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,设计方案中应包括密码技术相关内容。
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。

9.1.9.2.3 测评单元(L4-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。

9.1.9.3 产品采购和使用

9.1.9.3.1 测评单元(L4-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。

9.1.9.3.2 测评单元(L4-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。

9.1.9.3.3 测评单元(L4-CMS1-10)

该测评单元包括以下要求:

a) 测评指标:应预先对产品进行选型测试,确定产品的候选范围,并定期审定和更新候选产品名单。
b) 测评对象:记录表单类文档。
c) 测评实施:应核查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录。

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。

9.1.9.3.4 测评单元（L4-CMS1-11）

该测评单元包括以下要求：

a) 测评指标：应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查是否具有重要产品专项测试记录。

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。

9.1.9.4 自行软件开发

9.1.9.4.1 测评单元（L4-CMS1-12）

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。

9.1.9.4.2 测评单元（L4-CMS1-13）

该测评单元包括以下要求：

a) 测评指标：应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查软件开发管理制度是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批。

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。

9.1.9.4.3 测评单元（L4-CMS1-14）

该测评单元包括以下要求：

a) 测评指标：应制定代码编写安全规范，要求开发人员参照规范编写代码。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查代码编写安全规范是否明确代码安全编写规则。

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。

9.1.9.4.4 测评单元（L4-CMS1-15）

该测评单元包括以下要求：

a) 测评指标：应具备软件设计的相关文档和使用指南，并对文档使用进行控制。
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文档和使用指南，并对文档使用进行控制。
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。

9.1.9.4.5 测评单元（L4-CMS1-16）

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。

9.1.9.4.6 测评单元（L4-CMS1-17）

该测评单元包括以下要求：

a) 测评指标：应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查对程序资源库的修改、更新、发布进行授权和审批的文档或记录是否有批准人的签字。
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。

9.1.9.4.7 测评单元（L4-CMS1-18）

该测评单元包括以下要求：

a) 测评指标：应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
b) 测评对象：建设负责人。
c) 测评实施：应访谈建设负责人开发人员是否为专职，是否对开发人员活动进行控制等。
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。

9.1.9.5 外包软件开发

9.1.9.5.1 测评单元（L4-CMS1-19）

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。

9.1.9.5.2 测评单元(L4-CMS1-20)

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。

9.1.9.5.3 测评单元(L4-CMS1-21)

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源代码,并审查软件中可能存在的后门和隐蔽信道。

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) 应访谈建设负责人委托开发单位是否提供软件源代码;

2) 应核查软件测试报告是否审查了软件可能存在的后门和隐蔽信道。

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。

9.1.9.6 工程实施

9.1.9.6.1 测评单元(L4-CMS1-22)

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。

9.1.9.6.2 测评单元(L4-CMS1-23)

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。

9.1.9.6.3 测评单元(L4-CMS1-24)

该测评单元包括以下要求:

a) 测评指标:应通过第三方工程监理控制项目的实施过程。

b) 测评对象:记录表单类文档。

c) 测评实施：应核查工程监理报告是否明确了工程进展、时间计划、控制措施等方面内容。
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。

9.1.9.7 测试验收

9.1.9.7.1 测评单元(L4-CMS1-25)

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。

9.1.9.7.2 测评单元(L4-CMS1-26)

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，安全测试报告应包含密码应用安全性测试相关内容。
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，报告应包含密码应用安全性测试相关内容。
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。

9.1.9.8 系统交付

9.1.9.8.1 测评单元(L4-CMS1-27)

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系统交付的各类设备、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。

9.1.9.8.2 测评单元(L4-CMS1-28)

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。

9.1.9.8.3 测评单元(L4-CMS1-29)

该测评单元包括以下要求:

a) 测评指标:应保证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。

9.1.9.9 等级测评

9.1.9.9.1 测评单元(L4-CMS1-30)

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。

9.1.9.9.2 测评单元(L4-CMS1-31)

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。

9.1.9.9.3 测评单元(L4-CMS1-32)

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。

9.1.9.10 服务供应商管理

9.1.9.10.1 测评单元(L4-CMS1-33)

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。

9.1.9.10.2 测评单元(L4-CMS1-34)

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：应核查与服务供应商签订的服务合同或安全责任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。

9.1.9.10.3 测评单元(L4-CMS1-35)

该测评单元包括以下要求：

a) 测评指标：应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

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) 应核查是否具有服务供应商定期提交的安全服务报告；

2) 应核查是否定期审核评价服务供应商所提供的服务及服务内容变更情况，是否具有服务审核报告；

3) 应核查是否具有服务供应商评价审核管理制度，明确针对服务供应商的评价指标、考核内容等。

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。

9.1.10 安全运维管理

9.1.10.1 环境管理

9.1.10.1.1 测评单元(L4-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。

9.1.10.1.2 测评单元（L4-MMS1-02）

该测评单元包括以下要求：

a） 测评指标：应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。
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。

9.1.10.1.3 测评单元（L4-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，不随意放置含有敏感信息的纸档文件和移动介质等。
b） 测评对象：管理制度类文档和办公环境。
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明确来访人员的接待区域；
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。

9.1.10.1.4 测评单元（L4-MMS1-04）

该测评单元包括以下要求：

a） 测评指标：应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等。
b） 测评对象：记录表单类文档。
c） 测评实施包括以下内容：
1） 应核查出入人员授权审批记录是否明确对人员进行不同的授权；
2） 应核查重要区域是否安装监控系统，实时监控进入人员活动。
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。

9.1.10.2 资产管理

9.1.10.2.1 测评单元(L4-MMS1-05)

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。

9.1.10.2.2 测评单元(L4-MMS1-06)

该测评单元包括以下要求：

a) 测评指标：应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。

b) 测评对象：资产管理员单、管理制度类文档和设备。

c) 测评实施包括以下内容：

1) 应访谈资产管理员是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施的选取上是否不同；

2) 应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求；

3) 应核查资产清单中的设备是否具有相应标识，标识方法是否符合 2)中相关要求。

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。

9.1.10.2.3 测评单元(L4-MMS1-07)

该测评单元包括以下要求：

a) 测评指标：应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

b) 测评对象：管理制度类文档。

c) 测评实施包括以下内容：

1) 应核查信息分类文档是否规定了分类标识的原则和方法(如根据信息的重要程度、敏感程度或用途不同进行分类)；

2) 应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等要求。

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。

9.1.10.3 介质管理

9.1.10.3.1 测评单元(L4-MMS1-08)

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。

9.1.10.3.2 测评单元(L4-MMS1-09)

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。

9.1.10.4 设备维护管理

9.1.10.4.1 测评单元(L4-MMS1-10)

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。

9.1.10.4.2 测评单元(L4-MMS1-11)

该测评单元包括以下要求:

a) 测评指标:应建立配套设施、软硬件维护方面的管理制度,对其维护进行有效管理,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) 应核查是否具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。

9.1.10.4.3 测评单元(L4-MMS1-12)

该测评单元包括以下要求：

a) 测评指标：信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。

b) 测评对象：设备管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈设备管理员含有重要数据的设备带出工作环境是否有加密措施；

2) 应访谈设备管理员对带离机房的设备是否经过审批；

3) 应核查是否具有设备带离机房或办公地点的审批记录。

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。

9.1.10.4.4 测评单元(L4-MMS1-13)

该测评单元包括以下要求：

a) 测评指标：含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

b) 测评对象：设备管理员。

c) 测评实施：应访谈设备管理员含有存储介质的设备在报废或重用前，是否采取措施进行完全清除或被安全覆盖。

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。

9.1.10.5 漏洞和风险管理

9.1.10.5.1 测评单元(L4-MMS1-14)

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。

9.1.10.5.2 测评单元(L4-MMS1-15)

该测评单元包括以下要求：

a) 测评指标：应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

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开展安全测评；

2） 应核查是否具有安全测评报告；

3） 应核查是否具有安全整改应对措施文档。

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。

9.1.10.6 网络和系统安全管理

9.1.10.6.1 测评单元（L4-MMS1-16）

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，系统管理员是否划分了不同角色，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。

9.1.10.6.2 测评单元（L4-MMS1-17）

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。

9.1.10.6.3 测评单元（L4-MMS1-18）

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。

9.1.10.6.4 测评单元（L4-MMS1-19）

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。

9.1.10.6.5 测评单元（L4-MMS1-20）

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。

9.1.10.6.6 测评单元（L3-MMS1-21）

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对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。

b) 测评对象：系统管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈网络和系统相关人员是否指定专门部门或人员对日志、监测和报警数据等进行分析统计；

2) 应核查是否具有对日志、监测和报警数据等进行分析统计的报告。

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。

9.1.10.6.7 测评单元（L4-MMS1-22）

该测评单元包括以下要求：

a) 测评指标：应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。

b) 测评对象：系统管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈网络和系统相关人员调整配置参数结束后是否同步更新配置信息库，并核实配置信息库是否为最新版本；

2) 应核查是否具有变更运维的审批记录，如系统连接、安装系统组件或调整配置参数等活动；

3) 应核查是否具有针对变更运维的操作过程记录。

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。

9.1.10.6.8 测评单元（L4-MMS1-23）

该测评单元包括以下要求：

a) 测评指标:应严格控制运维工具的使用,经过审批后才可接入进行操作,操作过程中应保留不可更改的审计日志,操作结束后应删除工具中的敏感数据。
b) 测评对象:系统管理员和记录表单类文档。
c) 测评实施包括以下内容:
   1) 应访谈系统相关人员使用运维工具结束后是否删除工具中的敏感数据;
   2) 应核查是否具有运维工具接入系统的审批记录;
   3) 应核查运维工具的审计日志记录,审计日志是否不可以更改。
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。

9.1.10.6.9 测评单元(L4-MMS1-24)

该测评单元包括以下要求:

a) 测评指标:应严格控制远程运维的开通,经过审批后才可开通远程运维接口或通道,操作过程中应保留不可更改的审计日志,操作结束后立即关闭接口或通道。
b) 测评对象:系统管理员和记录表单类文档。
c) 测评实施包括以下内容:
   1) 应访谈系统相关人员日常运维过程中是否存在远程运维,若存在,远程运维结束后是否立即关闭了接口或通道;
   2) 应核查开通远程运维的审批记录;
   3) 应核查针对远程运维的审计日志是否不可以更改。
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。

9.1.10.6.10 测评单元(L4-MMS1-25)

该测评单元包括以下要求:

a) 测评指标:应保证所有与外部的连接均得到授权和批准,应定期检查违反规定无线上网及其他违反网络安全策略的行为。
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) 应访谈系统相关人员网络外联连接(如互联网、合作伙伴企业网、上级部门网络等)是否都得到授权与批准;
   2) 应访谈安全管理员是否定期核查违规联网行为;
   3) 应核查是否具有外联授权的记录文件。
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。

9.1.10.7 恶意代码防范管理

9.1.10.7.1 测评单元(L4-MMS1-26)

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。

9.1.10.7.2 测评单元(L4-MMS1-27)

该测评单元包括以下要求：

a) 测评指标：应定期验证防范恶意代码攻击的技术措施的有效性。

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) 若采用可信验证技术，应访谈安全管理员是否未发生过恶意代码攻击事件；

2) 若采用防恶意代码产品，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，是否未出现过大规模的病毒事件；

3) 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)或 2)和 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。

9.1.10.8 配置管理

9.1.10.8.1 测评单元(L4-MMS1-28)

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。

9.1.10.8.2 测评单元(L4-MMS1-29)

该测评单元包括以下要求：

a) 测评指标：应将基本配置信息改变纳入系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

b) 测评对象：系统管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库；

2) 应核查配置信息的变更流程是否具有相应的申报审批程序。

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。