6.1.8.3 产品采购和使用

6.1.8.3.1 测评单元(L1-CMS1-03)

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。

6.1.8.4 工程实施

6.1.8.4.1 测评单元(L1-CMS1-04)

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工程实施过程的管理。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否指定专门部门或人员对工程实施进行进度和质量控制。

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。

6.1.8.5 测试验收

6.1.8.5.1 测评单元(L1-CMS1-05)

该测评单元包括以下要求:

a) 测评指标:应进行安全性测试验收。

b) 测评对象:建设负责人。

c) 测评实施:应访谈建设负责人是否进行了安全性测试验收。

d) 单元判定:如果以上测评内容为肯定,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。

6.1.8.6 系统交付

6.1.8.6.1 测评单元(L1-CMS1-06)

该测评单元包括以下要求:

a) 测评指标:应制定交付清单,并根据交付清单对所交接的设备、软件和文档等进行清点。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否制定交付清单并说明交付的各类设备、软件、文档等。

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。

6.1.8.6.2 测评单元(L1-CMS1-07)

该测评单元包括以下要求:

a) 测评指标:应对负责运行维护的技术人员进行相应的技能培训。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查交付技术培训记录是否包括培训内容、培训时间和参与人员等。

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。

6.1.8.7 服务供应商管理

6.1.8.7.1 测评单元(L1-CMS1-08)

该测评单元包括以下要求:

a) 测评指标:应确保服务供应商的选择符合国家的有关规定。

b) 测评对象:建设负责人。

c) 测评实施:应访谈建设负责人选择的安全服务商是否符合国家有关规定。

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。

6.1.8.7.2 测评单元(L1-CMS1-09)

该测评单元包括以下要求:

a) 测评指标:应与选定的服务供应商签订与安全相关的协议,明确约定相关责任。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否具有与服务供应商签订的服务合同或安全责任书,是否明确了相关责任。

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。

6.1.9 安全运维管理

6.1.9.1 环境管理

6.1.9.1.1 测评单元(L1-MMS1-01)

该测评单元包括以下要求:

a) 测评指标:应指定专门的部门或人员负责机房安全,对机房出入进行管理,定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。

b) 测评对象:物理安全负责人和记录表单类文档。

c) 测评实施包括以下内容:

1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作,对机房的出入进行管理、对基础设施(如空调、供配电设备、灭火设备等)进行定期维护;

2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员。

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。

6.1.9.1.2 测评单元(L1-MMS1-02)

该测评单元包括以下要求:

a) 测评指标:应对机房的安全管理做出规定,包括物理访问、物品进出和环境安全等方面。

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) 应核查机房安全管理制度是否覆盖物理访问、物品进出和环境安全等方面内容；

2) 应核查物理访问、物品进出和环境安全等的相关记录是否与制度相符。

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。

6.1.9.2 介质管理

6.1.9.2.1 测评单元(L1-MMS1-03)

该测评单元包括以下要求：

a) 测评指标：应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点。

b) 测评对象：资产管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理；

2) 应核查介质管理记录是否记录介质归档、使用和定期盘点等情况。

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。

6.1.9.3 设备维护管理

6.1.9.3.1 测评单元(L1-MMS1-04)

该测评单元包括以下要求：

a) 测评指标：应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理。

b) 测评对象：设备管理员和管理制度类文档。

c) 测评实施包括以下内容：

1) 应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护；

2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。

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。

6.1.9.4 漏洞和风险管理

6.1.9.4.1 测评单元(L1-MMS1-05)

该测评单元包括以下要求：

a) 测评指标：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查是否有识别安全漏洞和隐患的安全报告或记录(如漏洞扫描报告、渗透测试报告和安全通报等)；

2) 应核查相关记录是否对发现的漏洞及时进行修补或评估可能的影响后进行修补。

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。

6.1.9.5 网络和系统安全管理

6.1.9.5.1 测评单元(L1-MMS1-06)

该测评单元包括以下要求:

a) 测评指标:应划分不同的管理员角色进行网络和系统的运维管理,明确各个角色的责任和权限。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查网络和系统安全管理文档,是否划分了网络和系统管理员等不同角色,并定义各个角色的责任和权限。

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。

6.1.9.5.2 测评单元(L1-MMS1-07)

该测评单元包括以下要求:

a) 测评指标:应指定专门的部门或人员进行账户管理,对申请账户、建立账户、删除账户等进行控制。

b) 测评对象:运维负责人和记录表单类文档。

c) 测评实施包括以下内容:

1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理;

2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。

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。

6.1.9.6 恶意代码防范管理

6.1.9.6.1 测评单元(L1-MMS1-08)

该测评单元包括以下要求:

a) 测评指标:应提高所有用户的防恶意代码意识,对外来计算机或存储设备接入系统前进行恶意代码检查等。

b) 测评对象:运维负责人和管理制度类文档。

c) 测评实施包括以下内容:

1) 应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识;

2) 应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系统前进行恶意代码检查。

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。

6.1.9.6.2 测评单元(L1-MMS1-09)

该测评单元包括以下要求:

a) 测评指标:应对恶意代码防范要求做出规定,包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

b) 测评对象:管理制度类文档。

c) 测评实施：应核查恶意代码防范管理制度是否包括防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容。

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。

6.1.9.7 备份与恢复管理

6.1.9.7.1 测评单元(L1-MMS1-10)

该测评单元包括以下要求：

a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等。

b) 测评对象：系统管理员和管理制度类文档。

c) 测评实施包括以下内容：

1) 应访谈系统管理员有哪些需定期备份的业务信息、系统数据及软件系统；

2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。

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。

6.1.9.7.2 测评单元(L1-MMS1-11)

该测评单元包括以下要求：

a) 测评指标：应规定备份信息的备份方式、备份频度、存储介质、保存期等。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容。

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。

6.1.9.8 安全事件处置

6.1.9.8.1 测评单元(L1-MMS1-12)

该测评单元包括以下要求：

a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件。

b) 测评对象：运维负责人和管理制度类文档。

c) 测评实施包括以下内容：

1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告；

2) 应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。

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。

6.1.9.8.2 测评单元(L1-MMS1-13)

该测评单元包括以下要求：

a) 测评指标：应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查安全事件报告和处置流程是否明确了与安全事件有关的工作职责，包括报告

单位(人)、接报单位(人)和处置单位等职责。

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。

6.2 云计算安全测评扩展要求

6.2.1 安全物理环境

6.2.1.1 基础设施位置

6.2.1.1.1 测评单元(L1-PES2-01)

该测评单元包括以下要求:

a) 测评指标:应保证云计算基础设施位于中国境内。

b) 测评对象:机房管理员、办公场地、机房和平台建设方案。

c) 测评实施包括以下内容:

1) 应访谈机房管理员云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内;

2) 应核查云计算平台建设方案,云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内。

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

6.2.2 安全通信网络

6.2.2.1 网络架构

6.2.2.1.1 测评单元(L1-CNS2-01)

该测评单元包括以下要求:

a) 测评指标:应保证云计算平台不承载高于其安全保护等级的业务应用系统。

b) 测评对象:云计算平台和业务应用系统定级备案材料。

c) 测评实施:应核查云计算平台和云计算平台承载的业务应用系统相关定级备案材料,云计算平台安全保护等级是否不低于其承载的业务应用系统安全保护等级。

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

6.2.2.1.2 测评单元(L1-CNS2-02)

该测评单元包括以下要求:

a) 测评指标:应实现不同云服务客户虚拟网络之间的隔离。

b) 测评对象:网络资源隔离措施、综合网管系统和云管理平台。

c) 测评实施包括以下内容:

1) 应核查云服务客户之间是否采取网络隔离措施;

2) 应核查云服务客户之间是否设置并启用网络资源隔离策略。

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

6.2.3 安全区域边界

6.2.3.1 访问控制

6.2.3.1.1 测评单元(L1-ABS2-01)

该测评单元包括以下要求：

a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。

b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备。

c) 测评实施包括以下内容：

1) 应核查是否在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

2) 应核查是否设置了云计算平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略等；

3) 应核查是否设置了云计算平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等；

4) 应核查是否设置了不同云服务客户间访问控制规则和访问控制策略等；

5) 应核查是否设置了云服务客户不同安全保护等级业务系统之间访问控制规则和访问控制策略等。

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

6.2.4 安全计算环境

6.2.4.1 访问控制

6.2.4.1.1 测评单元(L1-CES2-01)

该测评单元包括以下要求：

a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移。

b) 测评对象：虚拟机、虚拟机迁移记录和相关配置。

c) 测评实施包括以下内容：

1) 应核查虚拟机迁移时访问控制策略是否随之迁移；

2) 应核查是否具备虚拟机迁移记录及相关配置。

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

6.2.4.1.2 测评单元(L1-CES2-02)

该测评单元包括以下要求：

a) 测评指标：应允许云服务客户设置不同虚拟机之间的访问控制策略。

b) 测评对象：虚拟机和安全组或相关组件。

c) 测评实施：应核查云服务客户是否能够设置不同虚拟机之间访问控制策略。

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

6.2.4.2 数据完整性和保密性

6.2.4.2.1 测评单元(L1-CES2-03)

该测评单元包括以下要求：

a) 测评指标：应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

b) 测评对象：数据库服务器、数据存储设备和管理文档记录。

c) 测评实施包括以下内容：

1) 应核查云服务客户数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内；

2) 应核查上述数据出境时是否符合国家相关规定。

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

6.2.5 安全建设管理

6.2.5.1 云服务商选择

6.2.5.1.1 测评单元(L1-CMS2-01)

该测评单元包括以下要求：

a) 测评指标：应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。

b) 测评对象：系统建设负责人和服务合同。

c) 测评实施包括以下内容：

1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云计算平台及云服务商；

2) 应核查云服务商提供的相关服务合同是否明确其云计算平台具有与所承载的业务应用系统具有相应或高于的安全保护能力。

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

6.2.5.1.2 测评单元(L1-CMS2-02)

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标。

b) 测评对象：服务水平协议或服务合同。

c) 测评实施：应核查服务水平协议或服务合同是否规定了云服务的各项服务内容和具体指标等。

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

6.2.5.1.3 测评单元(L1-CMS2-03)

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

b) 测评对象：服务水平协议或服务合同。

c) 测评实施：应核查服务水平协议或服务合同中是否规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

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

6.2.5.2 供应链管理

6.2.5.2.1 测评单元(L1-CMS2-04)

该测评单元包括以下要求：

a) 测评指标：应确保供应商的选择符合国家有关规定。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查云服务商的选择是否符合国家的有关规定。

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

6.3 移动互联安全测评扩展要求

6.3.1 安全物理环境

6.3.1.1 无线接入点的物理位置

6.3.1.1.1 测评单元(L1-PES3-01)

该测评单元包括以下要求：

a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

b) 测评对象：无线接入设备。

c) 测评实施包括以下内容：

1) 应核查物理位置与无线信号的覆盖范围是否合理；

2) 应测试验证无线信号是否可以避免电磁干扰。

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。

6.3.2 安全区域边界

6.3.2.1 边界防护

6.3.2.1.1 测评单元(L1-ABS3-01)

该测评单元包括以下要求：

a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

b) 测评对象：无线接入网关设备。

c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。

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。

6.3.2.2 访问控制

6.3.2.2.1 测评单元(L1-ABS3-02)

该测评单元包括以下要求：

a) 测评指标：无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否开启接入认证功能，是否使用除 WEP 方式以外的其他方式进行认证，密钥长度不小于 8 位。
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。

6.3.3 安全计算环境

6.3.3.1 移动应用管控

6.3.3.1.1 测评单元（L1-CES3-01）

该测评单元包括以下要求：

a) 测评指标：应具有选择应用软件安装、运行的功能。
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查是否具有选择应用软件安装、运行的功能。
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。

6.3.4 安全建设管理

6.3.4.1 移动应用软件采购

6.3.4.1.1 测评单元（L1-CMS3-01）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
b) 测评对象：移动终端。
c) 测评实施：应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。
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。

6.4 物联网安全测评扩展要求

6.4.1 安全物理环境

6.4.1.1 感知节点设备物理防护

6.4.1.1.1 测评单元（L1-PES4-01）

该测评单元包括以下要求：

a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动。
b) 测评对象：感知节点设备所处物理环境和设计或验收文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致；
   2) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。

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。

6.4.1.1.2 测评单元(L1-PES4-02)

该测评单元包括以下要求：

a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域)。

b) 测评对象：感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容：

1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致；

2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域)。

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。

6.4.2 安全区域边界

6.4.2.1 接入控制

6.4.2.1.1 测评单元(L1-ABS4-01)

该测评单元包括以下要求：

a) 测评指标：应保证只有授权的感知节点可以接入。

b) 测评对象：感知节点设备和设计文档。

c) 测评实施：应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。

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。

6.4.3 安全运维管理

6.4.3.1 感知节点管理

6.4.3.1.1 测评单元(L1-MMS4-01)

该测评单元包括以下要求：

a) 测评指标：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。

b) 测评对象：维护记录。

c) 测评实施包括以下内容：

1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长；

2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。

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。

6.5 工业控制系统安全测评扩展要求

6.5.1 安全物理环境

6.5.1.1 室外控制设备物理防护

6.5.1.1.1 测评单元(L1-PES5-01)

该测评单元包括以下要求：

a) 测评指标：室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等。

b) 测评对象：室外控制设备。

c) 测评实施包括以下内容：

1) 应核查是否放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；

2) 应核查箱体或装置是否具有透风、散热、防盗、防雨和防火能力等。

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。

6.5.1.1.2 测评单元(L1-PES5-02)

该测评单元包括以下要求：

a) 测评指标：室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

b) 测评对象：室外控制设备。

c) 测评实施包括以下内容：

1) 应核查放置位置是否远离强电磁干扰和热源等环境；

2) 应核查是否有应急处置及检修维护记录。

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。

6.5.2 安全通信网络

6.5.2.1 网络架构

6.5.2.1.1 测评单元(L1-CNS5-01)

该测评单元包括以下要求：

a) 测评指标：工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用技术隔离手段。

b) 测评对象：网闸、路由器、交换机和防火墙等提供访问控制功能的设备。

c) 测评实施包括以下内容：

1) 应核查工业控制系统和企业其他系统之间是否部署单向隔离设备；

2) 应核查是否采用了有效的单向隔离策略实施访问控制；

3) 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。

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。

6.5.2.1.2 测评单元(L1-CNS5-02)

该测评单元包括以下要求：

a) 测评指标：工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。

b) 测评对象：路由器、交换机和防火墙等提供访问控制功能的设备。

c) 测评实施包括以下内容：

1) 应核查工业控制系统内部是否根据业务特点划分了不同的安全域；

2) 应核查各安全域之间访问控制设备是否配置了有效的访问控制策略。

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。

6.5.3 安全区域边界

6.5.3.1 访问控制

6.5.3.1.1 测评单元(L1-ABS5-01)

该测评单元包括以下要求：

a) 测评指标：应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备。

c) 测评实施包括以下内容：

1) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；

2) 应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。

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。

6.5.3.2 无线使用控制

6.5.3.2.1 测评单元(L1-ABS5-02)

该测评单元包括以下要求：

a) 测评指标：应对所有参与无线通信的用户(人员、软件进程或者设备)提供唯一性标识和鉴别。

b) 测评对象：无线通信网络及设备。

c) 测评实施包括以下内容：

1) 应核查无线通信的用户在登录时是否采用了身份鉴别措施；

2) 应核查用户身份标识是否具有唯一性。

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。

6.5.3.2.2 测评单元(L1-ABS5-03)

该测评单元包括以下要求：

a) 测评指标：应对无线连接的授权、监视以及执行使用进行限制。

b) 测评对象:无线通信网络及设备。

c) 测评实施:应核查无线配置文件是否对连接的授权、监视及执行进行限制。

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。

6.5.4 安全计算环境

6.5.4.1 控制设备安全

6.5.4.1.1 测评单元(L1-CES5-01)

该测评单元包括以下要求:

a) 测评指标:控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求,如受条件限制控制设备无法实现上述要求,应由其上位控制或管理设备实现同等功能或通过管理手段控制。

b) 测评对象:控制设备。

c) 测评实施包括以下内容:

1) 应核查控制设备是否具有身份鉴别、访问控制和安全审计等功能,如控制设备具备上述功能,则按照通用要求测评;

2) 如控制设备不具备上述功能,则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。

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。

6.5.4.1.2 测评单元(L1-CES5-02)

该测评单元包括以下要求:

a) 测评指标:应在经过充分测试评估后,在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作。

b) 测评对象:控制设备。

c) 测评实施包括以下内容:

1) 应核查是否有测试报告或测试评估记录;

2) 应核查控制设备版本、补丁及固件是否经过测试后进行了更新。

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 第二级测评要求

7.1 安全测评通用要求

7.1.1 安全物理环境

7.1.1.1 物理位置选择

7.1.1.1.1 测评单元(L2-PES1-01)

该测评单元包括以下要求:

a) 测评指标:机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b) 测评对象：记录类文档和机房。

c) 测评实施包括以下内容：

1) 应核查所在建筑物是否具有建筑物抗震设防审批文档；

2) 应核查机房是否不存在雨水渗漏；

3) 应核查机房门窗是否不存在因风导致的尘土严重；

4) 应核查屋顶、墙体、门窗和地面等是否没有破损开裂。

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。

7.1.1.1.2 测评单元(L2-PES1-02)

该测评单元包括以下要求：

a) 测评指标：机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

b) 测评对象：机房。

c) 测评实施：应核查机房是否不位于所在建筑物的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施。

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。

7.1.1.2 物理访问控制

7.1.1.2.1 测评单元(L2-PES1-03)

该测评单元包括以下要求：

a) 测评指标：机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

b) 测评对象：机房电子门禁系统和值守记录。

c) 测评实施包括以下内容：

1) 应核查是否安排专人值守或配置电子门禁系统；

2) 应核查相关记录是否能够控制、鉴别和记录进入的人员。

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。

7.1.1.3 防盗窃和防破坏

7.1.1.3.1 测评单元(L2-PES1-04)

该测评单元包括以下要求：

a) 测评指标：应将设备或主要部件进行固定，并设置明显的不易除去的标识。

b) 测评对象：机房设备或主要部件。

c) 测评实施包括以下内容：

1) 应核查机房内设备或主要部件是否固定；

2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标识。

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。

7.1.1.3.2 测评单元(L2-PES1-05)

该测评单元包括以下要求：

a) 测评指标：应将通信线缆铺设在隐蔽安全处。
b) 测评对象：机房通信线缆。
c) 测评实施：应核查机房内通信线缆是否铺设在隐蔽安全处，如桥架中等。
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。

7.1.1.4 防雷击

7.1.1.4.1 测评单元(L2-PES1-06)

该测评单元包括以下要求：
a) 测评指标：应将各类机柜、设施和设备等通过接地系统安全接地。
b) 测评对象：机房。
c) 测评实施：应核查机房内机柜、设施和设备等是否进行接地处理。
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。

7.1.1.5 防火

7.1.1.5.1 测评单元(L2-PES1-07)

该测评单元包括以下要求：
a) 测评指标：机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。
b) 测评对象：机房防火设施。
c) 测评实施包括以下内容：
   1) 应核查机房内是否设置火灾自动消防系统；
   2) 应核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火。
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。

7.1.1.5.2 测评单元(L2-PES1-08)

该测评单元包括以下要求：
a) 测评指标：机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
b) 测评对象：机房验收类文档。
c) 测评实施：应核查机房验收文档是否明确相关建筑材料的耐火等级。
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。

7.1.1.6 防水和防潮

7.1.1.6.1 测评单元(L2-PES1-09)

该测评单元包括以下要求：
a) 测评指标：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
b) 测评对象：机房。
c) 测评实施：应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施。
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