8.1.4.11 个人信息保护

8.1.4.11.1 测评单元(L3-CES1-34)

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：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。

8.1.4.11.2 测评单元(L3-CES1-35)

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。

8.1.5 安全管理中心

8.1.5.1 系统管理

8.1.5.1.1 测评单元(L3-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。

8.1.5.1.2 测评单元(L3-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。

8.1.5.2 审计管理

8.1.5.2.1 测评单元(L3-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) 应核查是否对安全审计操作进行审计。

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。

8.1.5.2.2 测评单元(L3-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。

8.1.5.3 安全管理

8.1.5.3.1 测评单元(L3-SMC1-05)

该测评单元包括以下要求：

a) 测评指标：应对安全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管理操作，并对这些操作进行审计。

b) 测评对象：提供集中安全管理功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否对安全管理员进行身份鉴别；

2) 应核查是否只允许安全管理员通过特定的命令或操作界面进行安全审计操作；

3) 应核查是否对安全管理操作进行审计。

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。

8.1.5.3.2 测评单元(L3-SMC1-06)

该测评单元包括以下要求:

a) 测评指标:应通过安全管理员对系统中的安全策略进行配置,包括安全参数的设置,主体、客体进行统一安全标记,对主体进行授权,配置可信验证策略等。

b) 测评对象:提供集中安全管理功能的系统。

c) 测评实施:应核查是否通过安全管理员对系统中的安全策略进行配置,包括安全参数的设置,主体、客体进行统一安全标记,对主体进行授权,配置可信验证策略等。

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。

8.1.5.4 集中管控

8.1.5.4.1 测评单元(L3-SMC1-07)

该测评单元包括以下要求:

a) 测评指标:应划分出特定的管理区域,对分布在网络中的安全设备或安全组件进行管控。

b) 测评对象:网络拓扑。

c) 测评实施包括以下内容:

1) 应核查是否划分出单独的网络区域用于部署安全设备或安全组件;

2) 应核查各个安全设备或安全组件是否集中部署在单独的网络区域内。

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。

8.1.5.4.2 测评单元(L3-SMC1-08)

该测评单元包括以下要求:

a) 测评指标:应能够建立一条安全的信息传输路径,对网络中的安全设备或安全组件进行管理。

b) 测评对象:路由器、交换机和防火墙等设备或相关组件。

c) 测评实施包括以下内容:

1) 应核查是否采用安全方式(如 SSH、HTTPS、IPSec VPN 等)对安全设备或安全组件进行管理;

2) 应核查是否使用独立的带外管理网络对安全设备或安全组件进行管理。

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,否则不符合本测评单元指标要求。

8.1.5.4.3 测评单元(L3-SMC1-09)

该测评单元包括以下要求:

a) 测评指标:应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。

b) 测评对象:综合网管系统等提供运行状态监测功能的系统。

c) 测评实施包括以下内容:

1) 应核查是否部署了具备运行状态监测功能的系统或设备,能够对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测;

2) 应测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阀值(或默认阀值)实时报警。

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。

8.1.5.4.4 测评单元(L3-SMC1-10)

该测评单元包括以下要求：

a) 测评指标：应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。

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) 应核查各个设备是否配置并启用了相关策略，将审计数据发送到独立于设备自身的外部集中安全审计系统中；

2) 应核查是否部署统一的集中安全审计系统，统一收集和存储各设备日志，并根据需要进行集中审计分析；

3) 应核查审计记录的留存时间是否至少为 6 个月。

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。

8.1.5.4.5 测评单元(L3-SMC1-11)

该测评单元包括以下要求：

a) 测评指标：应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

b) 测评对象：提供集中安全管控功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否能够对安全策略(如防火墙访问控制策略、入侵保护系统防护策略、WAF 安全防护策略等)进行集中管理；

2) 应核查是否实现对操作系统防恶意代码系统及网络恶意代码防护设备的集中管理，实现对防恶意代码病毒规则库的升级进行集中管理；

3) 应核查是否实现对各个系统或设备的补丁升级进行集中管理。

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。

8.1.5.4.6 测评单元(L3-SMC1-12)

该测评单元包括以下要求：

a) 测评指标：应能对网络中发生的各类安全事件进行识别、报警和分析。

b) 测评对象：提供集中安全管控功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否部署了相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警；

2) 应核查监测范围是否能够覆盖网络所有关键路径。

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。

8.1.6 安全管理制度

8.1.6.1 安全策略

8.1.6.1.1 测评单元(L3-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。

8.1.6.2 管理制度

8.1.6.2.1 测评单元(L3-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各类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。

8.1.6.2.2 测评单元(L3-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。

8.1.6.2.3 测评单元(L3-PSS1-04)

该测评单元包括以下要求：

a) 测评指标：应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

b) 测评对象：总体方针策略类文档、管理制度类文档、操作规程类文档和记录表单类文档。

c) 测评实施：应核查总体方针策略文件、管理制度和操作规程、记录表单是否全面且具有关联性和一致性。

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。

8.1.6.3 制定和发布

8.1.6.3.1 测评单元(L3-PSS1-05)

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。

c) 测评实施:应核查是否由专门的部门或人员负责制定安全管理制度。

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。

8.1.6.3.2 测评单元(L3-PSS1-06)

该测评单元包括以下要求:

a) 测评指标:安全管理制度应通过正式、有效的方式发布,并进行版本控制。

b) 测评对象:管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容;

2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发,如正式发文、领导签署和单位盖章等。

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。

8.1.6.4 评审和修订

8.1.6.4.1 测评单元(L3-PSS1-07)

该测评单元包括以下要求:

a) 测评指标:应定期对安全管理制度的合理性和适用性进行论证和审定,对存在不足或需要改进的安全管理制度进行修订。

b) 测评对象:信息/网络安全主管和记录表单类文档。

c) 测评实施包括以下内容:

1) 应访谈信息/网络安全主管是否定期对安全管理制度的合理性和适用性进行审定;

2) 应核查是否具有安全管理制度的审定或论证记录,如果对制度做过修订,核查是否有修订版本的安全管理制度。

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。

8.1.7 安全管理机构

8.1.7.1 岗位设置

8.1.7.1.1 测评单元(L3-ORS1-01)

该测评单元包括以下要求:

a) 测评指标:应成立指导和网络安全工作的委员会或领导小组,其最高领导由单位主管领导担任或授权。

b） 测评对象：信息/网络安全主管、管理制度类文档和记录表单类文档。

c） 测评实施包括以下内容：

1） 应访谈信息/网络安全主管是否成立了指导和管理网络安全工作的委员会或领导小组；

2） 应核查相关文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责；

3） 应核查委员会或领导小组的最高领导是否由单位主管领导担任或由其进行了授权。

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。

8.1.7.1.2 测评单元（L3-ORS1-02）

该测评单元包括以下要求：

a） 测评指标：应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。

b） 测评对象：信息/网络安全主管和管理制度类文档。

c） 测评实施包括以下内容：

1） 应访谈信息/网络安全主管是否设立网络安全管理工作的职能部门；

2） 应核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责；

3） 应核查岗位职责文档是否有岗位划分情况和岗位职责。

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。

8.1.7.1.3 测评单元（L3-ORS1-03）

该测评单元包括以下要求：

a） 测评指标：应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

b） 测评对象：信息/网络安全主管和管理制度类文档。

c） 测评实施包括以下内容：

1） 应访谈信息/网络安全主管是否进行了安全管理岗位的划分；

2） 应核查岗位职责文档是否明确了各部门及各岗位职责。

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。

8.1.7.2 人员配备

8.1.7.2.1 测评单元（L3-ORS1-04）

该测评单元包括以下要求：

a） 测评指标：应配备一定数量的系统管理员、审计管理员和安全管理员等。

b） 测评对象：信息/网络安全主管和记录表单类文档。

c） 测评实施包括以下内容：

1） 应访谈信息/网络安全主管是否配备系统管理员、审计管理员和安全管理员；

2） 应核查人员配备文档是否明确各岗位人员配备情况。

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。

8.1.7.2.2 测评单元(L3-ORS1-05)

该测评单元包括以下要求:

a) 测评指标:应配备专职安全管理员,不可兼任。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查人员配备文档是否配备了专职安全管理员。

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。

8.1.7.3 授权和审批

8.1.7.3.1 测评单元(L4-ORS1-06)

该测评单元包括以下要求:

a) 测评指标:应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。

b) 测评对象:管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查部门职责文档是否明确各部门审批事项;

2) 应核查岗位职责文档是否明确各岗位审批事项。

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。

8.1.7.3.2 测评单元(L4-ORS1-07)

该测评单元包括以下要求:

a) 测评指标:应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序,按照审批程序执行审批过程,对重要活动建立逐级审批制度。

b) 测评对象:操作规程类文档和记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查系统变更、重要操作、物理访问和系统接入等事项的操作规范是否明确建立了逐级审批程序;

2) 应核查审批记录、操作记录,审批结果是否与相关制度一致。

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。

8.1.7.3.3 测评单元(L4-ORS1-08)

该测评单元包括以下要求:

a) 测评指标:应定期审查审批事项,及时更新需授权和审批的项目、审批部门和审批人等信息。

b) 测评对象:信息/网络安全主管和记录表单类文档。

c) 测评实施包括以下内容:

1) 应访谈信息/网络安全主管是否对各类审批事项进行更新;

2) 应核查是否具有定期审查审批事项的记录。

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。

8.1.7.4 沟通和合作

8.1.7.4.1 测评单元(L3-ORS1-09)

该测评单元包括以下要求：

a) 测评指标：应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。

b) 测评对象：信息/网络安全主管和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈信息/网络安全主管是否建立了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制；

2) 应核查会议记录是否明确各类管理人员、组织内部机构和网络安全管理部门之间开展了合作与沟通。

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。

8.1.7.4.2 测评单元(L3-ORS1-10)

该测评单元包括以下要求：

a) 测评指标：应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。

b) 测评对象：信息/网络安全主管和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈信息/网络安全主管是否建立了与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制；

2) 应核查会议记录是否与网络安全职能部门、各类供应商、业界专家及安全组织开展了合作与沟通。

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。

8.1.7.4.3 测评单元(L3-ORS1-11)

该测评单元包括以下要求：

a) 测评指标：应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息。

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。

8.1.7.5 审核和检查

8.1.7.5.1 测评单元(L3-ORS1-12)

该测评单元包括以下要求：

a) 测评指标：应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

b) 测评对象:信息/网络安全主管和记录表单类文档。

c) 测评实施包括以下内容:

1) 应访谈信息/网络安全主管是否定期进行了常规安全检查;

2) 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。

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。

8.1.7.5.2 测评单元(L3-ORS1-13)

该测评单元包括以下要求:

a) 测评指标:应定期进行全面安全检查,检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

b) 测评对象:信息/网络安全主管和记录表单类文档。

c) 测评实施包括以下内容:

1) 应访谈信息/网络安全主管是否定期进行了全面安全检查;

2) 应核查全面安全检查记录是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

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。

8.1.7.5.3 测评单元(L3-ORS1-14)

该测评单元包括以下要求:

a) 测评指标:应制定安全检查表格实施安全检查,汇总安全检查数据,形成安全检查报告,并对安全检查结果进行通报。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录。

d) 单元判定:如果以上测评实施内容肯定,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。

8.1.8 安全管理人员

8.1.8.1 人员录用

8.1.8.1.1 测评单元(L3-HRS1-01)

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人员录用。

b) 测评对象:信息/网络安全主管。

c) 测评实施:应访谈信息/网络安全主管是否由专门的部门或人员负责人员的录用工作。

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。

8.1.8.1.2 测评单元(L3-HRS1-02)

该测评单元包括以下要求:

a) 测评指标:应对被录用人员的身份、安全背景、专业资格或资质等进行审查,对其所具有的技术

技能进行考核。

b) 测评对象:管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查人员安全管理文档是否说明录用人员应具备的条件(如学历、学位要求,技术人员应具备的专业技术水平,管理人员应具备的安全管理知识等);

2) 应核查是否具有人员录用时对录用人身份、安全背景、专业资格或资质等进行审查的相关文档或记录,是否记录审查内容和审查结果等;

3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。

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。

8.1.8.1.3 测评单元(L3-HRS1-03)

该测评单元包括以下要求:

a) 测评指标:应与被录用人员签署保密协议,与关键岗位人员签署岗位责任协议。

b) 测评对象:记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容;

2) 应核查岗位安全协议是否有岗位安全责任定义、协议的有效期限和责任人签字等内容。

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。

8.1.8.2 人员离岗

8.1.8.2.1 测评单元(L3-HRS1-04)

该测评单元包括以下要求:

a) 测评指标:应及时终止离岗人员的所有访问权限,取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否具有离岗人员终止其访问权限、交还身份证件、软硬件设备等的登记记录。

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。

8.1.8.2.2 测评单元(L3-HRS1-05)

该测评单元包括以下要求:

a) 测评指标:应办理严格的调离手续,并承诺调离后的保密义务后方可离开。

b) 测评对象:管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查人员离岗的管理文档是否规定了人员调离手续和离岗要求等;

2) 应核查是否具有按照离岗程序办理调离手续的记录;

3) 应核查保密承诺文档是否有调离人员的签字。

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。

8.1.8.3 安全意识教育和培训

8.1.8.3.1 测评单元(L3-HRS1-06)

该测评单元包括以下要求:

a) 测评指标:应对各类人员进行安全意识教育和岗位技能培训,并告知相关的安全责任和惩戒措施。

b) 测评对象:管理制度类文档。

c) 测评实施包括以下内容:

1) 应核查安全意识教育及岗位技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容;

2) 应核查安全责任和惩戒措施管理文档或培训文档是否包含具体的安全责任和惩戒措施。

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。

8.1.8.3.2 测评单元(L3-HRS1-07)

该测评单元包括以下要求:

a) 测评指标:应针对不同岗位制定不同的培训计划,对安全基础知识、岗位操作规程等进行培训。

b) 测评对象:记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查安全教育和培训计划文档是否具有不同岗位的培训计划;

2) 应核查培训内容是否包含安全基础知识、岗位操作规程等;

3) 应核查安全教育和培训记录是否有培训人员、培训内容、培训结果等描述。

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。

8.1.8.3.3 测评单元(L3-HRS1-08)

该测评单元包括以下要求:

a) 测评指标:应定期对不同岗位的人员进行技能考核。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否具有针对各岗位人员的技能考核记录。

d) 单元判定:如果以上测评实施为肯定,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。

8.1.8.4 外部人员访问管理

8.1.8.4.1 测评单元(L3-HRS1-09)

该测评单元包括以下要求:

a) 测评指标:应在外部人员物理访问受控区域前先提出书面申请,批准后由专人全程陪同,并登记备案。

b) 测评对象:管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容:

1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、

外部人员进入的访问控制措施等；

2） 应核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等；

3） 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等；

4） 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等；

5） 应核查外部人员访问重要区域的书面申请文档，是否具有批准人允许访问的批准签字等；

6） 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。

d） 单元判定：如果1）～6）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。

8.1.8.4.2 测评单元（L3-HRS1-10）

该测评单元包括以下要求：

a） 测评指标：应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。

b） 测评对象：管理制度类文档和记录表单类文档。

c） 测评实施包括以下内容：

1） 应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程；

2） 应核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问的批准签字等；

3） 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。

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。

8.1.8.4.3 测评单元（L3-HRS1-11）

该测评单元包括以下要求：

a） 测评指标：外部人员离场后应及时清除其所有的访问权限。

b） 测评对象：管理制度类文档和记录表单类文档。

c） 测评实施包括以下内容：

1） 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限；

2） 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。

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。

8.1.8.4.4 测评单元（L3-HRS1-12）

该测评单元包括以下要求：

a） 测评指标：获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

b） 测评对象：记录表单类文档。

c） 测评实施：应核查外部人员访问保密协议是否明确人员的保密义务（如不得进行非授权操作，不得复制信息等）。

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。

8.1.9 安全建设管理

8.1.9.1 定级和备案

8.1.9.1.1 测评单元(L3-CMS1-01)

该测评单元包括以下要求：

a) 测评指标：应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由。

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。

8.1.9.1.2 测评单元(L3-CMS1-02)

该测评单元包括以下要求：

a) 测评指标：应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见。

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。

8.1.9.1.3 测评单元(L3-CMS1-03)

该测评单元包括以下要求：

a) 测评指标：应保证定级结果经过相关部门的批准。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见。

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。

8.1.9.1.4 测评单元(L3-CMS1-04)

该测评单元包括以下要求：

a) 测评指标：应将备案材料报主管部门和公安机关备案。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查是否具有公安机关出具的备案证明文档。

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。

8.1.9.2 安全方案设计

8.1.9.2.1 测评单元(L3-CMS1-05)

该测评单元包括以下要求：

a) 测评指标：应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。
b) 测评对象：安全规划设计类文档。
c) 测评实施：应核查安全设计文档是否根据安全保护等级选择安全措施，是否根据安全需求调整安全措施。
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。

8.1.9.2.2 测评单元(L3-CMS1-06)

该测评单元包括以下要求：

a) 测评指标：应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。
b) 测评对象：安全规划设计类文档。
c) 测评实施：应核查是否有总体规划和安全设计方案等配套文件，设计方案中应包含密码技术相关内容。
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。

8.1.9.2.3 测评单元(L3-CMS1-07)

该测评单元包括以下要求：

a) 测评指标：应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体安全规划、安全设计方案等相关配套文件的批准意见和论证意见。
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。

8.1.9.3 产品采购和使用

8.1.9.3.1 测评单元(L3-CMS1-08)

该测评单元包括以下要求：

a) 测评指标：应确保网络安全产品采购和使用符合国家的有关规定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查有关网络安全产品是否符合国家的有关规定，如网络安全产品获得了销售许可等。
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。

8.1.9.3.2 测评单元(L3-CMS1-09)

该测评单元包括以下要求：

a) 测评指标：应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。
b) 测评对象：建设负责人和记录表单类文档。