3 测评单元(L4-CES1-07)

该测评单元包括以下要求：

a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应；

2) 应测试验证多余的、过期的账户是否被删除或停用。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.4 测评单元(L4-CES1-08)

该测评单元包括以下要求：

a) 测评指标:应授予管理用户所需的最小权限,实现管理用户的权限分离。

b) 测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容:

1) 应核查是否进行角色划分;

2) 应核查管理用户的权限是否已进行分离;

3) 应核查管理用户权限是否为其工作任务所需的最小权限。

d) 单元判定:如果1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.4.2.5 测评单元(L4-CES1-09)

该测评单元包括以下要求:

a) 测评指标:应由授权主体配置访问控制策略,访问控制策略规定主体对客体的访问规则。

b) 测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容:

1) 应核查是否由授权主体(如管理用户)负责配置访问控制策略;

2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则;

3) 应测试验证用户是否有可越权访问情形。

d) 单元判定:如果1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.4.2.6 测评单元(L4-CES1-10)

该测评单元包括以下要求:

a) 测评指标:访问控制的粒度应达到主体为用户级或进程级,客体为文件、数据库表级。

b) 测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施:应核查访问控制策略的控制粒度是否达到主体为用户级或进程级,客体为文件、数据库表、记录或字段级。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.1.4.2.7 测评单元(L4-CES1-11)

该测评单元包括以下要求:

a) 测评指标:应对主体、客体设置安全标记,并依据安全标记和强制访问控制规则确定主体对客体的访问。

b) 测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否对主体、客体设置了安全标记；

2) 应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3 安全审计

9.1.4.3.1 测评单元(L4-CES1-12)

该测评单元包括以下要求：

a) 测评指标：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否开启了安全审计功能；

2) 应核查安全审计范围是否覆盖到每个用户；

3) 应核查是否对重要的用户行为和重要安全事件进行审计。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3.2 测评单元(L4-CES1-13)

该测评单元包括以下要求：

a) 测评指标：审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施：应核查审计记录信息是否包括事件的日期和时间、主体标识、客体标识、事件类型、事件是否成功及其他与审计相关的信息。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.3.3 测评单元(L4-CES1-14)

该测评单元包括以下要求：

a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1） 应核查是否采取了保护措施对审计记录进行保护；

2） 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

d） 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3.4 测评单元（L4-CES1-15）

该测评单元包括以下要求：

a） 测评指标：应对审计进程进行保护，防止未经授权的中断。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c） 测评实施：应测试验证通过非审计管理员的其他账户来中断审计进程，验证审计进程是否受到保护。

d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.4 入侵防范

9.1.4.4.1 测评单元（L4-CES1-16）

该测评单元包括以下要求：

a） 测评指标：应遵循最小安装的原则，仅安装需要的组件和应用程序。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。

c） 测评实施包括以下内容：

1） 应核查是否遵循最小安装原则；

2） 应核查是否未安装非必要的组件和应用程序。

d） 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.4.2 测评单元（L4-CES1-17）

该测评单元包括以下要求：

a） 测评指标：应关闭不需要的系统服务、默认共享和高危端口。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。

c） 测评实施包括以下内容：

1） 应核查是否关闭了非必要的系统服务和默认共享；

2） 应核查是否不存在非必要的高危端口。

d） 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.4.3 测评单元(L4-CES1-18)

该测评单元包括以下要求:

a) 测评指标:应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

b) 测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。

c) 测评实施:应核查配置文件或参数等是否对终端接入范围进行限制。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.1.4.4.4 测评单元(L4-CES1-19)

该测评单元包括以下要求:

a) 测评指标:应提供数据有效性检验功能,保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

b) 测评对象:业务应用系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容:

1) 应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块;

2) 应测试验证是否对人机接口或通信接口输入的内容进行有效性检验。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.4.4.5 测评单元(L4-CES1-20)

该测评单元包括以下要求:

a) 测评指标:应能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞。

b) 测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件等。

c) 测评实施包括以下内容:

1) 应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞;

2) 应核查是否在经过充分测试评估后及时修补漏洞。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.4.4.6 测评单元(L4-CES1-21)

该测评单元包括以下要求:

a) 测评指标:应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警。

b) 测评对象:终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。

c) 测评实施包括以下内容:

1） 应访谈并核查是否有入侵检测的措施；

2） 应核查在发生严重入侵事件时是否提供报警。

d） 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.5 恶意代码防范

9.1.4.5.1 测评单元（L4-CES1-22）

该测评单元包括以下要求：

a） 测评指标：应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、移动终端、移动终端管理系统、移动终端管理客户端和控制设备等。

c） 测评实施包括以下内容：

1） 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为；

2） 应核查当识别入侵和病毒行为时，是否将其有效阻断。

d） 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.6 可信验证

9.1.4.6.1 测评单元（L4-CES1-23）

该测评单元包括以下要求：

a） 测评指标：可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

b） 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。

c） 测评实施包括以下内容：

1） 应核查是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证；

2） 应核查是否在应用程序的所有执行环节进行动态可信验证；

3） 应测试验证当检测到计算设备的可信性受到破坏后是否进行报警；

4） 应测试验证结果是否以审计记录的形式送至安全管理中心；

5） 应核查是否能够进行动态关联感知。

d） 单元判定：如果 1)～5)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.7 数据完整性

9.1.4.7.1 测评单元（L4-CES1-24）

该测评单元包括以下要求：

a） 测评指标：应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

b） 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

c) 测评实施包括以下内容：

1) 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性；

2) 应测试验证在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.7.2 测评单元(L4-CES1-25)

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

c) 测评实施包括以下内容：

1) 应核查设计文档，是否采用了密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；

2) 应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；

3) 应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.7.3 测评单元(L4-CES1-26)

该测评单元包括以下要求：

a) 测评指标：在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

b) 测评对象：业务应用系统和数据库管理系统等。

c) 测评实施包括以下内容：

1) 应核查设计文档，是否采用了密码技术保证数据发送和数据接收操作的不可抵赖性；

2) 应核查是否采取技术措施保证数据发送和数据接收操作的不可抵赖性；

3) 应测试验证是否能够检测到数据在传输过程中不能被篡改。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.8 数据保密性

9.1.4.8.1 测评单元(L4-CES1-27)

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重

要业务数据和重要个人信息等。

b) 测评对象：业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计文档，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；

2) 应通过嗅探等方式抓取传输过程中的数据包，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。

d) 单元判定：如果1)和2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.8.2 测评单元(L4-CES1-28)

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

c) 测评实施包括以下内容：

1) 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；

2) 应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；

3) 应测试验证是否对指定的数据进行加密处理。

d) 单元判定：如果1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.9 数据备份恢复

9.1.4.9.1 测评单元(L4-CES1-29)

该测评单元包括以下要求：

a) 测评指标：应提供重要数据的本地数据备份与恢复功能。

b) 测评对象：配置数据和业务数据。

c) 测评实施包括以下内容：

1) 应核查是否按照备份策略进行本地备份；

2) 应核查备份策略设置是否合理、配置是否正确；

3) 应核查备份结果是否与备份策略一致；

4) 应核查近期恢复测试记录是否能够进行正常的数据恢复。

d) 单元判定：如果1)～4)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.9.2 测评单元(L4-CES1-30)

该测评单元包括以下要求：

a) 测评指标：应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

b) 测评对象：配置数据和业务数据。

c) 测评实施：应核查是否提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.9.3 测评单元(L4-CES1-31)

该测评单元包括以下要求：

a) 测评指标：应提供重要数据处理系统的热冗余，保证系统的高可用性。

b) 测评对象：重要数据处理系统。

c) 测评实施：应核查重要数据处理系统(包括边界路由器、边界防火墙、核心交换机、应用服务器和数据库服务器等)是否采用热冗余方式部署。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.9.4 测评单元(L4-CES1-32)

该测评单元包括以下要求：

a) 测评指标：应建立异地灾难备份中心，提供业务应用的实时切换。

b) 测评对象：灾难备份中心及相关组件。

c) 测评实施包括以下内容：

1) 应核查是否建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备；

2) 应核查是否提供业务应用的实时切换功能。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.10 剩余信息保护

9.1.4.10.1 测评单元(L4-CES1-33)

该测评单元包括以下要求：

a) 测评指标：应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

b) 测评对象：终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施：应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.10.2 测评单元(L4-CES1-34)

该测评单元包括以下要求：

a) 测评指标：应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

b) 测评对象：终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施：应核查相关配置信息或系统设计文档，敏感数据所在的存储空间被释放或重新分配