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。

7.1.6.3.2 测评单元（L2-PSS1-05）

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。

7.1.6.4 评审和修订

7.1.6.4.1 测评单元（L2-PSS1-06）

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体系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。

7.1.7 安全管理机构

7.1.7.1 岗位设置

7.1.7.1.1 测评单元（L2-ORS1-01）

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。

7.1.7.1.2 测评单元(L2-ORS1-02)

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。

7.1.7.2 人员配备

7.1.7.2.1 测评单元(L2-ORS1-03)

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了系统管理员、审计管理员和安全管理员；

2) 应核查人员配备文档是否有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。

7.1.7.3 授权和审批

7.1.7.3.1 测评单元(L2-ORS1-04)

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。

7.1.7.3.2 测评单元(L2-ORS1-05)

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执行审批过程。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查各类审批记录是否针对系统变更、重要操作、物理访问和系统接入等事项进行审批。

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，否则不符合本测评单元指标要求。

7.1.7.4 沟通和合作

7.1.7.4.1 测评单元（L2-ORS1-06）

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。

7.1.7.4.2 测评单元（L2-ORS1-07）

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明确了与网络安全职能部门、各类供应商、业界专家及安全组织是否开展了合作与沟通。

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。

7.1.7.4.3 测评单元（L2-ORS1-08）

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，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。

7.1.7.5 审核和检查

7.1.7.5.1 测评单元（L2-ORS1-09）

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) 应核查常规安全核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。

7.1.8 安全管理人员

7.1.8.1 人员录用

7.1.8.1.1 测评单元(L2-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。

7.1.8.1.2 测评单元(L2-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。
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。

7.1.8.2 人员离岗

7.1.8.2.1 测评单元(L2-HRS1-03)

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。

7.1.8.3 安全意识教育和培训

7.1.8.3.1 测评单元(L2-HRS1-04)

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。

7.1.8.4 外部人员访问管理

7.1.8.4.1 测评单元(L2-HRS1-05)

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。

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。

7.1.8.4.2 测评单元(L2-HRS1-06)

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。

7.1.8.4.3 测评单元(L2-HRS1-07)

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。

7.1.9 安全建设管理

7.1.9.1 定级和备案

7.1.9.1.1 测评单元(L2-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。

7.1.9.1.2 测评单元(L2-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。

7.1.9.1.3 测评单元(L2-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。

7.1.9.1.4 测评单元(L2-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。

7.1.9.2 安全方案设计

7.1.9.2.1 测评单元(L2-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。

7.1.9.2.2 测评单元(L2-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进行安全方案设计。

b) 测评对象:安全规划设计类文档。

c) 测评实施:应核查安全设计方案是否是根据安全保护等级进行设计规划。

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。

7.1.9.2.3 测评单元(L2-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方案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:应核查安全方案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。

7.1.9.3 产品采购和使用

7.1.9.3.1 测评单元(L2-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。

7.1.9.3.2 测评单元(L2-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。

c) 测评实施包括以下内容:

1) 应访谈建设负责人是否采用了密码产品及其相关服务;

2) 应核查密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。

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。

7.1.9.4 自行软件开发

7.1.9.4.1 测评单元(L2-CMS1-10)

该测评单元包括以下要求:

a) 测评指标:应将开发环境与实际运行环境物理分开,测试数据和测试结果受到控制。

b) 测评对象:建设负责人。

c) 测评实施包括以下内容:

1) 应访谈建设负责人自主开发软件是否在独立的物理环境中完成编码和调试,与实际运行环境分开;

2) 应核查测试数据和结果是否受控使用。

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。

7.1.9.4.2 测评单元(L2-CMS1-11)

该测评单元包括以下要求:

a) 测评指标:应在软件开发过程中对安全性进行测试,在软件安装前对可能存在的恶意代码进行检测。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否具有软件安全测试报告和代码审计报告,明确软件存在的安全问题及可能存在的恶意代码。

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。

7.1.9.5 外包软件开发

7.1.9.5.1 测评单元(L2-CMS1-12)

该测评单元包括以下要求:

a) 测评指标:应在软件交付前检测其中可能存在的恶意代码。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查是否具有交付前的恶意代码检测报告。

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。

7.1.9.5.2 测评单元(L2-CMS1-13)

该测评单元包括以下要求：

a) 测评指标：应保证开发单位提供软件设计文档和使用指南。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。

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。

7.1.9.6 工程实施

7.1.9.6.1 测评单元(L2-CMS1-14)

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。

7.1.9.6.2 测评单元(L2-CMS1-15)

该测评单元包括以下要求：

a) 测评指标：应制定安全工程实施方案控制工程实施过程。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查安全工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。

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。

7.1.9.7 测试验收

7.1.9.7.1 测评单元(L2-CMS1-16)

该测评单元包括以下要求：

a) 测评指标：应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告。

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；

2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。

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。

7.1.9.7.2 测评单元(L2-CMS1-17)

该测评单元包括以下要求：

a) 测评指标：应进行上线前的安全性测试，并出具安全测试报告。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有上线前的安全测试报告。
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。

7.1.9.8 系统交付

7.1.9.8.1 测评单元（L2-CMS1-18）

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：应核查交付清单是否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。

7.1.9.8.2 测评单元（L2-CMS1-19）

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。

7.1.9.8.3 测评单元（L2-CMS1-20）

该测评单元包括以下要求：

a) 测评指标：应提供建设过程文档和运行维护文档。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查交付文档是否包括建设过程文档和运行维护文档等，提交的文档是否符合管理规定的要求。
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。

7.1.9.9 等级测评

7.1.9.9.1 测评单元（L2-CMS1-21）

该测评单元包括以下要求：

a) 测评指标：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。
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) 应访谈运维负责人本次测评是否为首次，若非首次，是否根据以往测评结果进行相应的安全整改；
   2) 应核查是否具有以往等级测评报告和安全整改方案。

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。

7.1.9.9.2 测评单元(L2-CMS1-22)

该测评单元包括以下要求：

a) 测评指标：应在发生重大变更或级别发生变化时进行等级测评。

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) 应核查是否有过重大变更或级别发生过变化及是否进行相应的等级测评；

2) 应核查是否具有相应情况下的等级测评报告。

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。

7.1.9.9.3 测评单元(L2-CMS1-23)

该测评单元包括以下要求：

a) 测评指标：应确保测评机构的选择符合国家有关规定。

b) 测评对象：等级测评报告和相关资质文件。

c) 测评实施：应核查以往等级测评的测评单位是否具有等级测评机构资质。

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。

7.1.9.10 服务供应商管理

7.1.9.10.1 测评单元(L2-CMS1-24)

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。

7.1.9.10.2 测评单元(L2-CMS1-25)

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相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查与服务服务商签订的服务合同或安全责任合同书是否明确了后期的技术支持和服务承诺等内容。

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。

7.1.10 安全运维管理

7.1.10.1 环境管理

7.1.10.1.1 测评单元(L2-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；

3) 应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息；

4) 应核查机房的基础设施的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)～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。

7.1.10.1.2 测评单元(L2-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。

7.1.10.1.3 测评单元(L2-MMS1-03)

该测评单元包括以下要求：

a) 测评指标：应不在重要区域接待来访人员，不随意放置包含敏感信息的纸档文件和移动介质等。

b) 测评对象：安全管理员和办公环境。

c) 测评实施包括以下内容：

1) 应访谈安全管理员是否有相关规定明确接待来访人员区域；

2) 应核查办公桌面上等位置是否未随意放置了含有敏感信息的纸档文件和移动介质等。

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。

7.1.10.2 资产管理

7.1.10.2.1 测评单元(L2-MMS1-04)

该测评单元包括以下要求：

a) 测评指标：应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容。
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。

7.1.10.3 介质管理

7.1.10.3.1 测评单元（L2-MMS1-05）

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和使用等情况。
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。

7.1.10.3.2 测评单元（L2-MMS1-06）

该测评单元包括以下要求：

a) 测评指标：应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
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在物理传输过程中的人员选择、打包、交付等情况是否进行控制；
   2) 应核查是否对介质的归档和查询等进行登记记录。
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。

7.1.10.4 设备维护管理

7.1.10.4.1 测评单元（L2-MMS1-07）

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。

7.1.10.4.2 测评单元(L2-MMS1-08)

该测评单元包括以下要求：

a) 测评指标：应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。

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) 应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容；

2) 应核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。

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。

7.1.10.5 漏洞和风险管理

7.1.10.5.1 测评单元(L2-MMS1-09)

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。

7.1.10.6 网络和系统安全管理

7.1.10.6.1 测评单元(L2-MMS1-10)

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。

7.1.10.6.2 测评单元(L2-MMS1-11)

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。

7.1.10.6.3 测评单元(L2-MMS1-12)

该测评单元包括以下要求：

a) 测评指标：应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略、账户管理(用户责任、义务、风险、权限审批、权限分配、账户注销等)、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与打补丁、审计日志管理、登录设备和系统的口令更新周期等方面。

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。

7.1.10.6.4 测评单元(L2-MMS1-13)

该测评单元包括以下要求：

a) 测评指标：应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。

b) 测评对象：操作规程类文档。

c) 测评实施：应核查重要设备或系统(如操作系统、数据库、网络设备、安全设备、应用和组件)的配置和操作手册是否明确操作步骤、参数配置等内容。

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。

7.1.10.6.5 测评单元(L2-MMS1-14)

该测评单元包括以下要求：

a) 测评指标：应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。

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。

7.1.10.7 恶意代码防范管理

7.1.10.7.1 测评单元(L2-MMS1-15)

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) 测评实施包括如下内容：

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。

7.1.10.7.2 测评单元(L2-MMS1-16)

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。

7.1.10.7.3 测评单元(L2-MMS1-17)

该测评单元包括以下要求：

a) 测评指标：应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。

b) 测评对象：安全管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否出现过大规模的病毒事件，如何处理；

2) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。

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。

7.1.10.8 配置管理

7.1.10.8.1 测评单元(L2-MMS1-18)

该测评单元包括以下要求：

a) 测评指标：应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

b) 测评对象：系统管理员。

c) 测评实施：应访谈系统管理员是否对系统的基本配置信息进行记录和保存。

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。

7.1.10.9 密码管理

7.1.10.9.1 测评单元(L2-MMS1-19)

该测评单元包括以下要求：