元指标要求。

7.1.1.6.2 测评单元(L2-PES1-10)

该测评单元包括以下要求：

a) 测评指标：应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房内是否采取了防止水蒸气结露的措施；

2) 应核查机房内是否采取了排泄地下积水，防止地下积水渗透的措施。

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。

7.1.1.7 防静电

7.1.1.7.1 测评单元(L2-PES1-11)

该测评单元包括以下要求：

a) 测评指标：应采用防静电地板或地面并采用必要的接地防静电措施。

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房内是否安装了防静电地板或地面；

2) 应核查机房内是否采用了接地防静电措施。

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。

7.1.1.8 温湿度控制

7.1.1.8.1 测评单元(L2-PES1-12)

该测评单元包括以下要求：

a) 测评指标：应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

b) 测评对象：机房温湿度调节设施。

c) 测评实施包括以下内容：

1) 应核查机房内是否配备了专用空调；

2) 应核查机房内温湿度是否在设备运行所允许的范围之内。

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。

7.1.1.9 电力供应

7.1.1.9.1 测评单元(L2-PES1-13)

该测评单元包括以下要求：

a) 测评指标：应在机房供电线路上配置稳压器和过电压防护设备。

b) 测评对象：机房供电设施。

c) 测评实施：应核查供电线路上是否配置了稳压器和过电压防护设备。

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。

7.1.1.9.2 测评单元(L2-PES1-14)

该测评单元包括以下要求：

a) 测评指标：应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

b) 测评对象：机房备用供电设施。

c) 测评实施包括以下内容：

1) 应核查机房是否配备 UPS 等后备电源系统；

2) 应核查 UPS 等后备电源系统是否满足设备在断电情况下的正常运行要求。

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。

7.1.1.10 电磁防护

7.1.1.10.1 测评单元(L2-PES1-15)

该测评单元包括以下要求：

a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰。

b) 测评对象：机房线缆。

c) 测评实施：应核查机房内电源线缆和通信线缆是否隔离铺设。

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。

7.1.2 安全通信网络

7.1.2.1 网络架构

7.1.2.1.1 测评单元(L2-CNS1-01)

该测评单元包括以下要求：

a) 测评指标：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。

b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否依据重要性、部门等因素划分不同的网络区域；

2) 应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。

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。

7.1.2.1.2 测评单元(L2-CNS1-02)

该测评单元包括以下要求：

a) 测评指标：应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

b) 测评对象：网络拓扑。

c) 测评实施包括以下内容：

1) 应核查网络拓扑图是否与实际网络运行环境一致；

2) 应核查重要网络区域是否未部署在网络边界处；

3） 应核查重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表(ACL)等。

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。

7.1.2.2 通信传输

7.1.2.2.1 测评单元(L2-CNS1-03)

该测评单元包括以下要求：

a） 测评指标：应采用校验技术保证通信过程中数据的完整性。

b） 测评对象：提供校验技术功能的设备或组件。

c） 测评实施：应核查是否在数据传输过程中使用校验技术来保护其完整性。

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。

7.1.2.3 可信验证

7.1.2.3.1 测评单元(L2-CNS1-04)

该测评单元包括以下要求：

a） 测评指标：可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并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。

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通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证；

2） 应核查当检测到通信设备的可信性受到破坏后是否进行报警；

3） 应核查验证结果是否以审计记录的形式送至安全管理中心。

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。

7.1.3 安全区域边界

7.1.3.1 边界防护

7.1.3.1.1 测评单元(L2-ABS1-01)

该测评单元包括以下要求：

a） 测评指标：应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

b） 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c） 测评实施包括以下内容：

1） 应核查在网络边界处是否部署访问控制设备；

2） 应核查设备配置信息是否指定端口进行跨越边界的网络通信，指定端口是否配置并启用了安全策略；

3） 应采用其他技术手段(如非法无线网络设备定位、核查设备配置信息等)核查是否不存在

其他未受控端口进行跨越边界的网络通信。

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。

7.1.3.2 访问控制

7.1.3.2.1 测评单元(L2-ABS1-02)

该测评单元包括以下要求：

a) 测评指标：应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查在网络边界或区域之间是否部署访问控制设备并启用访问控制策略；

2) 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。

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。

7.1.3.2.2 测评单元(L2-ABS1-03)

该测评单元包括以下要求：

a) 测评指标：应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否不存在多余或无效的访问控制策略；

2) 应核查不同的访问控制策略之间的逻辑关系及前后排列顺序是否合理。

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。

7.1.3.2.3 测评单元(L2-ABS1-04)

该测评单元包括以下要求：

a) 测评指标：应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c) 测评实施：应核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数。

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。

7.1.3.2.4 测评单元(L2-ABS1-05)

该测评单元包括以下要求：

a) 测评指标：应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。
c) 测评实施：应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力。
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。

7.1.3.3 入侵防范

7.1.3.3.1 测评单元(L2-ABS1-06)

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监视网络攻击行为。
b) 测评对象：抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统、入侵保护系统和入侵检测系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够检测到以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
   2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本；
   3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。
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。

7.1.3.4 恶意代码防范

7.1.3.4.1 测评单元(L2-ABS1-07)

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。
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。

7.1.3.5 安全审计

7.1.3.5.1 测评单元(L2-ABS1-08)

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。

7.1.3.5.2 测评单元（L2-ABS1-09）

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，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。

7.1.3.5.3 测评单元（L2-ABS1-10）

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：综合安全审计系统等。

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。

7.1.3.6 可信验证

7.1.3.6.1 测评单元（L2-ABS1-11）

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。

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） 应核查当检测到边界设备的可信性受到破坏后是否进行报警；

3） 应核查验证结果是否以审计记录的形式送至安全管理中心。

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。

7.1.4 安全计算环境

7.1.4.1 身份鉴别

7.1.4.1.1 测评单元(L2-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。

7.1.4.1.2 测评单元(L2-CES1-02)

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。

7.1.4.1.3 测评单元(L2-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。

7.1.4.2 访问控制

7.1.4.2.1 测评单元(L2-CES1-04)

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。

7.1.4.2.2 测评单元(L2-CES1-05)

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。

7.1.4.2.3 测评单元(L2-CES1-06)

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） 应核查并测试多余的、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。

7.1.4.2.4 测评单元（L2-CES1-07）

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。

7.1.4.3 安全审计

7.1.4.3.1 测评单元（L2-CES1-08）

该测评单元包括以下要求：

a） 测评指标：应提供安全审计功能，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） 应核查是否提供并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。

7.1.4.3.2 测评单元（L2-CES1-09）

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：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、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。

7.1.4.3.3 测评单元（L2-CES1-10）

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。

7.1.4.4 入侵防范

7.1.4.4.1 测评单元（L2-CES1-11）

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。

7.1.4.4.2 测评单元（L2-CES1-12）

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。

7.1.4.4.3 测评单元(L2-CES1-13)

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。

7.1.4.4.4 测评单元(L2-CES1-14)

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: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。

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。

7.1.4.4.5 测评单元(L2-CES1-15)

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、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) 应核查是否不存在高风险漏洞,如漏洞扫描、渗透测试等;

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。

7.1.4.5 恶意代码防范

7.1.4.5.1 测评单元(L2-CES1-16)

该测评单元包括以下要求:

a) 测评指标:应安装防恶意代码软件或配置具有相应功能的软件,并定期进行升级和更新防恶意代码库。

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)和移动终端等。

c) 测评实施内容包括以下:

1) 应核查是否安装了防恶意代码软件或相应功能的软件;

2） 应核查是否定期进行升级和更新防恶意代码库。

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。

7.1.4.6 可信验证

7.1.4.6.1 测评单元（L2-CES1-17）

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。

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） 应核查当检测到计算设备的可信性受到破坏后是否进行报警；

3） 应核查验证结果是否以审计记录的形式送至安全管理中心。

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。

7.1.4.7 数据完整性

7.1.4.7.1 测评单元（L2-CES1-18）

该测评单元包括以下要求：

a） 测评指标：应采用校验技术保证重要数据在传输过程中的完整性。

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：应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验技术或密码技术保证完整性。

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。

7.1.4.8 数据备份恢复

7.1.4.8.1 测评单元（L2-CES1-19）

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。

7.1.4.8.2 测评单元(L2-CES1-20)

该测评单元包括以下要求:

a) 测评指标:应提供异地数据备份功能,利用通信网络将重要数据定时批量传送至备用场地。

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数据备份功能,并通过通信网络将重要配置数据、重要业务数据定时批量传送至备份场地。

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。

7.1.4.9 剩余信息保护

7.1.4.9.1 测评单元(L2-CES1-21)

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,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。

7.1.4.10 个人信息保护

7.1.4.10.1 测评单元(L2-CES1-22)

该测评单元包括以下要求:

a) 测评指标:应仅采集和保存业务必需的用户个人信息。

b) 测评对象:用户数据、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) 应核查采集的用户个人信息是否是业务应用必需的;

2) 应核查是否制定了有关用户个人信息保护的管理制度和流程。

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。

7.1.4.10.2 测评单元(L2-CES1-23)

该测评单元包括以下要求:

a) 测评指标:应禁止未授权访问和非法使用用户个人信息。

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) 应核查是否采用技术措施限制对用户个人信息的访问和使用;

2) 应核查是否制定了有关用户个人信息保护的管理制度和流程。

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。

7.1.5 安全管理中心

7.1.5.1 系统管理

7.1.5.1.1 测评单元(L2-SMC1-01)

该测评单元包括以下要求：

a) 测评指标：应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

b) 测评对象：提供集中系统管理功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否对系统管理员进行身份鉴别；

2) 应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作；

3) 应核查是否对系统管理的操作进行审计。

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。

7.1.5.1.2 测评单元(L2-SMC1-02)

该测评单元包括以下要求：

a) 测评指标：应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

b) 测评对象：提供集中系统管理功能的系统。

c) 测评实施：应核查是否通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

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。

7.1.5.2 审计管理

7.1.5.2.1 测评单元(L2-SMC1-03)

该测评单元包括以下要求：

a) 测评指标：应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。

b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否对审计管理员进行身份鉴别；

2) 应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作；

3) 应核查是否对审计管理员的操作进行审计。

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。

7.1.5.2.2 测评单元(L2-SMC1-04)

该测评单元包括以下要求：

a) 测评指标：应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全

审计策略对审计记录进行存储、管理和查询等。

b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。

c) 测评实施：应核查是否通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

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。

7.1.6 安全管理制度

7.1.6.1 安全策略(L2-PSS1-01)

该测评单元包括以下要求：

a) 测评指标：应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

b) 测评对象：总体方针策略类文档。

c) 测评实施：应核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略。

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。

7.1.6.2 管理制度

7.1.6.2.1 测评单元(L2-PSS1-02)

该测评单元包括以下要求：

a) 测评指标：应对安全管理活动中的主要管理内容建立安全管理制度。

b) 测评对象：安全管理制度类文档。

c) 测评实施：应核查各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容。

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。

7.1.6.2.2 测评单元(L2-PSS1-03)

该测评单元包括以下要求：

a) 测评指标：应对管理人员或操作人员执行的日常管理操作建立操作规程。

b) 测评对象：操作规程类文档。

c) 测评实施：应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等。

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。

7.1.6.3 制定和发布

7.1.6.3.1 测评单元(L2-PSS1-04)

该测评单元包括以下要求：

a) 测评指标：应指定或授权专门的部门或人员负责安全管理制度的制定。

b) 测评对象：部门/人员职责文件等。