ICS 35.040
L80

35

中华人民共和国国家标准

GB/T 28448.1—XXXX

信息安全技术 网络安全等级保护测评要求

第 5 部分：工业控制安全扩展测评要求

Information Security Technology- Evaluation Requirement for Cybersecurity Classified Protection

Part 1：Industrial Control Security Extension Testing and Evaluation Requirement

征求意见稿

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

目 次

前　言

GB/T 28448《信息安全技术 网络安全等级保护测评要求》拟分成部分出版，各部分将按照应用的领域划分成安全通用测评要求和具体领域的安全扩展测评要求。目前计划发布以下部分：

——第 1 部分：安全通用测评要求；

——第 2 部分：云计算安全扩展测评要求；

——第 3 部分：移动互联安全扩展测评要求；

——第 4 部分：物联网安全扩展测评要求；

——第 5 部分：工控控制安全扩展测评要求；

——第 6 部分：大数据安全扩展测评要求。

本部分为 GB/T 28448 的第 5 部分。

本部分按照 GB/T 1.1－2009 给出的规则起草。

本部分代替 GB/T 28448-2012《信息技术 信息安全技术 信息系统安全等级保护测评要求》。与 GB/T 28448-2012 相比，除编辑性修改外主要技术变化如下：

——增加了总体要求，对 GB/T 22239.1-20XX 安全通用要求中的部分内容根据工控控制领域特点进行了增加、细化和增强。

——增加了安全等级保护测评定义、测评对象、单项测评、安全控制点测评、测评指标编码规则等内容。

——删除了测评框架、等级测评内容、区域间测评等内容。

——修改了单元测评、规范性引用文件、整体测评等内容。

本部分由全国信息安全标准化技术委员会提出。

本部分由全国信息安全标准化技术委员会归口。

本部分起草单位：XXX。

本部分主要起草人：XXX。

GB/T 28448 于 2012 年 6 月首次发布，本次为第一次修订。

引　言

GB/T 22240 在我国网络安全等级保护工作开展过程中发挥了重要的指导作用。GB/T 22240 自 2012 年发布以来，收到了许多标准使用者提出的修改意见和建议，在标准应用过程中，特别是云计算、移动互联、大数据、物联网和工控系统等新技术、新应用环境下也遇到了一些新的问题。此外，作为测评指标进行引用的 GB/T 22239 也启动了修订工作。为适应我国网络安全等级保护工作发展的需要，进一步与新版的 GB/T 22239 相协调，有必要对 GB/T 28448 进行修订。

网络安全等级保护测评要求
第 5 部分 工控控制安全扩展测评要求

1 范围

本部分规定了工控控制不同等级保护对象的安全扩展测评要求，包括对第一级工控系统、第二级工控系统、第三级工控系统和第四级工控系统进行安全扩展测评的单项测评要求和工控系统整体测评要求。本标准略去对第五级工控系统进行单项测评的具体内容要求。

本部分适用于信息安全测评服务机构、等级保护对象的主管部门及运营使用单位对等级保护对象安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的网络安全等级保护监督检查可以参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

GB17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22239.5-20XX 信息安全技术 网络安全等级保护基本要求 第 5 部分：工控控制安全扩展要求

GB/T 28449-20XX 信息安全技术 网络安全等级保护测评过程指南

GB/T 25070.5-20XX 信息安全技术 网络安全等级保护安全设计技术要求 第 5 部分：工控控制安全扩展要求

3 术语和定义

GB/T 25069-2010 和 GB/T 22239.5-20XX 界定的以及下列术语和定义适用于本文件。

3.1 访谈 interview

访谈是指测评人员通过引导等级保护对象相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、澄清或取得证据的过程。

3.2 核查 examination

核查是指测评人员通过对测评对象（如制度文档、各类设备、安全配置等）进行观察、查验、分析以帮助测评人员理解、澄清或取得证据的过程。

3.3 测试 testing

测试是指测评人员使用预定的方法/工具使测评对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行比对的过程。

3.4 安全等级保护测评 evaluation for security classified protection

安全等级保护测评（以下简称“等级测评”）是指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和计算标准，对未涉及国家秘密的等级保护对象进行安全等级保护状况进行检测评估的活动。等级测评是标准符合性评判活动，即依据信息安全等级保护的国家标准或行业标准，按照特定方法对等级保护对象的安全保护能力进行科学公正的综合

评判过程。

4 安全等级保护测评概述

4.1 安全等级保护测评方法

等级测评实施的基本方法是针对特定的测评对象，采用相关的测评手段，遵从一定的测评规程，获取需要的证据数据，给出是否达到特定级别安全保护能力的评判。等级测评实施的详细流程和方法参见 GB/T 28449-20XX。

本部分中针对每一个要求项的测评就构成一个单项测评，单项测评中的每一个具体测评实施要求项（以下简称“测评要求项”）是与安全控制点下面所包括的要求项（测评指标）相对应的。在对每一要求项进行测评时，可能用到访谈、核查和测试三种测试方法，也可能用到其中一种或两种。测评实施的内容完全覆盖了 GB/T 22239.5-20XX 及 GB/T25070.5-20XX（具体参见附录 C）中所有要求项的测评要求，使用时应当从单项测评的测评实施中抽取出对于 GB/T 22239.5-20XX 中每一个要求项的测评要求，并按照这些测评要求开发测评指导书，以规范和指导等级测评活动。

等级测评活动中涉及测评力度，包括测评广度（覆盖面）和测评深度（强弱度）。测评广度和测评深度特性影响着访谈、核查和测试的具体手段，也影响着证据数据的可信度，关于测评力度的具体描述参见附录 A。

4.2 单项测评和整体测评

安全等级保护测评分为单项测评和整体测评。

单项测评是针对各安全要求项的测评，支持测评结果的可重复性和可再现性。本部分中单项测评由测评指标、测评对象、测评实施和单项测评结果判定构成。

整体测评是在单项测评基础上，对等级保护对象整体安全保护能力的判断。整体安全保护能力从纵深防护和措施互补二个角度评判。

5 总体要求单项测评

5.1 总体技术能力测评

5.1.1 测评单元

a) 测评指标

工控控制系统与企业管理系统之间原则上应划分为两个区域，区域间应采用有效的隔离技术手段；禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。（新增）

b) 测评对象

网络拓扑结构、网闸、路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

1) 应确认工控控制系统的网络边界位置，并核查在网络边界处是否采用的有效的隔离措施实施访问控制；

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.1.2 测评单元

a) 测评指标

在工控控制系统内从生产管理层到现场设备层使用广域网的纵向交接处应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。（新增）

b) 测评对象

网络拓扑结构、加密认证设备、网闸、路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

应确认工控控制系统的网络边界位置，并核查在网络边界处是否采用的有效的认证、加密、访问控制等技术措施实施数据的远方安全传输以及纵向边界的安全防护。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

5.1.3 测评单元

a) 测评指标

涉及实时传输数据要求的工控控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离。（新增）

b) 测评对象

网络拓扑结构、网闸、路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

应确认工控控制系统关键部位的传输数据要求，涉及实时传输数据的，核查是否采用物理隔离措施实现关键部位安全防护。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

5.1.4 测评单元

a) 测评指标

工控控制系统内二级子系统统一成域，三级及以上子系统可单独成域；并采用 VLAN 或防火墙等技术手段实现各域之间的访问控制功能。（新增）

b) 测评对象

网络拓扑结构、路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

应确认工控控制系统内各子系统安全级别，并核查二、三、四级系统之间交换机、防火墙配置是否实现各域之间的访问控制功能。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

5.1.5 测评单元

a) 测评指标

工控控制系统应实现对网络流量、网络协议、网络设备安全日志、操作系统访问日志、数据库访问日志、业务应用系统运行日志、安全设施告警日志、控制设备运行日志等的集中收集、自动分析功能。（新增）

b) 测评对象

安全监控系统、安全审计系统、预警分析平台等审计类设备。

c) 测评实施

1) 应核查是否在系统中部署具备流量、日志监控功能的集中安全监控系统，对网络链路、安全设备、网络设备和服务器等的安全运行状况进行集中监测；

2) 应核查监测系统能否根据流量或日志的关联分析，形成预设值的（或默认阀值）实时报警。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

5.2 总体管理能力测评

5.2.1 测评单元

a) 测评指标

工控系统所属单位中出现多等级工控系统时，通用管理要求统一采用定级最高的工控系统执行。（新增）

b) 测评对象

定级文档。

c) 测评实施

应核查各工控系统定级报告，查看管理要求是否采用“就高原则”执行。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6 第一级单项测评

6.1 安全技术测评

6.1.1 物理和环境安全

6.1.1.1 物理访问控制

6.1.1.1.1 测评单元（L1-PES1-01）

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。（本条款引用自 GB/T 22239.1-20XX 5.1.1.1）

b) 测评对象

机房管理员和数据中心机房、场站机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.1.2 防盗窃和防破坏

6.1.1.2.1 测评单元（L1-PES1-02）

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记。（本条款引用自 GB/T 22239.1-20XX 5.1.1.2）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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记。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.1.3 防雷击

6.1.1.3.1 测评单元（L1-PES1-03）

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。（本条款引用自 GB/T 22239.1-20XX 5.1.1.3）

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.1.1.4 防火

6.1.1.4.1 测评单元（L1-PES1-04）

a) 测评指标

机房应设置灭火设备。（本条款引用自 GB/T 22239.1-20XX 5.1.1.4）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查灭火设备位置摆放是否合理；

2) 应核查机房内是否配备灭火设备且在有效期内；

3) 应访谈机房维护人员，询问是否对灭火设备定期进行核查和维护。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.1.5 防水和防潮

6.1.1.5.1 测评单元（L1-PES1-05）

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。（本条款引用自 GB/T 22239.1-20XX 5.1.1.5）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房的窗户、屋顶和墙壁等是否未出现过漏水、渗透和返潮现象；如果出现漏水、渗透和返潮现象，则查看是否能够及时修复解决；

2) 应核查机房的窗户、屋顶和墙壁是否采取了防雨水渗透的措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.1.6 温湿度控制

6.1.1.6.1 测评单元（L1-PES1-06）

a) 测评指标

机房应设置必要的温湿度控制设施，使机房温湿度的变化在设备运行所允许的范围之内。（本条款引用自 GB/T 22239.1-20XX 5.1.1.6）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房是否配备了专用空调，空调是否能够正常运行；

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，是否满足计算站场地的技术条件要求。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.1.7 电力供应

6.1.1.7.1 测评单元（L1-PES1-07）

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。（本条款引用自 GB/T 22239.1-20XX 5.1.1.7）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查供电可线路上是否配置了稳压器和过电压防护设备。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.1.1.8 室外控制设备防护

6.1.1.8.1 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备是否放置于采用铁板或其他防火尽缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备是否安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.1.1.8.2 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应远离极端天气环境，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行。

b) 测评对象

室外控制设备。

c) 测评实施

1) 应核查室外控制设备是否远离极端天气环境；

2) 应核查是否有极端天气时的检修维护记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.1.8.3 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备放置应远离强电磁干扰和热源。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备放置是否远离强电磁干扰和热源。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.1.2 网络和通信安全

6.1.2.1 网络架构

6.1.2.1.1 测评单元（L1-NCS1-01）

a) 测评指标

应保证网络设备的业务处理能力满足基本业务需要；（本条款引用自 GB/T 22239.1-20XX 5.1.2.1 a））

b) 测评对象

路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

1) 应访谈网络管理员了解系统的业务高峰时段，核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率；

2) 网络设备应未出现过宕机情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.1.2 测评单元（L1-NCS1-02）

a) 测评指标

应保证接入网络和核心网络的带宽满足基本业务需要。（本条款引用自 GB/T 22239.1-20XX 5.1.2.1 b））

b) 测评对象

网络管理员或综合网管系统。

c) 测评实施

应访谈网络管理员了解网络高峰时段，核查各通信链路带宽是否满足高峰时段的业务流量。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.1.2.2 通信传输

6.1.2.2.1 测评单元（L1-NCS1-03）

a) 测评指标

应采用校验码技术保证通信过程中数据的完整性。（本条款引用自 GB/T 22239.1-20XX 5.1.2.2）

b) 测评对象

加解密设备或组件。

c) 测评实施

应访谈安全管理员，询问是否在数据传输过程中使用校验码技术来保护其完整性。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

6.1.2.3 边界防护

6.1.2.3.1 测评单元（L1-NCS1-04）

a) 测评指标

应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。（本条款引用自 GB/T 22239.1-20XX 5.1.2.3）

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应确认等级保护对象的网络边界位置，并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，该端口配置并启用了安全策略；

3) 应访谈安全管理员或核查设备配置信息，是否不存在其他未受控端口进行跨越边界的网络通信。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.4 访问控制

6.1.2.4.1 测评单元（L1-NCS1-05）

a) 测评指标

应在网络边界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；（本条款引用自 GB/T 22239.1-20XX 5.1.2.4 a））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应核查在网络边界是否部署网络访问控制设备，是否启用访问控制策略；

2) 应核查设备的访问控制策略，确保手工配置或设备默认的最后一条策略为禁止所有网络通信。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.4.2 测评单元（L1-NCS1-06）

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；（本条款引用自 GB/T 22239.1-20XX 5.1.2.4 b））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应核查设备访问控制策略，访谈安全管理员每一条策略的用途，查看是否不存在多余或无效的访问控制策略；

2) 应核查安全策略逻辑关系及访问控制策略排列顺序是否合理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.2.4.3 测评单元（L1-NCS1-07）

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核查，以允许/拒绝数据包进出；（本条款引用自 GB/T 22239.1-20XX 5.1.2.4 c））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

应核查访问控制设备，查看是否对源地址、目的地址、源端口、目的端口和协议等进行核查。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.1.3 设备和计算安全

6.1.3.1 身份鉴别

6.1.3.1.1 测评单元（L1-ECS1-01）

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，用户名和口令不得相同，禁止明文存储口令。（增强）。（本条款引用自 GB/T 22239.1-20XX 5.1.3.1 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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，查看所有用户身份标识是否具有唯一性；

3) 应核查用户配置信息或访谈系统管理员，查看是否存在空密码用户；

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) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.1.2 测评单元（L1-ECS1-02）

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。（本条款引用自 GB/T 22239.1-20XX 5.1.3.1 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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达到一定次数后实现账户锁定功能；

3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.1.3 测评单元（L4-ECS1-36）

a) 测评指标

应能够对登录控制设备进行密码认证。

b) 测评对象

控制设备。

c) 测评实施

核查控制设备访问时是否提供密码认证选项。

d) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.2 访问控制

6.1.3.2.1 测评单元（L1-ECS1-03）

a) 测评指标

应对登录的用户分配账号和权限。（本条款引用自 GB/T 22239.1-20XX 5.1.3.2 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查或访谈用户账户和权限设置情况；

2) 应核查是否已禁用或限制匿名、默认账户的访问权限。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.2.2 测评单元（L1-ECS1-04）

a) 测评指标

应重命名默认账号或修改默认口令。（本条款引用自 GB/T 22239.1-20XX 5.1.3.2 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否不存在默认账号或默认账号已重命名；

2) 应核查是否已修改默认账号的默认口令。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.2.3 测评单元（L1-ECS1-05）

a) 测评指标

应及时删除或停用多余的、过期的账号，避免共享账号的存在。（本条款引用自 GB/T 22239.1-20XX 5.1.3.2 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否不存在多余或过期账号；

2) 应访谈了解是否不同用户采用不同登录账号登录系统。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.3 入侵防范

6.1.3.3.1 测评单元（L1-ECS1-06）

a) 测评指标

系统应遵循最小安装的原则，仅安装需要的组件和应用程序。（本条款引用自 GB/T 22239.1-20XX 5.1.3.3 a））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否遵循最小安装原则；

2) 应确认是否已经关闭非必要的组件和应用程序。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.3.2 测评单元（L1-ECS1-07）

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。（本条款引用自 GB/T 22239.1-20XX 5.1.3.3 b））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否定期对系统服务进行梳理，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.3.3 测评单元（L4-ECS1-36）

a) 测评指标

应使用专用设备或专用软件对控制设备进行更新。

b) 测评对象

控制设备。

c) 测评实施

应核查控制设备更新设备是否为专用设备或专用软件。

d) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

6.1.3.3.4 测评单元（L4-ECS1-30）

a) 测评指标

应关闭控制设备中不必要的端口和服务。

b) 测评对象

控制设备。

c) 测评实施

1) 应访谈管理员是否关闭了非必要的服务和端口；

2) 采用工控扫描设备对控制设备进行扫描。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.3.4 恶意代码防范

6.1.3.4.1 测评单元（L2-ECS1-08）

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。（本条款引用自 GB/T 22239.1-20XX 5.1.3.4）

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应查看防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.1.4 应用和数据安全

6.1.4.1 身份鉴别

6.1.4.1.1 测评单元（L1-ADS1-01）

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，鉴别信息具有复杂度要求并定期更换；（本条款引用自 GB/T 22239.1-20XX 5.1.4.1 a））

b) 测评对象

应用系统管理员和业务应用系统。

c) 测评实施

1) 应核查用户在登录时是否采用了身份鉴别措施；

2) 应核查用户登录时是否使用唯一性身份标识；

3) 应测试应用系统对用户身份标识有效性是否进行鉴别；

4) 应核查鉴别信息是否具有复杂度要求并定期更换；

5) 应核查用户配置信息或访谈应用系统管理员，查看是否不存在空密码用户。

d) **单项判定**

如果 1）-5）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.1.2 **测评单元（L1-ADS1-02）**

a) **测评指标**

应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；（本条款引用自 GB/T 22239.1-20XX 5.1.4.1 b））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应测试是否进行用户登录失败处理；

2) 应核查登录失败反馈信息是否进行模糊处理；

3) 应测试用户连续多次登录失败时应用系统是否采取必要的保护措施。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.2 **访问控制**

6.1.4.2.1 **测评单元（L1-ADS1-03）**

a) **测评指标**

应提供访问控制功能，对登录的用户分配帐号和权限；（本条款引用自 GB/T 22239.1-20XX 5.1.4.2 a））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应核查是否提供访问控制功能；

2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理；

3) 应测试不同岗位用户是否具有不同的权限。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.2.2 测评单元（L1-ADS1-04）

a) 测评指标

应重命名默认账户或修改默认口令；（本条款引用自 GB/T 22239.1-20XX 5.1.4.2 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否不存在默认账户或默认账户已重命名；

2) 应核查是否已修改默认账户的默认口令。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.2.3 测评单元（L1-ADS1-05）

a) 测评指标

应及时删除或停用多余的、过期的帐户，避免共享帐户的存在；（本条款引用自 GB/T 22239.1-20XX 5.1.4.2 c））

b) 测评对象

应用系统管理员和业务应用系统。

c) 测评实施

1) 应核查是否不存在多余账户或过期账户；

2) 应访谈了解是否不同用户采用不同登录账户登录应用系统。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.3 软件容错

6.1.4.3.1 测评单元（L1-ADS1-06）

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；（本条款引用自 GB/T 22239.1-20XX 5.1.4.3）

b) 测评对象

业务应用系统和系统设计文档等。

c) 测评实施

1) 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；

2) 应审核应用系统的源代码，在应用系统在人机接口或通信接口处是否对输入的数据进行有效性验证和处理；

3) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.4 数据完整性

6.1.4.4.1 测评单元（L1-ADS1-07）

a) **测评指标**

应采用校验码技术保证重要数据在传输过程中的完整性；（本条款引用自 GB/T 22239.1-20XX 5.1.4.4）

b) **测评对象**

系统设计文档和业务应用系统。

c) **测评实施**

1) 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码技术或加解密技术保证完整性；

2) 应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.1.4.5 数据备份恢复

6.1.4.5.1 测评单元（L1-ADS1-08）

a) **测评指标**

应提供重要数据的本地数据备份与恢复功能；（本条款引用自 GB/T 22239.1-20XX 5.1.4.5）

b) **测评对象**

配置数据和业务数据。

c) **测评实施**

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，查看是否能够进行正常的数据恢复。

d) **单项判定**

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2 安全管理测评

6.2.1 安全策略和管理制度

6.2.1.1 管理制度

6.2.1.1.1 测评单元(L1-PSS1-01）

a) 测评指标

应建立日常管理活动中常用的安全管理制度。（本条款引用自 GB/T 22239.1-20XX 5.2.1.1）

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，查看是否覆盖日常管理活动中的管理内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.1.1.2 测评单元(L1-PSS1-02）

a) 测评指标

应按照“谁主管谁负责，谁运营谁负责”的原则，建立工控系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。（新增）

b) 测评对象

安全管理制度类文档。

c) 测评实施

应核查工控系统安全管理制度，查看是否按照“谁主管谁负责，谁运营谁负责”的原则，制定信息安全工作的总体方针和安全策略，是否说明了机构安全工作的总体目标、范围、原则和安全框架等，是否将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.2 安全管理机构和人员

6.2.2.1 岗位设置

6.2.2.1.1 测评单元（L1-ORS1-01）

a) 测评指标

应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。（本条款引用自 GB/T 22239.1-20XX 5.2.2.1）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1） 应访谈信息安全主管，确认是否进行了信息安全管理岗位的划分；

2） 应核查岗位职责文档，查看是否明确了各岗位职责。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.1.2 测评单元（L1-ORS1-02）

a) 测评指标

应明确由主管安全生产的领导作为工控系统安全防护的主要责任人。（新增）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否由主管安全生产的领导作为工控系统安全防护的主要责任人；

2) 应核查岗位职责文档，查看是明确由主管安全生产的领导作为工控系统安全防护的主要责任人。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.2 资金保障

6.2.2.2.1 测评单元（L1-ORS1-01）

a) 测评指标

应保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金。（新增）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，是否能够保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金；

2) 应核查安全管理制度中是否有保障工控控制系统安全建设、运维、核查、等级保护

测评及其它信息安全资金的内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.3 人员配备

6.2.2.3.1 测评单元（L1-ORS1-02）

a) 测评指标

应配备一定数量的系统管理员、网络管理员、安全管理员等。（本条款引用自 GB/T 22239.1-20XX6.2.2.2）

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1） 应访谈信息安全主管，确认各岗位人员配备情况；

2） 应核查人员配备文档，查看各岗位人员配备情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.4 授权和审批

6.2.2.4.1 测评单元（L1-ORS1-03）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.2.3）

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

1） 应核查部门职责文档，查看各部门的职责和授权范围；

2） 应核查岗位职责文档，查看各岗位的职责和授权范围；

3） 应核查审批记录，查看审批事项、审批部门和批准人等内容是否与相关制度一致。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.2.5 人员录用

6.2.2.5.1 测评单元（L1-ORS1-04）

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。本条款引用自（GB/T 22239.1-20XX 6.2.2.4）

b) 测评对象

信息安全主管。

c) 测评实施

应访谈安全主管，询问是否由专门的部门或人员负责人员的录用工作。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.2.6 人员离岗

6.2.2.6.1 测评单元（L1-ORS1-05）

a) 测评指标

应及时终止离岗员工的所有访问权限，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。本条款引用自（GB/T 22239.1-20XX 6.2.2.5）

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交还身份证件、设备等的登记记录。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.2.7 安全意识教育和培训

6.2.2.7.1 测评单元（L1-ORS1-06）

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。本条款引用自（GB/T 22239.1-20XX 6.2.2.6）

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查信息安全教育及技能培训文档，查看是否明确培训周期、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，查看是否包含具体的安全责任和惩戒措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

6.2.2.8 外部人员访问管理

6.2.2.8.1 测评单元（L1-ORS1-07）

a) 测评指标

应确保在外部人员访问受控区域前得到授权或审批。本条款引用自（GB/T 22239.1-20XX 6.2.2.7））

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

1) 应核查外部人员访问管理文档，查看是否明确允许外部人员访问的范围（区域、系统、设备、信息等内容），外部人员进入的条件（对哪些重要区域的访问须提出书面申请批准后方可进入），外部人员进入的访问控制措施（由专人全程陪同或监督等）等；

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

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.3 安全建设管理

6.2.3.1 定级

6.2.3.1.1 测评单元（L1-CMS1-01）

a) 测评指标

应明确保护对象的边界和安全保护等级。（本条款引用自 GB/T 22239.1-20XX 5.2.3.1）

b) 测评对象

记录表单类文档。

c) 测评实施

应核查定级文档，查看文档是否明确保护对象的边界和安全保护等级，是否说明定级的方法和理由。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.2 安全方案设计

6.2.3.2.1 测评单元（L1-CMS1-02）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.3.2）

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，查看是否根据安全等级选择安全措施，是否根据安全需求调整安全措施。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.3 产品采购和使用

6.2.3.3.1 测评单元（L1-CMS1-03）

a) 测评指标

应确保信息安全产品采购和使用符合国家的有关规定。（本条款引用自 GB/T 22239.1-20XX 5.2.3.3）

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.3.2 测评单元（L1-CMS1-03）

a) 测评指标

工控控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用。（新增）

b) 测评对象

建设负责人、检测报告类文档。

c) 测评实施

1) 应访谈建设负责人，询问系统使用的工控控制系统重要设备及专用信息安全产品是否通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测；

2) 应核查工控控制系统通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测的检测报告。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.3.4 工程实施

6.2.3.4.1 测评单元（L1-CMS1-04）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.3.5）

b) 测评对象

建设负责人

c) 测评实施

应访谈建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.5 测试验收

6.2.3.5.1 测评单元（L1-CMS1-05）

a) 测评指标

应进行安全性测试验收。（本条款引用自 GB/T 22239.1-20XX 5.2.3.5）

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问是否进行了安全性测试验收。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.6 系统交付

6.2.3.6.1 测评单元（L1-CMS1-06）

a) 测评指标

1) 应根据交付清单对所交接的设备、软件和文档等进行清点；（本条款引用自 GB/T 22239.1-20XX 5.2.3.6 a））

a) 测评对象

记录表单类文档。

b) 测评实施

应核查是否具有交付清单，查看交付清单是否说明交付的各类设备、软件、文档等。

c) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.6.2 测评单元（L1-CMS1-07）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.3.6 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查是否有交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.7 服务供应商管理

6.2.3.7.1 测评单元（L1-CMS1-08）

a) 测评指标

应确保安全服务商的选择符合国家的有关规定；（本条款引用自 GB/T 22239.1-20XX 5.2.3.7 a））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问等级保护对象选择的安全服务商有哪些，是否符合国家有关规定。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.3.7.2 测评单元（L1-CMS1-09）

a) 测评指标

应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。（本条款引用自 GB/T 22239.1-20XX 5.2.3.7 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查是否具有与安全服务商签订的服务合同或安全责任合同书，查看是否明确了相关责任。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.4 安全运维管理

6.2.4.1 环境管理

6.2.4.1.1 测评单元（L1-MMS1-01）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.1 a））

b) 测评对象

物理安全负责人、记录表单类文档。

c) 测评实施

1) 应访谈物理安全负责人，询问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，由何部门/何人负责；

2) 应核查部门或人员岗位职责文档，查看是否明确机房安全的责任部门及人员；

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.1.2 测评单元（L1-MMS1-02）

a) 测评指标

应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。（本条款引用自 GB/T 22239.1-20XX 5.2.4.1 b））

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

1) 应核查机房安全管理制度，查看制度内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容；

2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录，是否与制度相符。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.1.3　测评单元（L4-PES1-24）

a)　测评指标

室外控制设备应明确专人负责，并定期进行核查、维护和清洁工作。

b)　测评对象

室外控制设备。

c)　测评实施

1)　应询问管理员室外控制设备是否有专人负责；

2)　应核查相关记录是否定期对室外控制设备进行核查、维护和清洁工作的记录。

d)　单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.2　介质管理

6.2.4.2.1　测评单元（L1-MMS1-03）

a)　测评指标

应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。（本条款引用自 GB/T 22239.1-20XX 5.2.4.2）

b)　测评对象

资产管理员、记录表单类文档。

c)　测评实施

1)　应访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理；

2)　应核查介质使用管理记录，查看其是否记录介质归档和使用等情况。

d)　单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.2.2　测评单元（L1-MMS1-03）

a)　测评指标

应建立隔离区域移动存储介质安全管理制度，对移动存储介质的使用进行限制。（新增）

b)　测评对象

资产管理员、管理制度类文档、记录表单类文档。

c)　测评实施

1)　应访谈资产管理员，询问是否建立隔离区域移动存储介质安全管理制度，是否对移动存储介质的使用进行限制；

2) 应查看是否有隔离区域移动存储介质安全管理制度是否有限制移动存储介质使用的内容；

3) 应核查隔离区与移动介质使用管理记录，查看其是否记录隔离区域移动存储介质归档和使用等情况。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.3 设备维护管理

6.2.4.3.1 测评单元（L1-MMS1-04）

a) 测评指标

应对等级保护对象相关的各种设备（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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.3）

b) 测评对象

设备管理员、管理制度类文档。

c) 测评实施

1) 应访谈设备管理员，询问是否对各类设施、设备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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.4 漏洞和风险管理

6.2.4.4.1 测评单元（L1-MMS1-05）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.4））

b) 测评对象

安全管理员、记录表单类文档。

c) 测评实施

1) 应访谈安全管理员，询问是否定期进行漏洞扫描，对发现的漏洞是否及时进行修补或评估可能的影响后进行修补；

2) 应核查漏洞扫描报告，查看内容是否描述了存在的漏洞、严重级别、原因分析和改进意见等方面。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

6.2.4.5 网络和系统安全管理

6.2.4.5.1 测评单元（L1-MMS1-06）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.5 a））

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，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）；

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.4.5.2 测评单元（L1-MMS1-07）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.5 b））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问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，查看是否对申请账户、建立账户、删除账户等进行控制。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.6 恶意代码防范管理

6.2.4.6.1 测评单元（L1-MMS1-08）

a) 测评指标

应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码核查等；（本条款引用自 GB/T 22239.1-20XX 5.2.4.6 a））

b) 测评对象

运维负责人。

c) 测评实施

应访谈运维负责人，询问是否采取告知方式提升员工的防病毒意识。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.4.6.2 测评单元（L1-MMS1-09）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.6 b））

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，查看是否明确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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.4.6.3 测评单元（L1-MMS1-09）

a) 测评指标

在更新恶意代码库、木马库以及 IDS 规则库前，应首先在测试环境中测试通过，对隔离区域恶意代码更新应有专人负责，更新操作应离线进行，并保存更新记录。（新增）

b) 测评对象

安全管理员、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈系统管理员，询问是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行，是否保存更新记录。

2) 应核查恶意代码防范管理制度，查看是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行等内容。

3) 应核查更新记录，查看是否有更新前在测试环境中测试通过的记录，隔离区域恶意代码更新是否为专人负责，更新操作是否离线的记录。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.7 备份与恢复管理

6.2.4.7.1 测评单元（L1-MMS1-10）

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；（本条款引用自 GB/T 22239.1-20XX 5.2.4.7 a））

b) 测评对象

系统管理员、网络管理员、数据库管理员和管理制度类文档。

c) 测评实施

1) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.7.2 测评单元（L1-MMS1-11）

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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.7 b））

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，查看是否明确备份方式、频度、介质、保存期等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.4.8 安全事件处置

6.2.4.8.1 测评单元（L1-MMS1-12）

a) 测评指标

应报告所发现的安全弱点和可疑事件；（本条款引用自 GB/T 22239.1-20XX 5.2.4.8 a））

b) 测评对象

运维负责人、管理制度类文档。

c) 测评实施

1) 应访谈运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应进行及时报告；

2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

6.2.4.8.2 **测评单元（L1-MMS1-13）**

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。（本条款引用自 GB/T 22239.1-20XX 5.2.4.8 b））

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，查看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) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

6.2.4.8.3 **测评单元（L1-MMS1-13）**

a) **测评指标**

应建立工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件。（新增）

b) **测评对象**

管理制度类文档、记录表单类文档。

c) **测评实施**

1) 应核查安全事件报告和处置管理制度，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容；

2) 应核查安全事件报告和处理程序文档，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7 第二级单项测评

7.1 安全技术测评

7.1.1 物理和环境安全

7.1.1.1 物理位置的选择

7.1.1.1.1 测评单元（L2-PES1-01）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.1.1 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 应核查是否存在雨水渗漏；

3) 应核查门窗是否因风导致的尘土严重；

4) 应核查屋顶、墙体、门窗和地面等是否破损开裂。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.1.2 测评单元（L2-PES1-02）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.1.1 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查是否不位于所在建筑物的顶层或地下室；

2) 如果机房位于所在建筑物的顶层或地下室，应核查是否采取了防水和防潮措施。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.2 物理访问控制

7.1.1.2.1 测评单元（L2-PES1-03）

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；（本

条款引用自 GB/T 22239.1-20XX 6.1.1.2 a））

b) 测评对象

机房管理员和数据中心机房、场站机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.2.2 测评单元（L2-PES1-04）

a) 测评指标

外部人员应经过审批才可进入机房，并限制和监控其活动范围；（本条款引用自 GB/T 22239.1-20XX 6.1.1.2 b））

b) 测评对象

记录类文档和机房管理员。

c) 测评实施

1) 应访谈是否通过审批限制外部人员进行机房，并限制和监控其活动范围；

2) 应核查是否具有外部人员进入机房的审批和监控记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.3 防盗窃和防破坏

7.1.1.3.1 测评单元（L2-PES1-05）

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记；（本条款引用自 GB/T 22239.1-20XX 6.1.1.3 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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记。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.3.2 测评单元（L2-PES1-06）

a) 测评指标

应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。（本条款引用自 GB/T 22239.1-20XX 6.1.1.3 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房内通信线缆是否铺设在隐蔽处或桥架中。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.1.4 防雷击

7.1.1.4.1 测评单元（L2-PES1-07）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.1.4）

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.1.5 防火

7.1.1.5.1 测评单元（L2-PES1-08）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.1.5 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.5.2 测评单元（L2-PES1-09）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.1.5 b））

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) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.6 防水和防潮

7.1.1.6.1 测评单元（L2-PES1-10）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.1.6 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.1.6.2 测评单元（L2-PES1-11）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.1.6 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.7 防静电

7.1.1.7.1 测评单元（L2-PES1-12）

a) 测评指标

应安装防静电地板并采用必要的接地防静电措施。（本条款引用自 GB/T 22239.1-20XX 6.1.1.7）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否安装了防静电地板；

2) 应核查机房内是否采用了接地防静电措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.8 温湿度控制

7.1.1.8.1 测评单元（L2-PES1-13）

a) 测评指标

机房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。（本条款引用自 GB/T 22239.1-20XX 6.1.1.8）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.9 电力供应

7.1.1.9.1 测评单元（L2-PES1-14）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.1.9 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.1.9.2 测评单元（L2-PES1-15）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.1.9 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查是否配备 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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.10 电磁防护

7.1.1.10.1 测评单元（L2-PES1-16）

a) 测评指标

电源线和通信线缆应隔离铺设，避免互相干扰。（本条款引用自 GB/T 22239.1-20XX 6.1.1.10）

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.1.11 室外控制设备防护

7.1.1.11.1 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备是否放置于采用铁板或其他防火尽缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备是否安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.1.11.2 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应远离极端天气环境，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行。

b) 测评对象

室外控制设备。

c) 测评实施

1) 应核查室外控制设备是否远离极端天气环境；

2) 应核查是否有极端天气时的检修维护记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.1.11.3 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备放置应远离强电磁干扰和热源。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备放置是否远离强电磁干扰和热源。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

7.1.2 网络和通信安全

7.1.2.1 网络架构

7.1.2.1.1 测评单元（L2-NCS1-01）

a) 测评指标

应保证网络设备的业务处理能力满足业务高峰期需要；（本条款引用自 GB/T 22239.1-20XX 6.1.2.1 a））

b) 测评对象

路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

1) 应访谈网络管理员了解系统的业务高峰时段，核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率；

2) 网络设备应未出现过宕机情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.2 测评单元（L2-NCS1-02）

a) 测评指标

应保证接入网络和核心网络的带宽满足业务高峰期需要；（本条款引用自 GB/T 22239.1-20XX 6.1.2.1 b））

b) 测评对象

网络管理员或综合网管系统。

c) 测评实施

1) 应访谈网络管理员了解网络高峰时段；

2) 应核查综合网管系统，查看各通信链路带宽是否满足高峰时段的业务流量。

d) 单项判定

如果 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.3 测评单元（L2-NCS1-03）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.2.1 c））

b) 测评对象

路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

1) 应访谈网络管理员依据何种原则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访谈结果一致。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.1.4 测评单元（L2-NCS1-04）

a) 测评指标

应避免将重要网络区域部署在网络边界处且没有边界防护措施。（本条款引用自 GB/T 22239.1-20XX 6.1.2.1 d））

b) 测评对象

网络管理员和网络拓扑图。

c) 测评实施

1) 应访谈网络管理员并查看网络拓扑图，核查重要网络区域不能部署在网络边界处且没有边界防护措施；

2) 应访谈网络管理员并查看网络拓扑图，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、ACL 等。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.2 通信传输

7.1.2.2.1 测评单元（L2-NCS1-05）

a) 测评指标

应采用校验码技术保证通信过程中数据的完整性。（本条款引用自 GB/T 22239.1-20XX 6.1.2.2）

b) 测评对象

加解密设备或组件。

c) 测评实施

应访谈安全管理员，询问是否在数据传输过程中使用校验码技术来保护其完整性。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.2.3 边界防护

7.1.2.3.1 测评单元（L2-NCS1-06）

a) 测评指标

应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。（本条款引用自 GB/T 22239.1-20XX 6.1.2.3）

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应确认等级保护对象的网络边界位置，并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，该端口配置并启用了安全策略；

3) 应访谈安全管理员或核查设备配置信息，是否不存在其他未受控端口进行跨越边界的网络通信。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.4 访问控制

7.1.2.4.1 测评单元（L2-NCS1-07）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.2.4 a））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应核查在网络边界或区域之间是否部署网络访问控制设备，是否启用访问控制策略；

2) 应核查设备的访问控制策略，确保手工配置或设备默认的最后一条策略为禁止所有网络通信。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.4.2 测评单元（L2-NCS1-08）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.2.4 b））

b) **测评对象**

网闸、防火墙、路由器和交换机等访问控制类设备。

c) **测评实施**

1) 应核查设备访问控制策略，访谈安全管理员每一条策略的用途，查看是否不存在多余或无效的访问控制策略；

2) 应核查安全策略逻辑关系及访问控制策略排列顺序是否合理。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.4.3 **测评单元（L2-NCS1-09）**

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核查，以允许/拒绝数据包进出；（本条款引用自 GB/T 22239.1-20XX 6.1.2.4 c））

b) **测评对象**

网闸、防火墙、路由器和交换机等访问控制类设备。

c) **测评实施**

应核查访问控制设备，查看是否对源地址、目的地址、源端口、目的端口和协议等进行核查。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.2.4.4 **测评单元（L2-NCS1-10）**

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，控制粒度为端口级。（本条款引用自 GB/T 22239.1-20XX 6.1.2.4 d））

b) **测评对象**

网闸、防火墙、路由器和交换机等访问控制类设备。

c) **测评实施**

应核查访问控制策略查看是否有明确的源地址、目的地址、源端口、目的端口和协议，访问控制粒度是否为端口级。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.2.4.5 测评单元（L2-NCS1-10）

a) 测评指标

工控控制系统隔离区域确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量；拨号服务器和客户端均应使用经安全加固的达到国家相应要求的操作系统，并采取加密、数字证书认证和访问控制等安全防护和其他管理措施。（新增）

b) 测评对象

拨号服务类设备。

c) 测评实施

1) 询问管理员工控控制系统隔离区域是否使用拨号服务类设备；

2) 应核查工控控制系统隔离区域是否有拨号服务类设备，是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用经安全加固的达到国家相应要求的操作系统，并采取加密、数字证书认证和访问控制等安全防护和其他管理措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.5 入侵防范

7.1.2.5.1 测评单元（L2-NCS1-11）

a) 测评指标

应在关键网络节点处监视网络攻击行为。（本条款引用自 GB/T 22239.1-20XX 6.1.2.5 ）

b) 测评对象

IPS、IDS、抗 APT 攻击、防 DDoS 和网络回溯等系统或设备。

c) 测评实施

1) 应核查相关系统或设备，查看能否检测以下攻击行为：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，查看是否及时更新；

3) 应测试相关系统或设备，验证其策略有效性；

4) 应核查相关系统或设备的防护策略，是否能够覆盖网络所有关键节点。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.6 安全审计

7.1.2.6.1 测评单元（L2-NCS1-12）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.2.6 a））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否开启了日志记录或安全审计功能；

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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.6.2 测评单元（L2-NCS1-13）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.2.6 b））

b) 测评对象

路由器、交换机和防火墙等设备。

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) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.2.6.3 测评单元（L2-NCS1-14）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.2.6 c））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制和备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3 设备和计算安全

7.1.3.1 身份鉴别

7.1.3.1.1 测评单元（L2-ECS1-01）

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，用户名和口令不得相同，禁止明文存储口令。（增强）。（本条款引用自 GB/T 22239.1-20XX 6.1.3.1 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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，查看所有用户身份标识是否具有唯一性；

3) 应核查用户配置信息或访谈系统管理员，查看是否存在空密码用户；

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) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.1.2 测评单元（L2-ECS1-02）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.1 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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达到一定次数后实现账户锁定功能；

3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.1.3 测评单元（L2-ECS1-03）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.1 d））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.3.1.4 测评单元（L4-ECS1-08）

a) 测评指标

应能够对控制设备控制及操作指令进行加密传输及认证鉴别。

b) 测评对象

控制设备。

c) 测评实施

1) 应核查控制设备控制及操作指令在进行远程传输时，是否进行加密处理；

2) 应查看智能控制装置，核查当现场设备层向控制装置发起会话连接时，是否使用认证措施进行会话认证（非身份认证）。

d) 单项判定

如果 1）-2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.1.5 测评单元（L4-ECS1-36）

e) 测评指标

应能够对登录控制设备进行密码认证。

f) 测评对象

控制设备。

g) 测评实施

核查控制设备访问时是否提供密码认证选项。

h) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.2 访问控制

7.1.3.2.1 测评单元（L2-ECS1-04）

a) 测评指标

应对登录的用户分配账号和权限。（本条款引用自 GB/T 22239.1-20XX 6.1.3.2 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查或访谈用户账户和权限设置情况；

2) 应核查是否已禁用或限制匿名、默认账户的访问权限。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.2.2 测评单元（L2-ECS1-05）

a) 测评指标

应重命名系统默认账号或修改默认口令。（本条款引用自 GB/T 22239.1-20XX 6.1.3.2 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否不存在默认账号或默认账号已重命名；

2) 应核查是否已修改默认账号的默认口令。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.2.3 测评单元（L2-ECS1-06）

a) 测评指标

应及时删除或停用多余的、过期的账号，避免共享账号的存在。（本条款引用自 GB/T 22239.1-20XX 6.1.3.2 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否不存在多余或过期账号；

2) 应访谈了解是否不同用户采用不同登录账号登录系统。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.2.4 **测评单元（L2-ECS1-07）**

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.2 d））

b) **测评对象**

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) **测评实施**

1) 应核查访问控制策略，查看管理用户的权限是否已进行分离；

2) 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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.3 **安全审计**

7.1.3.3.1 **测评单元（L2-ECS1-08）**

a) **测评指标**

应启用安全审计功能，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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.3 a））

b) **测评对象**

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) **测评实施**

1) 应核查是否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) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.3.2 **测评单元（L2-ECS1-09）**

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.3 b））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.3.3.3 测评单元（L2-ECS1-10）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.3 c））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制及备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.3.3.4 测评单元（L4-ECS1-25）

a) 测评指标

控制设备应具备日志收集功能。

b) 测评对象

控制设备。

c) 测评实施

应核查控制设备是否具有日志收集功能。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.3.3.5 测评单元（L4-ECS1-26）

a) 测评指标

控制设备的时钟保持应与时钟服务器同步。

b) 测评对象

控制设备。

c) 测评实施

应核查控制设备的时钟，确认其与时钟服务器是否同步。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.3.4 入侵防范

7.1.3.4.1 测评单元（L2-ECS1-11）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.4 a））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否遵循最小安装原则；

2) 应确认是否已经关闭非必要的组件和应用程序。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.4.2 测评单元（L2-ECS1-12）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.4 b））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否定期对系统服务进行梳理，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.4.3 测评单元（L2-ECS1-13）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.4 c））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应核查配置文件是否对终端接入范围进行限制。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.3.4.4 测评单元（L2-ECS1-14）

a) 测评指标

应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自 GB/T 22239.1-20XX 6.1.3.4 d））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应进行漏洞扫描，核查是否不存在高风险漏洞；

2) 应访谈系统管理员，查看是否在经过充分测试评估后及时修补漏洞。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.4.5 测评单元（L4-ECS1-36）

e) 测评指标

应使用专用设备或专用软件对控制设备进行更新。

f) 测评对象

控制设备。

g) 测评实施

应核查控制设备更新设备是否为专用设备或专用软件。

h) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.4.6 测评单元（L4-ECS1-30）

e) 测评指标

应关闭控制设备中不必要的端口和服务。

f) 测评对象

控制设备。

g) 测评实施

3) 应访谈管理员是否关闭了非必要的服务和端口；

4) 采用工控扫描设备对控制设备进行扫描。

h) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.5 恶意代码防范

7.1.3.5.1 测评单元（L2-ECS1-15）

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。（本条款引用自 GB/T 22239.1-20XX 6.1.3.5）

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应查看防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.3.5.2 测评单元（L4-ECS1-41）

a) 测评指标

应保证控制设备在入网前经过国家相关测评机构的安全性检测，确保控制设备固件中不存在恶意代码程序。

b) 测评对象

控制设备。

c) 测评实施

应核查控制设备经过国家相关测评机构检测的检测报告，明确控制设备固件中是否不存在恶意代码程序。若检测报告显示控制设备固件存在恶意代码程序，则询问终端管理员是否对恶意代码进行过处理，查看相关的处理报告和记录，并确认目前是否已不存在恶意代码程序。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6 资源控制

7.1.3.6.1 测评单元（L2-ECS1-16）

a) 测评指标

应限制单个用户或进程对系统资源的最大使用限度。（本条款引用自 GB/T 22239.1-20XX 6.1.3.6）

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员核查系统资源控制的管理措施，如核查配置参数是否设置最大进程数；

2) 应引用产品（应用）测试结果，确认目前系统资源利用率在允许范围之内或者查看数据库表空间，目前总体数据库表空间占用率是否超过阀值，是否存在对数据库资源过大或最小的用户的限制措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.3.6.2 测评单元（L2-ECS1-16）

a) 测评指标

应关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等，确需保留的必须通过相关的技术措施实施严格的监控管理。（新增）

b) 测评对象

终端和服务器等设备物理接口。

c) 测评实施

1) 应核查终端和服务器是否关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等；

2) 应访谈管理员对确需保留的软盘驱动、光盘驱动、USB 接口、串行口等是否通过相关的技术措施实施严格的监控管理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4 应用和数据安全

7.1.4.1 身份鉴别

7.1.4.1.1 测评单元（L2-ADS1-01）

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，鉴别信息具有复杂度要求

并定期更换；（本条款引用自 GB/T 22239.1-20XX 6.1.4.1 a））

b) 测评对象

应用系统管理员和业务应用系统。

c) 测评实施

1) 应核查用户在登录时是否采用了身份鉴别措施；

2) 应核查用户登录时是否使用唯一性身份标识；

3) 应测试应用系统对用户身份标识有效性是否进行鉴别；

4) 应核查鉴别信息是否具有复杂度要求并定期更换；

5) 应核查用户配置信息或访谈应用系统管理员，查看是否不存在空密码用户。

d) 单项判定

如果 1）-5）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.1.2 测评单元（L2-ADS1-02）

a) 测评指标

应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；（本条款引用自 GB/T 22239.1-20XX 6.1.4.1 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试是否进行用户登录失败处理；

2) 应核查登录失败反馈信息是否进行模糊处理；

3) 应测试用户连续多次登录失败时应用系统是否采取必要的保护措施。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.1.3 测评单元（L2-ADS1-03）

a) 测评指标

应强制用户首次登录时修改初始口令；（本条款引用自 GB/T 22239.1-20XX 6.1.4.1 c））

b) 测评对象

业务应用系统。

c) 测评实施

应测试用户首次登录时是否被强制修改初始口令。

d) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护

对象不符合或部分符合本单项测评指标要求。

7.1.4.1.4 测评单元（L2-ADS1-04）

a) 测评指标

用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。（本条款引用自 GB/T 22239.1-20XX 6.1.4.1 d））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试管理员是否能够对用户鉴别信息进行重置；

2) 应核查用户身份鉴别信息丢失或失效时，是否采取其他技术措施保证应用系统安全。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.2 访问控制

7.1.4.2.1 测评单元（L2-ADS1-05）

a) 测评指标

应提供访问控制功能，对登录的用户分配帐号和权限；（本条款引用自 GB/T 22239.1-20XX 6.1.4.2 a））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否提供访问控制功能；

2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理；

3) 应测试不同岗位用户是否具有不同的权限。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.2.2 测评单元（L2-ADS1-06）

a) 测评指标

应重命名默认账户或修改默认口令；（本条款引用自 GB/T 22239.1-20XX 6.1.4.2 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否不存在默认账户或默认账户已重命名；

2) 应核查是否已修改默认账户的默认口令。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.2.3 **测评单元（L2-ADS1-07）**

a) **测评指标**

应及时删除或停用多余的、过期的帐户，避免共享帐户的存在；（本条款引用自 GB/T 22239.1-20XX 6.1.4.2 c））

b) **测评对象**

应用系统管理员和业务应用系统。

c) **测评实施**

1) 应核查是否不存在多余账户或过期账户；

2) 应访谈了解是否不同用户采用不同登录账户登录应用系统。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.3 **安全审计**

7.1.4.3.1 **测评单元（L2-ADS1-08）**

a) **测评指标**

应提供并启用安全审计功能，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；（本条款引用自 GB/T 22239.1-20XX 6.1.4.3 a））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应核查是否提供并启用了安全审计功能；

2) 应核查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) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.3.2 **测评单元（L2-ADS1-09）**

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；（本条款引用自 GB/T 22239.1-20XX 6.1.4.3 b））

b) 测评对象

业务应用系统。

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) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.3.3 测评单元（L2-ADS1-10）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.4.3 c））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制及备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.4 软件容错

7.1.4.4.1 测评单元（L2-ADS1-11）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.4.4 a））

b) 测评对象

业务应用系统和系统设计文档等。

c) 测评实施

1) 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；

2) 应审核应用系统的源代码，在应用系统在人机接口或通信接口处是否对输入的数据进行有效性验证和处理；

3) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

7.1.4.4.2 测评单元（L2-ADS1-12）

a) 测评指标

在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；（本条款引用自 GB/T 22239.1-20XX 6.1.4.4 b））

b) 测评对象

系统设计文档和维护文档等。

c) 测评实施

1) 应核查应用系统设计文档和维护文档，应用系统有故障发生时是否能继续提供一部分功能；

2) 应核查应用系统设计文档和维护文档，应用系统有故障发生后，是否能够实施必要的措施使系统恢复功能。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.5 资源控制

7.1.4.5.1 测评单元（L2-ADS1-13）

a) 测评指标

当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；（本条款引用自 GB/T 22239.1-20XX 6.1.4.5 a））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。

d) 单项判定

如果 1） 为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.5.2 测评单元（L2-ADS1-14）

a) 测评指标

应能够对系统的最大并发会话连接数进行限制；（本条款引用自 GB/T 22239.1-20XX 6.1.4.5 b））

b) 测评对象

业务应用系统或中间件等。

c) 测评实施

1) 应核查应用系统配置信息是否对最大并发会话连接数进行限制；

2) 应核查中间件配置信息是否对最大并发会话连接数进行限制。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.5.3 测评单元（L2-ADS1-15）

a) 测评指标

应能够对单个账户的多重并发会话进行限制；（本条款引用自 GB/T 22239.1-20XX 6.1.4.5 c））

b) 测评对象

业务应用系统。

c) 测评实施

应测试是否能够正确地限制单个账户的多重并发会话数。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.4.6 数据完整性

7.1.4.6.1 测评单元（L2-ADS1-16）

a) 测评指标

应采用校验码技术保证重要数据在传输过程中的完整性；（本条款引用自 GB/T 22239.1-20XX 6.1.4.6）

b) 测评对象

系统设计文档和业务应用系统。

c) 测评实施

1) 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码技术或加解密技术保证完整性；

2) 应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.7 数据备份恢复

7.1.4.7.1 测评单元（L2-ADS1-17）

a) 测评指标

应提供重要数据的本地数据备份与恢复功能；（本条款引用自 GB/T 22239.1-20XX 6.1.4.7 a））

b) 测评对象

配置数据和业务数据。

c) 测评实施

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，查看是否能够进行正常的数据恢复。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.7.2 测评单元（L2-ADS1-18）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.4.7 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.1.4.8 剩余信息保护

7.1.4.8.1 测评单元（L2-ADS1-19）

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；（本条款引用自 GB/T 22239.1-20XX 6.1.4.8）

b) 测评对象

业务应用系统。

c) 测评实施

应核查相关配置信息或访谈应用系统管理员，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) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.9 个人信息保护

7.1.4.9.1 测评单元（L2-ADS1-20）

a) 测评指标

应仅采集和保存业务必需的用户信息；（本条款引用自 GB/T 22239.1-20XX 6.1.4.9 a））

b) 测评对象

用户数据和业务应用系统。

c) 测评实施

应核查采集的用户信息是否是业务应用必需的。

d) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.1.4.9.2 测评单元（L2-ADS1-21）

a) 测评指标

应禁止未授权访问和使用用户信息。（本条款引用自 GB/T 22239.1-20XX 6.1.4.9 b））

b) 测评对象

用户数据和业务应用系统。

c) 测评实施

应核查是否通过访问控制限制对用户信息的访问和使用。

d) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2 安全管理测评

7.2.1 安全策略和管理制度

7.2.1.1 管理制度

7.2.1.1.1 测评单元（L2-PSS1-01）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.1.1 a））

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，查看是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.1.1.2 测评单元（L2-PSS1-02）

a) 测评指标

应对要求管理人员或操作人员执行的日常管理操作建立操作规程。（本条款引用自 GB/T 22239.1-20XX 6.2.1.1 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.1.1.3 测评单元(L1-PSS1-02）

a) 测评指标

应按照“谁主管谁负责，谁运营谁负责”的原则，建立工控系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。（新增）

b) 测评对象

安全管理制度类文档。

c) 测评实施

应核查工控系统安全管理制度，查看是否按照“谁主管谁负责，谁运营谁负责”的原则，制定信息安全工作的总体方针和安全策略，是否说明了机构安全工作的总体目标、范围、原则和安全框架等，是否将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

7.2.1.2 制定和发布

7.2.1.2.1 测评单元（L2-PSS1-03）

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。（本条款引用自 GB/T 22239.1-20XX7.2.1.2 a））

b) 测评对象

信息安全主管。

c) 测评实施

应访谈安全主管，询问是否由专门的部门或人员负责制定安全管理制度。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.1.2.2 测评单元（L2-PSS1-04）

a) 测评指标

安全管理制度应通过正式和有效的方式发布，并进行版本控制。（本条款引用自 GB/T 22239.1-20XX 6.2.1.2 b））

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

1) 应核查制度制定和发布要求管理文档，查看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，查看是否通过正式、有效的方式收发（如正式发文、领导签署和单位盖章等），是否注明发布范围。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.1.3 评审和修订

7.2.1.3.1 测评单元（L2-PSS1-05）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.1.3）

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈安全主管，询问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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2 安全管理机构和人员

7.2.2.1 岗位设置

7.2.2.1.1 测评单元（L2-ORS1-01）

a) 测评指标

应设立信息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。（本条款引用自 GB/T 22239.1-20XX 6.2.2.1 a））

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否进行了信息安全管理职能部门的划分；

2) 应核查部门职责文档，查看是否明确信息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，查看岗位划分情况和岗位职责。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.1.2 测评单元（L2-ORS1-02）

a) 测评指标

应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。（本条款引用自 GB/T 22239.1-20XX 6.2.2.1 b））

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1） 应访谈信息安全主管，确认是否进行了信息安全管理岗位的划分；

2） 应核查岗位职责文档，查看是否明确了各岗位职责。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.1.3 测评单元（L1-ORS1-02）

a) 测评指标

应明确由主管安全生产的领导作为工控系统安全防护的主要责任人。（新增）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否由主管安全生产的领导作为工控系统安全防护的主要责任人；

2) 应核查岗位职责文档，查看是明确由主管安全生产的领导作为工控系统安全防护的主要责任人。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.2 资金保障

7.2.2.2.1 测评单元（L1-ORS1-01）

a) 测评指标

应保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金。（新增）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，是否能够保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金；

2) 应核查安全管理制度中是否有保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金的内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.3 人员配备

7.2.2.3.1 测评单元（L2-ORS1-03）

a) 测评指标

应配备一定数量的系统管理员、网络管理员、安全管理员等。（本条款引用自 GB/T 22239.1-20XX 6.2.2.2）

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1） 应访谈信息安全主管，确认各岗位人员配备情况；

2） 应核查人员配备文档，查看各岗位人员配备情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.4 授权和审批

7.2.2.4.1 测评单元（L2-ORS1-04）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.2.3 a））

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

1） 应核查部门职责文档，查看各部门的职责和授权范围；

2） 应核查岗位职责文档，查看各岗位的职责和授权范围；

3） 应核查审批记录，查看审批事项、审批部门和批准人等内容是否与相关制度一致。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.4.2 测评单元（L2-ORS1-05）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.2.3 b））

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，查看是否针对系统变更、重要操作、物理访问和系统接入等事项进行审批。

d) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.5 沟通和合作

7.2.2.5.1 测评单元（L2-ORS1-06）

a) 测评指标

应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题。（本条款引用自 GB/T 22239.1-20XX 6.2.2.4 a））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否建立了各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通机制；

2) 应核查会议记录，查看各类管理人员之间、组织内部机构之间以及信息安全职能部门内部是否开展了合作与沟通。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.5.2 测评单元（L2-ORS1-07）

a) 测评指标

应加强与兄弟单位、公安机关、各类供应商、业界专家及安全组织的合作与沟通。（本条款引用自 GB/T 22239.1-20XX 6.2.2.4 b））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否建立了与兄弟单位、公安机关、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，查看与兄弟单位、公安机关、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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.5.3 测评单元（L2-ORS1-08）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.2.4 c））

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，查看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) 单项判定

如果 以上测评实施内容，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.6 审核和核查

7.2.2.6.1 测评单元（L2-ORS1-09）

a) 测评指标

应定期进行常规安全核查，核查内容包括系统日常运行、系统漏洞和数据备份等情况。（本条款引用自 GB/T 22239.1-20XX 6.2.2.5）

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否定期进行了常规安全核查；

2) 应核查常规安全核查记录，查看记录内容是否包括了系统日常运行、系统漏洞和数据备份等情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.7 人员录用

7.2.2.7.1 测评单元（L2-ORS1-10）

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；（本条款引用自（GB/T 22239.1-20XX 7.2.2.6 a））

b) 测评对象

信息安全主管。

c) 测评实施

应访谈安全主管，询问是否由专门的部门或人员负责人员的录用工作。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.2.7.2 测评单元（L2-ORS1-11）

a) 测评指标

应对被录用人员的身份、背景、专业资格和资质等进行审查。（本条款引用自（GB/T 22239.1-20XX 7.2.2.6 b））

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

1) 应核查人员安全管理文档，查看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、背景、专业资格和资质等进行审查的相关文档或记录，查看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，查看是否记录考核内容和考核结果等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.8 人员离岗

7.2.2.8.1 测评单元（L2-ORS1-12）

a) 测评指标

应及时终止离岗员工的所有访问权限，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。（本条款引用自（GB/T 22239.1-20XX 7.2.2.7）

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交还身份证件、设备等的登记记录。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.2.9 安全意识教育和培训

7.2.2.9.1 测评单元（L2-ORS1-13）

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。（本条款引用自（GB/T 22239.1-20XX 7.2.2.8）

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查信息安全教育及技能培训文档，查看是否明确培训周期、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，查看是否包含具体的安全责任和惩戒措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.10 外部人员访问管理

7.2.2.10.1 测评单元（L2-ORS1-14）

a) 测评指标

应确保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；（本条款引用自（GB/T 22239.1-20XX 7.2.2.9 a））

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

1) 应核查外部人员访问管理文档，查看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，查看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，查看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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.10.2 测评单元（L2-ORS1-15）

a) 测评指标

应确保在外部人员接入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；（本条款引用自（GB/T 22239.1-20XX 7.2.2.9 b））

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

1) 应核查外部人员访问管理文档，查看是否明确外部人员接入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，查看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，查看是否记录了外部人员访问的权限、时限、账户等。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.2.10.3 **测评单元（L2-ORS1-16）**

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。（本条款引用自（GB/T 22239.1-20XX 7.2.2.9 c））

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**

1) 应核查外部人员访问管理文档，查看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，查看是否记录了访问权限清除时间。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3 **安全建设管理**

7.2.3.1 **定级和备案**

7.2.3.1.1 **测评单元（L2-CMS1-01）**

a) **测评指标**

应以书面的形式说明保护对象的边界、安全保护等级及确定等级的方法和理由；（本条款引用自 GB/T 22239.1-20XX 6.2.3.1 a））

b) **测评对象**

记录表单类文档。

c) **测评实施**

应核查定级文档，查看文档是否明确保护对象的边界和安全保护等级，是否说明定级的方法和理由。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.1.2 **测评单元（L2-CMS1-02）**

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.1 b））

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.1.3 测评单元（L2-CMS1-03）

a) 测评指标

应确保定级结果经过相关部门的批准；（本条款引用自 GB/T 22239.1-20XX 6.2.3.1 c））

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，查看是否有上级主管部门或本单位相关部门的审批意见。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.1.4 测评单元（L2-CMS1-04）

a) 测评指标

应将备案材料报主管部门和相应公安机关备案。（本条款引用自 GB/T 22239.1-20XX 6.2.3.1 d））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.2 安全方案设计

7.2.3.2.1 测评单元（L2-CMS1-05）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.2 a））

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，查看是否根据安全等级选择安全措施，是否根据安全需求调整安全措施。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.2.2 **测评单元（L2-CMS1-06）**

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.2 b））

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。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.2.3 **测评单元（L2-CMS1-07）**

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。（本条款引用自 GB/T 22239.1-20XX 6.2.3.2 c））

b) **测评对象**

记录表单类文档。

c) **测评实施**

1) 应核查配套文件的论证评审记录或文档，查看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论证意见；

2) 应核查是否有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

7.2.3.3 产品采购和使用

7.2.3.3.1 测评单元（L2-CMS1-08）

a) 测评指标

应确保信息安全产品采购和使用符合国家的有关规定；（本条款引用自 GB/T 22239.1-20XX 6.2.3.3 a））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.3.2 测评单元（L2-CMS1-09）

a) 测评指标

应确保密码产品采购和使用符合国家密码主管部门的要求。（本条款引用自 GB/T 22239.1-20XX 6.2.3.3 b））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.3.3 测评单元（L1-CMS1-03）

a) 测评指标

工控控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用。（新增）

b) 测评对象

建设负责人、检测报告类文档。

c) 测评实施

1) 应访谈建设负责人，询问系统使用的工控控制系统重要设备及专用信息安全产品是

否通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测；

2) 应核查工控控制系统通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测的检测报告。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.4 自行软件开发

7.2.3.4.1 测评单元（L2-CMS1-10）

a) **测评指标**

应确保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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.4 a））

b) **测评对象**

建设负责人。

c) **测评实施**

1) 应访谈建设负责人，询问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) **单项判定**

如果 1）-2 为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.4.2 测评单元（L2-CMS1-11）

a) **测评指标**

应确保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。（本条款引用自 GB/T 22239.1-20XX 6.2.3.4 b））

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，明确软件存在的安全问题及可能存在的恶意代码。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.5 外包软件开发

7.2.3.5.1 测评单元（L2-CMS1-12）

a) **测评指标**

应在软件交付前检测软件质量和其中可能存在的恶意代码；（本条款引用自 GB/T 22239.1-20XX 6.2.3.5 a））

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软件质量和恶意代码检测报告。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.5.2 测评单元（L2-CMS1-13）

a) 测评指标

应要求开发单位提供软件设计文档和使用指南。（本条款引用自 GB/T 22239.1-20XX 6.2.3.5 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.5.3 测评单元（L2-CMS1-13）

a) 测评指标

应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。（新增）

b) 测评对象

外包合同。

c) 测评实施

应核查外包开发合同中是否包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.6 工程实施

7.2.3.6.1 测评单元（L2-CMS1-14）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.6 a））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.6.2 测评单元（L2-CMS1-15）

a) 测评指标

应制定工程实施方案控制安全工程实施过程。（本条款引用自 GB/T 22239.1-20XX 6.2.3.6 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查工程实施方案，查看其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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.7 测试验收

7.2.3.7.1 测评单元（L2-CMS1-16）

a) 测评指标

在制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；（本条款引用自 GB/T 22239.1-20XX 6.2.3.7 a））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查是否具有工程测试验收方案，查看其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) 应核查是否具有测试验收报告，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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.7.2 **测评单元（L2-CMS1-17）**

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。（本条款引用自 GB/T 22239.1-20XX 6.2.3.7 b））

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) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.8 **系统交付**

7.2.3.8.1 **测评单元（L2-CMS1-18）**

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.8 a））

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清单，查看交付清单是否说明交付的各类设备、软件、文档等。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.8.2 **测评单元（L2-CMS1-19）**

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.8 b））

b) **测评对象**

记录表单类文档。

c) 测评实施

应核查是否有交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.8.3 测评单元（L2-CMS1-20）

a) 测评指标

应确保提供建设过程中的文档和指导用户进行运行维护的文档。（本条款引用自 GB/T 22239.1-20XX 6.2.3.8 c））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查交付文档，查看是否有指导用户进行运维的文档等，提交的文档是否符合管理规定的要求。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.9 等级测评

7.2.3.9.1 测评单元（L2-CMS1-21）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.9 a））

b) 测评对象

运维负责人和记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，本次测评是否为首次，若非首次，以往进行过几次测评，是否根据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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.9.2 测评单元（L2-CMS1-22）

a) 测评指标

应在发生重大变更或系统级别发生变化时进行等级测评；（本条款引用自 GB/T 22239.1-20XX 6.2.3.9 b））

b) 测评对象

运维负责人和记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，是否过重大变更或级别发生过变化，若有，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.3.9.3 测评单元（L2-CMS1-23）

a) 测评指标

应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。（本条款引用自 GB/T 22239.1-20XX 6.2.3.9 c））

b) 测评对象

运维负责人。

c) 测评实施

应访谈运维负责人，以往等级测评的测评单位是否具有国家相关等级测评资质的单位。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.3.10 服务供应商管理

7.2.3.10.1 测评单元（L2-CMS1-24）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.3.10 a））

b) 测评对象

运维负责人。

c) 测评实施

应访谈建设负责人，询问等级保护对象选择的安全服务商有哪些，是否符合国家有关规定。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

7.2.3.10.2 测评单元（L2-CMS1-25）

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信息安全相关义务。（本条款引用自 GB/T 22239.1-20XX 6.2.3.10 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查是否具有与安全服务商签订的服务合同或安全责任合同书，查看是否明确了后期的技术支持和服务承诺等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4 安全运维管理

7.2.4.1 环境管理

7.2.4.1.1 测评单元（L2-MMS1-01）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.1 a））

b) 测评对象

物理安全负责人、记录表单类文档。

c) 测评实施

1) 应访谈物理安全负责人，询问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，由何部门/何人负责；
2) 应核查部门或人员岗位职责文档，查看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，查看是否记录来访人员、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，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.1.2 测评单元（L2-MMS1-02）

a) 测评指标

应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；（本条款引用自 GB/T 22239.1-20XX 6.2.4.1 b）

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

1) 应核查机房安全管理制度，查看制度内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容；

2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录，是否与制度相符。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.1.3 测评单元（L2-MMS1-03）

a) 测评指标

应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等。（本条款引用自 GB/T 22239.1-20XX 6.2.4.1 c）

b) 测评对象

管理制度类文档、办公环境。

c) 测评实施

1) 应访谈重要区域相关人员在哪接待来访人员或者是否有相关规定；

2) 应核查办公桌面上是否包含敏感信息的纸档文件、移动介质等。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.1.4 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应明确专人负责，并定期进行核查、维护和清洁工作。

b) 测评对象

室外控制设备。

c) 测评实施

1) 应询问管理员室外控制设备是否有专人负责；

2) 应核查相关记录是否定期对室外控制设备进行核查、维护和清洁工作的记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.2 资产管理

7.2.4.2.1 测评单元（L2-MMS1-04）

a) 测评指标

应编制并保存与等级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。（本条款引用自 GB/T 22239.1-20XX 6.2.4.2）

b) 测评对象

记录表单类文档。

c) 测评实施

应核查资产清单，查看其内容是否覆盖资产责任部门、重要程度和所处位置等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.3 介质管理

7.2.4.3.1 测评单元（L2-MMS1-05）

a) 测评指标

应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；（本条款引用自 GB/T 22239.1-20XX 6.2.4.3 a））

b) 测评对象

资产管理员、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理；

2) 应核查介质使用管理记录，查看其是否记录介质归档和使用等情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.3.2 测评单元（L2-MMS1-06）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.4.3 b））

b) 测评对象

资产管理员、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问介质在物理传输过程中的人员、打包交付等情况是否进行控制；

2) 应核查是否有对介质的归档和查询等的登记记录。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.3.3 **测评单元（L1-MMS1-03）**

a) **测评指标**

应建立隔离区域移动存储介质安全管理制度，对移动存储介质的使用进行限制。（新增）

b) **测评对象**

资产管理员、管理制度类文档、记录表单类文档。

c) **测评实施**

1) 应访谈资产管理员，询问是否建立隔离区域移动存储介质安全管理制度，是否对移动存储介质的使用进行限制；

2) 应查看是否有隔离区域移动存储介质安全管理制度是否有限制移动存储介质使用的内容；

3) 应核查隔离区与移动介质使用管理记录，查看其是否记录隔离区域移动存储介质归档和使用等情况。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.4 **设备维护管理**

7.2.4.4.1 **测评单元（L2-MMS1-07）**

a) **测评指标**

应对等级保护对象相关的各种设备（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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.4 a））

b) **测评对象**

设备管理员、管理制度类文档。

c) **测评实施**

1) 应访谈设备管理员，询问是否对各类设施、设备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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.4.2 测评单元（L2-MMS1-08）

a) 测评指标

应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。（本条款引用自 GB/T 22239.1-20XX 6.2.4.4 b））

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

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

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

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.5 漏洞和风险管理

7.2.4.5.1 测评单元（L2-MMS1-09）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.5）

b) 测评对象

安全管理员、记录表单类文档。

c) 测评实施

1) 应访谈安全管理员，询问是否定期进行漏洞扫描，对发现的漏洞是否及时进行修补或评估可能的影响后进行修补；

2) 应核查漏洞扫描报告，查看内容是否描述了存在的漏洞、严重级别、原因分析和改进意见等方面。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.6 网络和系统安全管理

7.2.4.6.1 测评单元（L2-MMS1-10）

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；（本

条款引用自 GB/T 22239.1-20XX 6.2.4.6 a））

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文档，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）；

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.6.2 测评单元（L2-MMS1-11）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.6 b））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问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，查看是否对申请账户、建立账户、删除账户等进行控制。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.6.3 测评单元（L2-MMS1-12）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.6 c））

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，查看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、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备

和系统的口令更新周期等方面。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.6.4 测评单元（L2-MMS1-13）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.6 d）

b) 测评对象

操作规程类文档。

c) 测评实施

1) 应核查是否针对网络和系统制定了重要设备（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，查看是否明确操作步骤、维护记录、参数配置等内容。

d) 单项判定

如果 1)）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.6.5 测评单元（L2-MMS1-14）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.4.6 e）

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.7 恶意代码防范管理

7.2.4.7.1 测评单元（L2-MMS1-15）

a) 测评指标

应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码核查等；（本条款引用自 GB/T 22239.1-20XX 6.2.4.7 a）

b) 测评对象

运维负责人。

c) 测评实施

应访谈运维负责人，询问是否采取告知方式提升员工的防病毒意识。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.7.2 测评单元（L2-MMS1-16）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.7 b）

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，查看是否明确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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.7.3 测评单元（L2-MMS1-17）

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。（本条款引用自 GB/T 22239.1-20XX 6.2.4.7 c）

b) 测评对象

安全管理员、记录表单类文档。

c) 测评实施

1) 应访谈安全管理员，询问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。

3) 应定期采用技术手段测试验证恶意代码防范技术措施的有效性。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.7.4 测评单元（L1-MMS1-09）

a) 测评指标

在更新恶意代码库、木马库以及 IDS 规则库前，应首先在测试环境中测试通过，对隔离区域恶意代码更新应有专人负责，更新操作应离线进行，并保存更新记录。（新增）

b) 测评对象

安全管理员、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈系统管理员，询问是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行，是否保存更新记录。

2) 应核查恶意代码防范管理制度，查看是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行等内容。

3) 应核查更新记录，查看是否有更新前在测试环境中测试通过的记录，隔离区域恶意代码更新是否为专人负责，更新操作是否离线的记录。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.8 配置管理

7.2.4.8.1 测评单元（L2-MMS1-18）

a) 测评指标

应记录和保存系统的基本配置信息，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。（本条款引用自 GB/T 22239.1-20XX 6.2.4.8）

b) 测评对象

系统管理员。

c) 测评实施

1) 应访谈系统管理员，询问是否对基本配置信息进行记录和保存。

2) 查看记录表单类文档是否对基本配置信息进行记录

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.9 密码管理

7.2.4.9.1 测评单元（L2-MMS1-19）

a) 测评指标

应使用符合国家密码管理规定的密码技术和产品；（本条款引用自 GB/T 22239.1-20XX 6.2.4.9 a））

b) 测评对象

安全管理员。

c) 测评实施

应核查该是否获得有效的国家密码管理规定的检测报告或密码产品型号证书。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.10 变更管理

7.2.4.10.1 测评单元（L2-MMS1-21）

a) 测评指标

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。（本条款引用自 GB/T 22239.1-20XX 6.2.4.10）

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查变更方案，查看其是否包含变更类型、变更原因、变更过程、变更前评估等内容；

2) 应核查是否具有变更方案评审记录和变更过程记录文档。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.11 备份与恢复管理

7.2.4.11.1 测评单元（L2-MMS1-22）

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.11 a））

b) 测评对象

系统管理员、网络管理员、数据库管理员、管理制度类文档。

c) 测评实施

1) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.11.2 **测评单元（L2-MMS1-23）**

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；（本条款引用自 GB/T 22239.1-20XX 6.2.4.11 b）

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，查看是否明确备份方式、频度、介质、保存期等内容。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.11.3 **测评单元（L2-MMS1-24）**

a) **测评指标**

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。（本条款引用自 GB/T 22239.1-20XX 6.2.4.11 c）

b) **测评对象**

管理制度类文档。

c) **测评实施**

应核查备份和恢复的策略，查看内容是否明确备份策略和恢复策略文档规范了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.12 **安全事件处置**

7.2.4.12.1 **测评单元（L2-MMS1-25）**

a) **测评指标**

应报告所发现的安全弱点和可疑事件；（本条款引用自 GB/T 22239.1-20XX 6.2.4.12 a）

b) **测评对象**

运维负责人、管理制度类文档。

c) 测评实施

1) 应访谈运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应进行及时报告；

2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.12.2 测评单元（L2-MMS1-26）

a) 测评指标

应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等；（本条款引用自 GB/T 22239.1-20XX 6.2.4.12 c）

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管理制度，查看内容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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.12.3 测评单元（L2-MMS1-27）

a) 测评指标

应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。（本条款引用自 GB/T 22239.1-20XX 6.2.4.12 d）

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查安全事件报告和响应处置记录，查看其是否记录引发安全事件的系统弱点、不同安全事件发生的原因、处置过程、经验教训总结、补救措施等内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.12.4 测评单元（L1-MMS1-13）

a) 测评指标

应建立工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件。（新增）

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

1) 应核查安全事件报告和处置管理制度，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容；

2) 应核查安全事件报告和处理程序文档，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容。。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.13 应急预案管理

7.2.4.13.1 测评单元（L2-MMS1-28）

a) 测评指标

应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；（本条款引用自 GB/T 22239.1-20XX 6.2.4.13 a））

b) 测评对象

管理制度类文档。

c) 测评实施

应核查是否具有根据应急预案框架制定不同事件的应急预案（如针对机房、系统、网络等各个层面）。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

7.2.4.13.2 测评单元（L2-MMS1-29）

a) 测评指标

应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；（本条款引用自 GB/T 22239.1-20XX 6.2.4.13 b））

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查应急预案框架或相关文档，查看是否明确应急小组、相关设备及资金保障。

d) **单项判定**

如果 1）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.13.3 **测评单元（L2-MMS1-30）**

a) **测评指标**

应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。（本条款引用自 GB/T 22239.1-20XX 6.2.4.13 c））

b) **测评对象**

运维负责人、记录表单类文档。

c) **测评实施**

1) 应访谈运维负责人，是否定期对相关人员进行应急预案培训和演练；

2) 应核查应急预案培训记录，查看是否明确培训对象、培训内容、培训结果等；

3) 应核查应急预案演练记录，查看是否记录演练时间、主要操作内容、演练结果等。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.14 **外包运维管理**

7.2.4.14.1 **测评单元（L2-MMS1-31）**

a) **测评指标**

应确保外包运维服务商的选择符合国家的有关规定；（本条款引用自 GB/T 22239.1-20XX 6.2.4.14 a））

b) **测评对象**

运维负责人。

c) **测评实施**

1) 应访谈运维负责人，询问对等级保护对象进行运维是否有外包运维服务情况；

2) 应访谈运维负责人，询问对等级保护对象进行外包运维服务的服务单位是否符合国家有关规定。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

7.2.4.14.2 **测评单元（L2-MMS1-32）**

a) **测评指标**

应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。（本

条款引用自 GB/T 22239.1-20XX 6.2.4.14 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查外包运维服务协议，查看协议内容是否明确约定外包运维的范围和工作内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8 第三级单项测评

8.1 安全技术测评

8.1.1 物理和环境安全

8.1.1.1 物理位置的选择

8.1.1.1.1 测评单元（L3-PES1-01）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.1 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 应核查是否存在雨水渗漏；

3) 应核查门窗是否因风导致的尘土严重；

4) 应核查屋顶、墙体、门窗和地面等是否破损开裂。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.1.2 测评单元（L3-PES1-02）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.1.1 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查是否不位于所在建筑物的顶层或地下室；

2) 如果机房位于所在建筑物的顶层或地下室，应核查是否采取了防水和防潮措施。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.2 物理访问控制

8.1.1.2.1 测评单元（L3-PES1-03）

a) 测评指标

机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。（本条款引用自 GB/T 22239.1-20XX 7.1.1.2）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查出入口是否配置电子门禁系统；

2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.3 防盗窃和防破坏

8.1.1.3.1 测评单元（L3-PES1-04）

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记；（本条款引用自 GB/T 22239.1-20XX 7.1.1.3 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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记。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.3.2 测评单元（L3-PES1-05）

a) 测评指标

应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；（本条款引用自 GB/T 22239.1-20XX 7.1.1.3 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房内通信线缆是否铺设在隐蔽处或桥架中。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.3.3 测评单元（L3-PES1-06）

a) 测评指标

应设置机房防盗报警系统或设置有专人值守的视频监控系统。（本条款引用自 GB/T 22239.1-20XX 7.1.1.3 c））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否配置防盗报警系统或专人值守的视频监控系统；

2) 应核查防盗报警系统或视频监控系统是否启用。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.4 防雷击

8.1.1.4.1 测评单元（L3-PES1-07）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.4 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.4.2 测评单元（L3-PES1-08）

a) 测评指标

应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。（本条款引用自 GB/T

22239.1-20XX 7.1.1.4 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否设置防感应雷措施；

2) 应核查防雷装置是否通过验收或国家有关部门的技术检测。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.5 防火

8.1.1.5.1 测评单元（L3-PES1-09）

a) 测评指标

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.5 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.5.2 测评单元（L3-PES1-10）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.5 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.5.3 测评单元（L3-PES1-11）

a) 测评指标

应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。（本条款引用自 GB/T 22239.1-20XX 7.1.1.5 c））

b) 测评对象

机房管理员和机房。

c) 测评实施

1) 应访谈机房管理员是否进行了区域划分；

2) 应核查各区域间是否采取了防火措施进行隔离。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.6 防水和防潮

8.1.1.6.1 测评单元（L3-PES1-12）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.6 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.6.2 测评单元（L3-PES1-13）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.6 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.6.3 测评单元（L3-PES1-14）

a) 测评指标

应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。（本条款引用自 GB/T 22239.1-20XX 7.1.1.6 c））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否安装了对水敏感的检测装置；

2) 应核查防水检测和报警装置是否启用。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.7 防静电

8.1.1.7.1 测评单元（L3-PES1-15）

a) 测评指标

应安装防静电地板并采用必要的接地防静电措施；（本条款引用自 GB/T 22239.1-20XX 7.1.1.7 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否安装了防静电地板；

2) 应核查机房内是否采用了接地防静电措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.7.2 测评单元（L3-PES1-16）

a) 测评指标

应采用措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。（本条款引用自 GB/T 22239.1-20XX 7.1.1.7 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房内是否配备了防静电设备。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.8 温湿度控制

8.1.1.8.1 测评单元（L3-PES1-17）

a) 测评指标

机房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。（本条款引用自 GB/T 22239.1-20XX 7.1.1.8）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.9 电力供应

8.1.1.9.1 测评单元（L3-PES1-18）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.9 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.9.2 测评单元（L3-PES1-19）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.1.9 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查是否配备 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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.9.3 测评单元（L3-PES1-20）

a) 测评指标

应设置冗余或并行的电力电缆线路为计算机系统供电。（本条款引用自 GB/T 22239.1-20XX 7.1.1.9 c））

b) 测评对象

机房管理员和机房。

c) 测评实施

1) 应访谈机房管理员确认机房供电是否来自两个不同的变电站；

2) 应核查机房内是否设置了冗余或并行的电力电缆线路为计算机系统供电。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.1.10 电磁防护

8.1.1.10.1 测评单元（L3-PES1-21）

a) 测评指标

电源线和通信线缆应隔离铺设，避免互相干扰。（本条款引用自 GB/T 22239.1-20XX 7.1.1.10）

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.10.2 测评单元（L3-PES1-22）

a) 测评指标

应对关键设备实施电磁屏蔽。（本条款引用自 GB/T 22239.1-20XX 7.1.1.10 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房内是否为关键设备配备了电磁屏蔽装置。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.11 室外控制设备防护

8.1.1.11.1 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备是否放置于采用铁板或其他防火尽缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备是否安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.1.11.2 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应远离极端天气环境，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行。

b) 测评对象

室外控制设备。

c) 测评实施

1) 应核查室外控制设备是否远离极端天气环境；

2) 应核查是否有极端天气时的检修维护记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

8.1.1.11.3 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备放置应远离强电磁干扰和热源。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备放置是否远离强电磁干扰和热源。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.2 网络和通信安全

8.1.2.1 网络架构

8.1.2.1.1 测评单元（L3-NCS1-01）

a) 测评指标

应保证网络设备的业务处理能力满足业务高峰期需要；（本条款引用自 GB/T 22239.1-20XX 7.1.2.1 a））

b) 测评对象

路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

1) 应访谈网络管理员了解系统的业务高峰时段，核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率；

2) 网络设备应未出现过宕机情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.1.2 测评单元（L3-NCS1-02）

a) 测评指标

应保证网络各个部分的带宽满足业务高峰期需要；（本条款引用自 GB/T 22239.1-20XX 7.1.2.1 b））

b) 测评对象

网络管理员或综合网管系统。

c) 测评实施

1) 应访谈网络管理员了解网络高峰时段；

2) 应核查综合网管系统，查看各通信链路带宽是否满足高峰时段的业务流量。

d) **单项判定**

如果 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.1.3 **测评单元（L3-NCS1-03）**

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.1 c））

b) **测评对象**

路由器、交换机和防火墙等网络通信类设备。

c) **测评实施**

1) 应访谈网络管理员依据何种原则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访谈结果一致。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.1.4 **测评单元（L3-NCS1-04）**

a) **测评指标**

应避免将重要网络区域部署在网络边界处且没有边界防护措施；（本条款引用自 GB/T 22239.1-20XX 7.1.2.1 d））

b) **测评对象**

网络管理员和网络拓扑图。

c) **测评实施**

1) 应访谈网络管理员并查看网络拓扑图，核查重要网络区域不能部署在网络边界处且直接连接外部等级保护对象；

2) 应访谈网络管理员并查看网络拓扑图，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、ACL 等。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.1.5 **测评单元（L3-NCS1-05）**

a) **测评指标**

应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。（本条款引用自 GB/T 22239.1-20XX 7.1.2.1 e））

b) 测评对象

网络管理员和网络拓扑图。

c) 测评实施

应访谈管理员并查看网络拓扑图，核查系统是否有主要网络设备、安全设备和通信线路的硬件冗余。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.2.2 通信传输

8.1.2.2.1 测评单元（L3-NCS1-06）

a) 测评指标

应采用校验码技术或加解密技术保证通信过程中数据的完整性；（本条款引用自 GB/T 22239.1-20XX 7.1.2.2 a））

b) 测评对象

加解密设备或组件。

c) 测评实施

1) 应访谈安全管理员，询问是否在数据传输过程中使用校验码技术或其他加解密技术来保护其完整性；

2) 应核查加解密设备或组件，查看是否保证通信过程中数据的完整性。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.2.2 测评单元（L3-NCS1-07）

a) 测评指标

应采用加解密技术保证通信过程中敏感信息字段或整个报文的保密性。（本条款引用自 GB/T 22239.1-20XX 7.1.2.2 b））

b) 测评对象

加解密设备或组件。

c) 测评实施

1) 应访谈安全管理员，询问是否具有在通信过程中是否采取保密措施，具体措施有哪些；

2) 应测试在通信过程中是否对敏感信息字段或整个报文进行加密。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不

符合或部分符合本单项测评指标要求。

8.1.2.3 边界防护

8.1.2.3.1 测评单元（L3-NCS1-08）

a) 测评指标

应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；（本条款引用自 GB/T 22239.1-20XX 7.1.2.3 a））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应确认等级保护对象的网络边界位置，并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，该端口配置并启用了安全策略；

3) 应访谈安全管理员或核查设备配置信息，是否不存在其他未受控端口进行跨越边界的网络通信。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.3.2 测评单元（L3-NCS1-09）

a) 测评指标

应能够对非授权设备私自联到内部网络的行为进行限制或核查；（本条款引用自 GB/T 22239.1-20XX 7.1.2.3 b））

b) 测评对象

网络准入控制系统或设备。

c) 测评实施

1) 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断；

2) 应核查所有路由器和交换机闲置端口是否均已关闭。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.3.3 测评单元（L3-NCS1-10）

a) 测评指标

应能够对内部用户非授权联到外部网络的行为进行限制或核查；（本条款引用自 GB/T 22239.1-20XX 7.1.2.3 c））

b) 测评对象

网络准入控制系统或设备。

c) 测评实施

应核查是否采用技术措施防止内部用户非法外联行为。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.2.3.4 测评单元（L3-NCS1-11）

a) 测评指标

应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。（本条款引用自 GB/T 22239.1-20XX 7.1.2.3 d））

b) 测评对象

网络拓扑图和无线网络设备。

c) 测评实施

1) 应访谈网络管理员无线网络的部署方式，是否单独组网后再连接到有线网络；

2) 应确保无线网络通过受控的边界防护设备接入到内部有线网络。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.4 访问控制

8.1.2.4.1 测评单元（L3-NCS1-12）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.4 a））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应核查在网络边界或区域之间是否部署网络访问控制设备，是否启用访问控制策略；

2) 应核查设备的访问控制策略，确保手工配置或设备默认的最后一条策略为禁止所有网络通信。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.4.2 测评单元（L3-NCS1-13）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.4 b））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应核查设备访问控制策略，访谈安全管理员每一条策略的用途，查看是否不存在多余或无效的访问控制策略；

2) 应核查安全策略逻辑关系及访问控制策略排列顺序是否合理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.4.3 测评单元（L3-NCS1-14）

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核查，以允许/拒绝数据包进出；（本条款引用自 GB/T 22239.1-20XX 7.1.2.4 c））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

应核查访问控制设备，查看是否对源地址、目的地址、源端口、目的端口和协议等进行核查。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.2.4.4 测评单元（L3-NCS1-15）

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，控制粒度为端口级；（本条款引用自 GB/T 22239.1-20XX 7.1.2.4 d））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

应核查访问控制策略查看是否有明确的源地址、目的地址、源端口、目的端口和协议，访问控制粒度是否为端口级。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

8.1.2.4.5 测评单元（L3-NCS1-16）

a) 测评指标

应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。（本条款引用自 GB/T 22239.1-20XX 7.1.2.4 e））

b) 测评对象

应用层防火墙等访问控制类设备。

c) 测评实施

1) 应核查在关键网络节点处是否部署应用层访问控制设备，是否启用访问控制策略；

2) 应核查设备是否通过访问控制策略对进出网络的信息内容进行过滤，实现对内容的访问控制。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.4.6 测评单元（L2-NCS1-10）

a) 测评指标

工控控制系统隔离区域确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量；拨号服务器和客户端均应使用经安全加固的达到国家相应要求的操作系统，并采取加密、数字证书认证和访问控制等安全防护和其他管理措施。（新增）

b) 测评对象

拨号服务类设备。

c) 测评实施

1) 询问管理员工控控制系统隔离区域是否使用拨号服务类设备；

2) 应核查工控控制系统隔离区域是否有拨号服务类设备，是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用经安全加固的达到国家相应要求的操作系统，并采取加密、数字证书认证和访问控制等安全防护和其他管理措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.5 入侵防范

8.1.2.5.1 测评单元（L3-NCS1-17）

a) 测评指标

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；（本条款引用自 GB/T 22239.1-20XX 7.1.2.5 a））

b) 测评对象

IPS、IDS、抗 APT 攻击、防 DDoS 和网络回溯等系统或设备。

c) 测评实施

1) 应核查相关系统或设备，查看能否检测、防止或限制从外部发起的网络攻击行为；

2) 应核查相关系统或设备的规则库版本，查看是否及时更新；

3) 应测试相关系统或设备，验证其策略有效性；

4) 应核查相关系统或设备的防护策略，是否能够覆盖网络所有关键节点。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.5.2 测评单元（L3-NCS1-18）

a) 测评指标

应在关键网络节点处检测和限制从内部发起的网络攻击行为；（本条款引用自 GB/T 22239.1-20XX 7.1.2.5 b））

b) 测评对象

IPS、IDS、抗 APT 攻击、防 DDoS 和网络回溯等系统或设备。

c) 测评实施

1) 应核查相关系统或设备，查看能否检测和限制从内部发起的网络攻击行为；

2) 应核查相关系统或设备的规则库版本，查看是否及时更新；

3) 应测试相关系统或设备，验证其策略有效性；

4) 应核查相关系统或设备的防护策略，是否能够覆盖网络所有关键节点。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.5.3 测评单元（L3-NCS1-19）

a) 测评指标

应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；（本条款引用自 GB/T 22239.1-20XX 7.1.2.5 c））

b) 测评对象

网络回溯和抗 APT 攻击等系统或设备。

c) 测评实施

1) 应核查是否部署网络回溯系统或抗 APT 攻击系统用来检测新型网络攻击；

2) 应核查系统能否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

d) 单项判定

如果 1）- 2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.2.5.4 测评单元（L3-NCS1-20）

a) 测评指标

当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。（本条款引用自 GB/T 22239.1-20XX 7.1.2.5 d））

b) 测评对象

IPS、IDS、抗 APT 攻击、防 DDoS 和网络回溯等系统或设备。

c) 测评实施

1) 应核查相关系统或设备，查看记录中是否包括：入侵源 IP、攻击类型、攻击目的、攻击时间等；

2) 应测试相关系统或设备验证其报警策略的有效性。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.6 恶意代码防范

8.1.2.6.1 测评单元（L3-NCS1-21）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.6 a））

b) 测评对象

防病毒网关和 UTM 等防恶意代码设备。

c) 测评实施

1) 应核查在关键网络节点处是否有相应的防恶意代码措施；

2) 应核查防恶意代码产品，查看其运行是否正常，恶意代码库是否及时更新。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.6.2 测评单元（L3-NCS1-22）

a) 测评指标

应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。（本条款引用自 GB/T 22239.1-20XX 7.1.2.6 b））

b) 测评对象

防垃圾邮件网关等设备。

c) 测评实施

1) 应核查在关键网络节点处是否部署了防垃圾邮件类产品；

2) 应核查防垃圾邮件产品，查看其运行是否正常，防垃圾邮件规则库是否及时更新。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.7 安全审计

8.1.2.7.1 测评单元（L3-NCS1-23）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.7 a））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否开启了日志记录或安全审计功能；

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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.7.2 测评单元（L3-NCS1-24）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.7 b））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 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) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.7.3 测评单元（L3-NCS1-25）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.7 c））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制及备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.7.4 测评单元（L3-NCS1-26）

a) 测评指标

审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；（本条款引用自 GB/T 22239.1-20XX 7.1.2.7 d））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否统一使用系统范围内唯一确定的时钟，以确保审计分析的正确性。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.7.5 测评单元（L3-NCS1-27）

a) 测评指标

应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。（本条款引用自 GB/T 22239.1-20XX 7.1.2.7 e））

b) 测评对象

上网行为管理系统或日志审计类设备。

c) 测评实施

1) 应访谈并核查是否对远程访问用户及互联网访问用户行为单独进行审计分析。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.8 集中管控

8.1.2.8.1 测评单元（L3-NCS1-28）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.8 a））

b) 测评对象

安全管理员和网络拓扑图。

c) 测评实施

1) 应访谈安全管理员并核查网络拓扑，查看是否划分单独网络区域用于部署安全管理系统；

2) 应核查各安全管理系统是否集中部署在安全管理区域。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.8.2 测评单元（L3-NCS1-29）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.8 b））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查网络是否建立安全的路由控制策略，如使用静态路由，或对动态路由协议启用加密认证机制；

2) 应核查网络中是否划分单独的管理 VLAN 用于对安全设备或安全组件进行管理；

3) 应核查网络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) 单项判定

如果 1）-3）其中之一为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.2.8.3 测评单元（L3-NCS1-30）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.8 c））

b) 测评对象

集中安全管控系统、IPS、ID 等。

c) 测评实施

1) 应核查是否在网络中部署具备状态监控功能的集中安全管控系统，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) 应核查监测系统能否根据网络链路、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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.8.4 测评单元（L3-NCS1-31）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.8 d））

b) 测评对象

综合安全审计系统、数据库审计系统或集中安全管控系统等。

c) 测评实施

1) 应核查网络中各设备是否配置独立于设备的集中安全管控系统，用于收集、存储设备日志；

2) 应核查是否部署统一的集中安全管控系统，统一收集、存储各设备日志，并根据需要进行集中审计分析。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.8.5 测评单元（L3-NCS1-32）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.2.8 e））

b) 测评对象

集中安全管控系统等。

c) 测评实施

1) 应核查是否通过安全管理区对网络安全策略（如防火墙访问控制策略、IPS 防护策略、WAF 防护策略等）进行统一管理；

2) 应核查是否实现对主机操作系统的防病毒软件及网络恶意代码防护设备的统一管理，实现病毒库的实时、统一升级；

3) 应核查是否实现网络中各设备统一、及时的补丁升级。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.2.8.6 测评单元（L3-NCS1-33）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.2.8 f））

b) 测评对象

集中安全管控系统等。

c) 测评实施

1) 应核查网络中是否在网络边界及关键节点，部署集中安全管控系统，并通过声光方式实时报警；

2) 应核查集中安全管控系统的检测范围是否能够覆盖网络所有关键路径。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3 设备和计算安全

8.1.3.1 身份鉴别

8.1.3.1.1 测评单元（L3-ECS1-01）

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，用户名和口令不得相同，禁止明文存储口令。（增强）。（本条款引用自 GB/T 22239.1-20XX 7.1.3.1 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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，查看所有用户身份标识是否具有唯一性；

3) 应核查用户配置信息或访谈系统管理员，查看是否存在空密码用户；

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) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.1.2 测评单元（L3-ECS1-02）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.1 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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达到一定次数后实现账户锁定功能；

3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.1.3 测评单元（L3-ECS1-03）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.1 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.1.4 测评单元（L3-ECS1-04）

a) 测评指标

应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。（本条款引用自 GB/T 22239.1-20XX 7.1.3.1 d））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别；

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.1.5 测评单元（L4-ECS1-08）

e) 测评指标

应能够对控制设备控制及操作指令进行加密传输及认证鉴别。

f) 测评对象

控制设备。

g) 测评实施

3) 应核查控制设备控制及操作指令在进行远程传输时，是否进行加密处理；

4) 应查看智能控制装置，核查当现场设备层向控制装置发起会话连接时，是否使用认证措施进行会话认证（非身份认证）。

h) 单项判定

如果 1）-2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.1.6 测评单元（L4-ECS1-36）

i) 测评指标

应能够对登录控制设备进行密码认证。

j) 测评对象

控制设备。

k) 测评实施

核查控制设备访问时是否提供密码认证选项。

l) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.2 访问控制

8.1.3.2.1 测评单元（L3-ECS1-05）

a) 测评指标

应对登录的用户分配账号和权限。（本条款引用自 GB/T 22239.1-20XX 7.1.3.2 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查或访谈用户账号和权限设置情况；

2) 应核查是否已禁用或限制匿名、默认账号的访问权限。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.2.2 测评单元（L3-ECS1-06）

a) 测评指标

应重命名默认账号或修改默认口令。（本条款引用自 GB/T 22239.1-20XX 7.1.3.2 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否不存在默认账号或默认账号已重命名；

2) 应核查是否已修改默认账号的默认口令。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.2.3 测评单元（L3-ECS1-07）

a) 测评指标

应及时删除或停用多余的、过期的账号，避免共享账号的存在。（本条款引用自 GB/T 22239.1-20XX 7.1.3.2 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否不存在多余或过期账号；

2) 应访谈了解是否不同用户采用不同登录账号登录系统。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.2.4 测评单元（L3-ECS1-08）

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。（本条款引用自 GB/T

22239.1-20XX 7.1.3.2 d））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查访问控制策略，查看管理用户的权限是否已进行分离；

2) 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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.2.5 测评单元（L3-ECS1-09）

a) 测评指标

应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。（本条款引用自 GB/T 22239.1-20XX 7.1.3.2 e））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否有管理用户负责配置访问控制策略；

2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则；

3) 应测试用户是否有可越权访问情形。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.2.6 测评单元（L3-ECS1-10）

a) 测评指标

访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。（本条款引用自 GB/T 22239.1-20XX 7.1.3.2 f））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.2.7 测评单元（L3-ECS1-11）

a) 测评指标

应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。（本条款引用自 GB/T 22239.1-20XX 7.1.3.2 g））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否依据安全策略对敏感信息资源设置了安全标记；

2) 应测试依据主体、客体安全标记控制主体对客体访问的强制访问控制功能。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.3 安全审计

8.1.3.3.1 测评单元（L3-ECS1-12）

a) 测评指标

应启用安全审计功能，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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.3 a））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应核查是否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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.3.2 测评单元（L3-ECS1-13）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.3 b））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.3.3 测评单元（L3-ECS1-14）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.3 c））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制及备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.3.4 测评单元（L3-ECS1-15）

a) 测评指标

应对审计进程进行保护，防止未经授权的中断。（本条款引用自 GB/T 22239.1-20XX 7.1.3.3 d））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应测试可否通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.3.5 测评单元（L3-ECS1-16）

a) 测评指标

审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。

（本条款引用自 GB/T 22239.1-20XX 7.1.3.3 e））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应核查是否统一使用系统范围内唯一确定的时钟，以确保审计分析的正确性。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.3.6 测评单元（L4-ECS1-25）

e) 测评指标

控制设备应具备日志收集功能。

f) 测评对象

控制设备。

g) 测评实施

应核查控制设备是否具有日志收集功能。

h) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.3.7 测评单元（L4-ECS1-26）

e) 测评指标

控制设备的时钟保持应与时钟服务器同步。

f) 测评对象

控制设备。

g) 测评实施

应核查控制设备的时钟，确认其与时钟服务器是否同步。

h) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.4 入侵防范

8.1.3.4.1 测评单元（L3-ECS1-17）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.4 a））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否遵循最小安装原则；

2) 应确认是否已经关闭非必要的组件和应用程序。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.4.2 测评单元（L3-ECS1-18）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.4 b））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否定期对系统服务进行梳理，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.4.3 测评单元（L3-ECS1-19）

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。（本条款引用自 GB/T 22239.1-20XX 7.1.3.4 c））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应核查配置文件是否对终端接入范围进行限制。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.4.4 测评单元（L3-ECS1-20）

a) 测评指标

应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自 GB/T 22239.1-20XX 7.1.3.4 d））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应进行漏洞扫描，核查是否不存在高风险漏洞；

2) 应访谈系统管理员，查看是否在经过充分测试评估后及时修补漏洞。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.4.5 测评单元（L3-ECS1-21）

a) 测评指标

应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。（本条款引用自 GB/T 22239.1-20XX 7.1.3.4 e））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈并查看入侵检测的措施，访谈是否部署了入侵检测工具；

2) 应查看重要节点的入侵行为记录和报警情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.4.6 测评单元（L4-ECS1-36）

i) 测评指标

应使用专用设备或专用软件对控制设备进行更新。

j) 测评对象

控制设备。

k) 测评实施

应核查控制设备更新设备是否为专用设备或专用软件。

l) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.4.7 测评单元（L4-ECS1-30）

i) 测评指标

应关闭控制设备中不必要的端口和服务。

j) 测评对象

控制设备。

k) 测评实施

5) 应访谈管理员是否关闭了非必要的服务和端口；

6) 采用工控扫描设备对控制设备进行扫描。

l) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.5 恶意代码防范

8.1.3.5.1 测评单元（L3-ECS1-22）

a) 测评指标

应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。（本条款引用自 GB/T 22239.1-20XX 7.1.3.5）

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应查看防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库，或查看是否采用可信计算技术建立从系统到应用的信任链；

2) 应访谈管理员，查看是否有保护重要系统程序或文件完整性的措施；

3) 应当检测到程序或文件受到破坏后，是否具备恢复的措施。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.5.2 测评单元（L4-ECS1-41）

e) 测评指标

应保证控制设备在入网前经过国家相关测评机构的安全性检测，确保控制设备固件中不存在恶意代码程序。

f) 测评对象

控制设备。

g) 测评实施

应核查控制设备经过国家相关测评机构检测的检测报告，明确控制设备固件中是否不存在恶意代码程序。若检测报告显示控制设备固件存在恶意代码程序，则询问终端管理员是否对恶意代码进行过处理，查看相关的处理报告和记录，并确认目前是否已不存在恶意代码程序。

h) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.6 资源控制

8.1.3.6.1 测评单元（L3-ECS1-23）

a) 测评指标

应限制单个用户或进程对系统资源的最大使用限度。（本条款引用自 GB/T 22239.1-20XX 7.1.3.6 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员核查系统资源控制的管理措施，如核查配置参数是否设置最大进程数；

2) 应引用产品（应用）测试结果，确认目前系统资源利用率在允许范围之内或者查看数据库表空间，目前总体数据库表空间占用率是否超过阀值，是否存在对数据库资源过大或最小的用户的限制措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.6.2 测评单元（L3-ECS1-24）

a) 测评指标

应提供重要节点设备的硬件冗余，保证系统的可用性。（本条款引用自 GB/T 22239.1-20XX 7.1.3.6 b））

b) 测评对象

终端、控制设备和服务器等设备。

c) 测评实施

查看重要节点设备是否有硬件冗余。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.3.6.3 测评单元（L3-ECS1-25）

a) 测评指标

应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况。（本条款引用自 GB/T 22239.1-20XX 7.1.3.7 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员，核查重要节点的系统 CPU、硬盘、内存、磁盘容量、网络服务等系统监控的手段和措施；

2) 应询问管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.6.4 测评单元（L3-ECS1-26）

a) 测评指标

应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。（本条款引用自 GB/T 22239.1-20XX 7.1.3.7 d））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员，查看是否有报警机制；

2) 应询问管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.3.6.5 测评单元（L2-ECS1-16）

a) 测评指标

应关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等，确需保留的必须通过相关的技术措施实施严格的监控管理。（新增）

b) 测评对象

终端和服务器等设备物理接口。

c) 测评实施

1) 应核查终端和服务器是否关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等；

2) 应访谈管理员对确需保留的软盘驱动、光盘驱动、USB 接口、串行口等是否通过相关的技术措施实施严格的监控管理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4 应用和数据安全

8.1.4.1 身份鉴别

8.1.4.1.1 测评单元（L3-ADS1-01）

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，鉴别信息具有复杂度要求并定期更换；（本条款引用自 GB/T 22239.1-20XX 7.1.4.1 a））

b) 测评对象

应用系统管理员和业务应用系统。

c) 测评实施

1) 应核查用户在登录时是否采用了身份鉴别措施；

2) 应核查用户登录时是否使用唯一性身份标识；

3) 应测试应用系统对用户身份标识有效性是否进行鉴别；

4) 应核查鉴别信息是否具有复杂度要求并定期更换；

5) 应核查用户配置信息或访谈应用系统管理员，查看是否不存在空密码用户。

d) 单项判定

如果 1）-5）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.1.2 测评单元（L3-ADS1-02）

a) 测评指标

应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；（本条款引用自 GB/T 22239.1-20XX 7.1.4.1 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试是否进行用户登录失败处理；

2) 应核查登录失败反馈信息是否进行模糊处理；

3) 应测试用户连续多次登录失败时应用系统是否采取必要的保护措施。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.1.3 测评单元（L3-ADS1-03）

a) 测评指标

应强制用户首次登录时修改初始口令；（本条款引用自 GB/T 22239.1-20XX 7.1.4.1 c））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试用户首次登录时是否被强制修改初始口令。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.1.4 测评单元（L3-ADS1-04）

a) 测评指标

用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。（本条款引用自 GB/T 22239.1-20XX 7.1.4.1 d））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试管理员是否能够对用户鉴别信息进行重置；

2) 应核查用户身份鉴别信息丢失或失效时，是否采取其他技术措施保证应用系统安全。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.1.5 测评单元（L3-ADS1-05）

a) 测评指标

应采用两种或两种以上组合的鉴别技术实现用户身份鉴别。（本条款引用自 GB/T 22239.1-20XX 7.1.4.1 e））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.2 访问控制

8.1.4.2.1 测评单元（L3-ADS1-06）

a) 测评指标

应提供访问控制功能，对登录的用户分配账户和权限；（本条款引用自 GB/T 22239.1-20XX 7.1.4.2 a））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否提供访问控制功能；

2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理；

3) 应测试不同岗位用户是否具有不同的权限。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.2.2 测评单元（L3-ADS1-07）

a) 测评指标

应重命名默认账户或修改默认口令；（本条款引用自 GB/T 22239.1-20XX 7.1.4.2 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否不存在默认账户或默认账户已重命名；

2) 应核查是否已修改默认账户的默认口令。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.2.3 测评单元（L3-ADS1-08）

a) 测评指标

应及时删除或停用多余的、过期的帐户，避免共享帐户的存在；（本条款引用自 GB/T 22239.1-20XX 7.1.4.2 c））

b) 测评对象

应用系统管理员和业务应用系统。

c) 测评实施

1) 应核查是否不存在多余账户或过期账户；

2) 应访谈了解是否不同用户采用不同登录账户登录应用系统。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.2.4 测评单元（L3-ADS1-09）

a) 测评指标

应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；（本条款引用自 GB/T 22239.1-20XX 7.1.4.2 d））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查不同岗位用户是否仅拥有其工作任务所需的最小权限；

2) 应核查业务岗位与管理岗位用户操作权限相互之间是否相互制约；

3) 应核查关键业务岗位用户操作权限相互之间是否相互制约；

4) 应核查关键管理岗位用户操作权限相互之间是否相互制约。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.2.5 测评单元（L3-ADS1-10）

a) 测评指标

应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；（本条款引用自 GB/T 22239.1-20XX 7.1.4.2 e））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否由管理用户负责配置访问控制策略；

2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则；

3) 应测试用户是否不存在可越权访问情形。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.2.6 测评单元（L3-ADS1-11）

a) 测评指标

访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；（本条款引用自 GB/T 22239.1-20XX 7.1.4.2 f））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级。

d) **单项判定**

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.2.7 **测评单元（L3-ADS1-12）**

a) **测评指标**

应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。（本条款引用自 GB/T 22239.1-20XX 7.1.4.2 g））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应核查是否依据安全策略对敏感信息资源设置了安全标记；

2) 应测试依据主体、客体安全标记控制主体对客体访问的强制访问控制功能。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.3 **安全审计**

8.1.4.3.1 **测评单元（L3-ADS1-13）**

a) **测评指标**

应提供并启用安全审计功能，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；（本条款引用自 GB/T 22239.1-20XX 7.1.4.3 a））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应核查是否提供并启用了安全审计功能；

2) 应核查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) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.3.2 **测评单元（L3-ADS1-14）**

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；（本条款引用自 GB/T 22239.1-20XX 7.1.4.3 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 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) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.3.3 测评单元（L3-ADS1-15）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.4.3 c））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制及备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.3.4 测评单元（L3-ADS1-16）

a) 测评指标

应对审计进程进行保护，防止未经授权的中断；（本条款引用自 GB/T 22239.1-20XX 7.1.4.3 d））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试应用系统，可试图通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.3.5 测评单元（L3-ADS1-17）

a) 测评指标

审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；（本条款引用自 GB/T 22239.1-20XX 7.1.4.3 e））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否统一使用系统范围内唯一确定的时钟，以确保审计分析的正确性。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.4 软件容错

8.1.4.4.1 测评单元（L3-ADS1-18）

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；（本条款引用自 GB/T 22239.1-20XX 7.1.4.4 a））

b) 测评对象

业务应用系统和系统设计文档等。

c) 测评实施

1) 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；

2) 应审核应用系统的源代码，在应用系统在人机接口或通信接口处是否对输入的数据进行有效性验证和处理；

3) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.4.2 测评单元（L3-ADS1-19）

a) 测评指标

在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；（本条款引用自 GB/T 22239.1-20XX 7.1.4.4 b））

b) 测评对象

开发文档和维护文档等。

c) 测评实施

1) 应核查应用系统设计文档和维护文档，应用系统有故障发生时是否能继续提供一部

分功能；

2) 应核查应用系统设计文档和维护文档，应用系统有故障发生后，是否能够实施必要的措施使系统恢复功能。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.4.3 **测评单元（L3-ADS1-20）**

a) **测评指标**

应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。（本条款引用自 GB/T 22239.1-20XX 7.1.4.4 c））

b) **测评对象**

系统设计文档和维护文档等。

c) **测评实施**

1) 应核查应用系统设计文档和维护文档，当故障发生时应用系统是否能自动保护当前所有状态；

2) 应核查应用系统设计文档和维护文档，应用系统发生故障后能够恢复故障时的状态。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.5 **资源控制**

8.1.4.5.1 **测评单元（L3-ADS1-21）**

a) **测评指标**

当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；（本条款引用自 GB/T 22239.1-20XX 7.1.4.5 a））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。

d) **单项判定**

如果 1） 为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.5.2 **测评单元（L3-ADS1-22）**

a) **测评指标**

应能够对系统的最大并发会话连接数进行限制；（本条款引用自 GB/T 22239.1-20XX 7.1.4.5 b））

b) 测评对象

业务应用系统或中间件等。

c) 测评实施

1) 应核查应用系统配置信息是否对最大并发会话连接数进行限制；

2) 应核查中间件配置信息是否对最大并发会话连接数进行限制。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.5.3 测评单元（L3-ADS1-23）

a) 测评指标

应能够对单个账户的多重并发会话进行限制；（本条款引用自 GB/T 22239.1-20XX 7.1.4.5 c））

b) 测评对象

业务应用系统。

c) 测评实施

应测试是否能够正确地限制单个账户的多重并发会话数。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.4.5.4 测评单元（L3-ADS1-24）

a) 测评指标

应能够对并发进程的每个进程占用的资源分配最大限额。（本条款引用自 GB/T 22239.1-20XX 7.1.4.5 d））

b) 测评对象

业务应用系统或中间件等。

c) 测评实施

1) 应核查是否对并发进程的每个进程占用的资源设置最大限额；

2) 应测试应用系统，验证并发进程的每个进程占用资源是否被限制在最大限额内。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.6 数据完整性

8.1.4.6.1 测评单元（L3-ADS1-25）

a) 测评指标

应采用校验码技术或加解密技术保证重要数据在传输过程中的完整性；（本条款引用自GB/T 22239.1-20XX 7.1.4.6 a））

b) 测评对象

系统设计文档和业务应用系统。

c) 测评实施

1) 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码技术或加解密技术保证完整性；

2) 应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.6.2 测评单元（L3-ADS1-26）

a) 测评指标

应采用校验码技术或加解密技术保证重要数据在存储过程中的完整性；（本条款引用自GB/T 22239.1-20XX 7.1.4.6 b））

b) 测评对象

系统设计文档、业务应用系统和数据加解密系统。

c) 测评实施

1) 应核查设计文档，是否采用校验码技术或加解密技术保证重要配置数据、重要业务数据在存储过程中的完整性；

2) 应核查数据加解密系统是否能够保证重要配置数据、重要业务数据在存储过程中的完整性；

3) 应测试在存储过程中对重要配置数据、重要业务数据进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.7 数据保密性

8.1.4.7.1 测评单元（L3-ADS1-27）

a) 测评指标

应采用加解密技术保证重要数据在传输过程中的保密性；（本条款引用自 GB/T 22239.1-20XX 7.1.4.7 a））

b) 测评对象

系统设计文档和业务应用系统。

c) 测评实施

1) 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加解密技术保证保密性；

2) 应通过嗅探等方式抓取传输过程中的数据包，查看重要管理数据、重要业务数据在传输过程中是否进行了加密处理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.7.2 测评单元（L3-ADS1-28）

a) 测评指标

应采用加解密技术保证重要数据在存储过程中的保密性；（本条款引用自 GB/T 22239.1-20XX 7.1.4.7 b））

b) 测评对象

系统设计文档、业务应用系统和数据加解密系统。

c) 测评实施

1) 应核查是否采用加解密技术保证重要配置数据、重要业务数据在存储过程中的保密性；

2) 应核查数据加解密系统是否能够保证重要配置数据、重要业务数据在存储过程中的保密性。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.8 数据备份恢复

8.1.4.8.1 测评单元（L3-ADS1-29）

a) 测评指标

应提供重要数据的本地数据备份与恢复功能；（本条款引用自 GB/T 22239.1-20XX 7.1.4.8 a））

b) 测评对象

配置数据和业务数据。

c) 测评实施

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，查看是否能够进行正常的数据恢复。

d) **单项判定**

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.8.2 **测评单元（L3-ADS1-30）**

a) **测评指标**

应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；（本条款引用自 GB/T 22239.1-20XX 7.1.4.8 b））

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实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.4.8.3 **测评单元（L3-ADS1-31）**

a) **测评指标**

应提供重要数据处理系统的热冗余，保证系统的高可用性；（本条款引用自 GB/T 22239.1-20XX 7.1.4.8 c））

b) **测评对象**

重要数据处理系统。

c) **测评实施**

应核查重要数据处理系统（包括边界交换机、边界防火墙、核心路由器、应用服务器和数据库服务器等）是否采用热冗余方式部署。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.1.4.9 **剩余信息保护**

8.1.4.9.1 **测评单元（L3-ADS1-32）**

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；（本条款引用自GB/T 22239.1-20XX 7.1.4.9 a））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查相关配置信息或访谈应用系统管理员，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) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.9.2 测评单元（L3-ADS1-33）

a) 测评指标

应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。（本条款引用自GB/T 22239.1-20XX 7.1.4.9 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查相关配置信息或访谈应用系统管理员，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.10 个人信息保护

8.1.4.10.1 测评单元（L3-ADS1-34）

a) 测评指标

应仅采集和保存业务必需的用户信息；（本条款引用自 GB/T 22239.1-20XX 7.1.4.10 a））

b) 测评对象

用户数据和业务应用系统。

c) 测评实施

1) 应核查采集的用户信息是否是业务应用必需的。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.1.4.10.2 测评单元（L3-ADS1-35）

a) 测评指标

应禁止未授权访问和使用用户信息。（本条款引用自 GB/T 22239.1-20XX 7.1.4.10 b））

b) 测评对象

用户数据和业务应用系统。

c) 测评实施

1) 应核查是否通过访问控制限制对用户信息的访问和使用。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2 安全管理测评

8.2.1 安全策略和管理制度

8.2.1.1 安全策略

8.2.1.1.1 测评单元（L3-PSS1-01）

a) 测评指标

应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。本条款引用自 GB/T 22239.1-20XX 7.2.1.1）

b) 测评对象

总体方针策略类文档。

c) 测评实施

应核查信息安全工作的总体方针和安全策略文件，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.1.2 管理制度

8.2.1.2.1 测评单元（L3-PSS1-02）

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。本条款引用自 GB/T 22239.1-20XX 7.2.1.2 a））

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，查看是否覆盖物理、网络、主机系统、数据、应用、建设和

运维等层面的管理内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.1.2.2 测评单元（L3-PSS1-03）

a) 测评指标

应对要求管理人员或操作人员执行的日常管理操作建立操作规程。本条款引用自 GB/T 22239.1-20XX 7.2.1.2 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.1.2.3 测评单元（L3-PSS1-04）

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信息安全管理制度体系。本条款引用自 GB/T 22239.1-20XX 7.2.1.2 c））

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是否形成体系化。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.1.2.4 测评单元(L1-PSS1-02）

a) 测评指标

应按照“谁主管谁负责，谁运营谁负责”的原则，建立工控系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。（新增）

b) 测评对象

安全管理制度类文档。

c) 测评实施

应核查工控系统安全管理制度，查看是否按照“谁主管谁负责，谁运营谁负责”的原则，制定信息安全工作的总体方针和安全策略，是否说明了机构安全工作的总体目标、范围、原则和安全框架等，是否将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.1.3 制定和发布

8.2.1.3.1 测评单元（L3-PSS1-05）

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。本条款引用自 GB/T 22239.1-20XX 7.2.1.3 a））

b) 测评对象

信息安全主管。

c) 测评实施

应访谈安全主管，询问是否由专门的部门或人员负责制定安全管理制度。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.1.3.2 测评单元（L3-PSS1-06）

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。本条款引用自 GB/T 22239.1-20XX 7.2.1.3 b））

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

1) 应核查制度制定和发布要求管理文档，查看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，查看是否通过正式、有效的方式收发（如正式发文、领导签署和单位盖章等），是否注明发布范围。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.1.4 评审和修订

8.2.1.4.1 测评单元（L3-PSS1-07）

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。本条款引用自 GB/T 22239.1-20XX 7.2.1.4））

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈安全主管，询问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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2 安全管理机构和人员

8.2.2.1 岗位设置

8.2.2.1.1 测评单元（L3-ORS1-01）

a) 测评指标

应成立指导和管理信息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委任或授权，并定期组织开展信息安全工作。（本条款引用自 GB/T 22239.1-20XX 7.2.2.1 a））

b) 测评对象

信息安全主管、管理制度类文档和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否成立了指导和管理信息安全工作的委员会或领导小组；

2) 应核查部门职责文档，查看信息安全工作的委员会或领导小组构成情况和相关职责；

3) 应核查信息安全工作的委员会或领导小组开展工作的会议纪要或相关记录。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.1.2 测评单元（L3-ORS1-02）

a) 测评指标

应设立信息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。（本条款引用自 GB/T 22239.1-20XX 7.2.2.1 b））

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否进行了信息安全管理职能部门的划分；

2) 应核查部门职责文档，查看是否明确信息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，查看岗位划分情况和岗位职责。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.1.3 测评单元（L3-ORS1-03）

a) 测评指标

应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。（本条款引用自 GB/T 22239.1-20XX 7.2.2.1 c））

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否进行了信息安全管理岗位的划分；

2) 应核查岗位职责文档，查看是否明确了各岗位职责。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.1.4 测评单元（L1-ORS1-02）

a) 测评指标

应明确由主管安全生产的领导作为工控系统安全防护的主要责任人。（新增）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否由主管安全生产的领导作为工控系统安全防护的主要责任人；

2) 应核查岗位职责文档，查看是明确由主管安全生产的领导作为工控系统安全防护的主要责任人。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.2 资金保障

8.2.2.2.1 测评单元（L1-ORS1-01）

a) 测评指标

应保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金。（新增）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，是否能够保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金；

2) 应核查安全管理制度中是否有保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金的内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.3 人员配备

8.2.2.3.1 测评单元（L3-ORS1-04）

a) 测评指标

应配备一定数量的系统管理员、网络管理员、安全管理员等。（本条款引用自 GB/T 22239.1-20XX 7.2.2.2 a））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认各岗位人员配备情况；

2) 应核查人员配备文档，查看各岗位人员配备情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.3.2 测评单元（L3-ORS1-05）

a) 测评指标

应配备专职安全管理员，不可兼任。（本条款引用自 GB/T 22239.1-20XX 7.2.2.2 b））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查人员配备文档，查看是否配备了专职安全管理员。

d) **单项判定**

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.4 授权和审批

8.2.2.4.1 测评单元（L4-ORS1-06）

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。（本条款引用自 GB/T 22239.1-20XX 7.2.2.3 a））

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**

1) 应核查部门职责文档，查看各部门的职责和授权范围；

2) 应核查岗位职责文档，查看各岗位的职责和授权范围；

3) 应核查审批记录，查看审批事项、审批部门和批准人等内容是否与相关制度一致。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.4.2 测评单元（L4-ORS1-07）

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。本条款引用自 GB/T 22239.1-20XX 7.2.2.3 b））

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**

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，查看相关操作过程中是否建立了逐级审批程序；

2) 应核查审批记录、操作记录，查看审批结果是否与相关制度一致。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.4.3 测评单元（L4-ORS1-08）

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。本条

款引用自 GB/T 22239.1-20XX 7.2.2.3 c））

b) 测评对象

信息安全主管。

c) 测评实施

1) 应访谈信息安全主管，询问是否对各类审批事项进行更新。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.5 沟通和合作

8.2.2.5.1 测评单元（L3-ORS1-09）

a) 测评指标

应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题。本条款引用自 GB/T 22239.1-20XX 7.2.2.4 a））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否建立了各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通机制；

2) 应核查会议记录，查看各类管理人员之间、组织内部机构之间以及信息安全职能部门内部是否开展了合作与沟通。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.5.2 测评单元（L3-ORS1-10）

a) 测评指标

应加强与兄弟单位、公安机关、各类供应商、业界专家及安全组织的合作与沟通。本条款引用自 GB/T 22239.1-20XX 7.2.2.4 b））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否建立了与兄弟单位、公安机关、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，查看与兄弟单位、公安机关、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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.5.3 **测评单元（L3-ORS1-11）**

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。本条款引用自 GB/T 22239.1-20XX 7.2.2.4 c））

b) **测评对象**

记录表单类文档。

c) **测评实施**

1) 应核查外联单位联系列表，查看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) **单项判定**

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.6 **审核和核查**

8.2.2.6.1 **测评单元（L3-ORS1-12）**

a) **测评指标**

应定期进行常规安全核查，核查内容包括系统日常运行、系统漏洞和数据备份等情况。本条款引用自 GB/T 22239.1-20XX 7.2.2.5 a））

b) **测评对象**

信息安全主管和记录表单类文档。

c) **测评实施**

1) 应访谈信息安全主管，确认是否定期进行了常规安全核查；

2) 应核查常规安全核查记录，查看记录内容是否包括了系统日常运行、系统漏洞和数据备份等情况。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.6.2 **测评单元（L3-ORS1-13）**

a) **测评指标**

应定期进行全面安全核查，核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。本条款引用自 GB/T 22239.1-20XX 7.2.2.5 b））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否定期进行了全面安全核查；

2) 应核查全面安全核查记录，查看记录内容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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.6.3 测评单元（L3-ORS1-14）

a) 测评指标

应制定安全核查表格实施安全核查，汇总安全核查数据，形成安全核查报告，并对安全核查结果进行通报。本条款引用自 GB/T 22239.1-20XX 7.2.2.5 c））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查安全核查表格、安全核查记录、安全核查报告、安全核查结果通报记录，以此确认是否开展了安全核查，记录了核查数据，形成了核查报告，并对安全核查结果进行了通报。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.7 人员录用

8.2.2.7.1 测评单元（L3-ORS1-15）

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；本条款引用自（GB/T 22239.1-20XX 8.2.2.6 a））

b) 测评对象

信息安全主管。

c) 测评实施

应访谈安全主管，询问是否由专门的部门或人员负责人员的录用工作。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.2.7.2 测评单元（L3-ORS1-16）

a) 测评指标

应被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；本条款引用自（GB/T 22239.1-20XX 8.2.2.6 b））

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

1) 应核查人员安全管理文档，查看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、背景、专业资格和资质等进行审查的相关文档或记录，查看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，查看是否记录考核内容和考核结果等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.7.3 测评单元（L3-ORS1-17）

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。本条款引用自（GB/T 22239.1-20XX 8.2.2.6 c））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查保密协议，查看是否有保密范围、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，查看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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.8 人员离岗

8.2.2.8.1 测评单元（L3-ORS1-18）

a) 测评指标

应及时终止离岗员工的所有访问权限，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；本条款引用自（GB/T 22239.1-20XX 8.2.2.7 a））

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交还身份证件、设备等的登记记录。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.2.8.2 测评单元（L3-ORS1-19）

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。本条款引用自（GB/T 22239.1-20XX 8.2.2.7 b））

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

1) 应核查人员离岗的管理文档，查看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，查看是否有调离人员的签字。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.9 安全意识教育和培训

8.2.2.9.1 测评单元（L3-ORS1-20）

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；本条款引用自（GB/T 22239.1-20XX 8.2.2.8 a））

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查信息安全教育及技能培训文档，查看是否明确培训周期、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，查看是否包含具体的安全责任和惩戒措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.9.2 测评单元（L3-ORS1-21）

a) 测评指标

应针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。本条款引用自（GB/T 22239.1-20XX 8.2.2.8 b））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查安全教育和培训计划文档，查看是否具有不同岗位的培训计划；查看培训内容是否包含信息安全基础知识、岗位操作规程等；

2) 应核查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.10 外部人员访问管理

8.2.2.10.1 测评单元（L3-ORS1-22）

a) 测评指标

应确保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；本条款引用自（GB/T 22239.1-20XX 8.2.2.9 a））

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

1) 应核查外部人员访问管理文档，查看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，查看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，查看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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.10.2 测评单元（L3-ORS1-23）

a) 测评指标

应确保在外部人员接入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；本条款引用自（GB/T 22239.1-20XX 8.2.2.9 b））

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

1) 应核查外部人员访问管理文档，查看是否明确外部人员接入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，查看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，查看是否记录了外部人员访问的权限、时限、账户等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.10.3 测评单元（L3-ORS1-24）

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；本条款引用自（GB/T 22239.1-20XX 8.2.2.9 c））

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

1) 应核查外部人员访问管理文档，查看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，查看是否记录了访问权限清除时间。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.2.10.4 测评单元（L3-ORS1-25）

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。本条款引用自（GB/T 22239.1-20XX 8.2.2.9 d））

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3 安全建设管理

8.2.3.1 定级和备案

8.2.3.1.1 测评单元（L3-CMS1-01）

a) 测评指标

应以书面的形式说明保护对象的边界、安全保护等级及确定等级的方法和理由；（本条款引用自 GB/T 22239.1-20XX 7.2.3.1 a））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查定级文档，查看文档是否明确等级保护对象的边界和等级保护对象的安全保护等级，是否说明定级的方法和理由。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.1.2 测评单元（L3-CMS1-02）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.1 b））

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.1.3 测评单元（L3-CMS1-03）

a) 测评指标

应确保定级结果经过相关部门的批准；（本条款引用自 GB/T 22239.1-20XX 7.2.3.1 c））

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，查看是否有上级主管部门或本单位相关部门的审批意见。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.1.4 测评单元（L3-CMS1-04）

a) 测评指标

应将备案材料报主管部门和相应公安机关备案。（本条款引用自 GB/T 22239.1-20XX 7.2.3.1 d））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.2 安全方案设计

8.2.3.2.1 测评单元（L3-CMS1-05）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.2 a））

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，查看是否根据安全等级选择安全措施，是否根据安全需求调整安全措施。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.2.2 测评单元（L3-CMS1-06）

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，并形成配套文件；（本条款引用自 GB/T 22239.1-20XX 7.2.3.2 b））

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。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.2.3 测评单元（L3-CMS1-07）

a) 测评指标

应组织相关部门和有关安全专家对总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。（本条款引用自 GB/T 22239.1-20XX 7.2.3.2 c））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查配套文件的论证评审记录或文档，查看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论证意见；

2) 应核查是否有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.3.3 产品采购和使用

8.2.3.3.1 测评单元（L3-CMS1-08）

a) 测评指标

应确保信息安全产品采购和使用符合国家的有关规定；（本条款引用自 GB/T 22239.1-20XX 7.2.3.3 a））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.3.2 测评单元（L3-CMS1-09）

a) 测评指标

应确保密码产品采购和使用符合国家密码主管部门的要求；（本条款引用自 GB/T 22239.1-20XX 7.2.3.3 b））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.3.3 测评单元（L3-CMS1-10）

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。（本条款引用自 GB/T 22239.1-20XX 7.2.3.3 c））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.3.4 测评单元（L1-CMS1-03）

a) 测评指标

工控控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用。（新增）

b) 测评对象

建设负责人、检测报告类文档。

c) 测评实施

1) 应访谈建设负责人，询问系统使用的工控控制系统重要设备及专用信息安全产品是否通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测；

2) 应核查工控控制系统通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测的检测报告。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.3.4 自行软件开发

8.2.3.4.1 测评单元（L3-CMS1-11）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.4 a））

b) 测评对象

建设负责人。

c) 测评实施

1) 应访谈建设负责人，询问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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.3.4.2 测评单元（L3-CMS1-12）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.4 b））

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，查看文件是否明确软件设计、开发、测试和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和审批。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.4.3 测评单元（L3-CMS1-13）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.4 c））

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，查看规范中是否明确代码安全编写规则。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.4.4 测评单元（L3-CMS1-14）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.4 d））

b) 测评对象

软件开发类文档。

c) 测评实施

应核查是否具有软件开发文档和使用指南。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.4.5 测评单元（L3-CMS1-15）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.4 e））

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，明确软件存在的安全问题及可能存在的恶意代码。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.4.6 测评单元（L3-CMS1-16）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.4 f））

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，查看是否有批准人的签字。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.4.7 测评单元（L3-CMS1-17）

a) 测评指标

应确保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。（本条款引用自 GB/T 22239.1-20XX 7.2.3.4 g））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问开发人员是否为专职，是否对开发人员活动进行控制等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.5 外包软件开发

8.2.3.5.1 测评单元（L3-CMS1-18）

a) 测评指标

应在软件交付前检测软件质量和其中可能存在的恶意代码；（本条款引用自 GB/T 22239.1-20XX 7.2.3.5 a））

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软件质量和恶意代码检测报告。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.5.2 测评单元（L3-CMS1-19）

a) 测评指标

应要求开发单位提供软件设计文档和使用指南；（本条款引用自 GB/T 22239.1-20XX 7.2.3.5 b））

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

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.5.3 测评单元（L3-CMS1-20）

a) 测评指标

应要求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。（本条款引用自 GB/T 22239.1-20XX 7.2.3.5 c））

b) 测评对象

建设负责人和记录表单类文档。

c) 测评实施

1) 应访谈建设负责人，询问是否具有软件源代码；

2) 应核查软件测试报告，查看是否明确审查了软件可能存在的后门和隐蔽信道并记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.3.5.4 测评单元（L2-CMS1-13）

a) 测评指标

应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。（新增）

b) 测评对象

外包合同。

c) 测评实施

应核查外包开发合同中是否包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.6 工程实施

8.2.3.6.1 测评单元（L3-CMS1-21）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.6 a））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.6.2 测评单元（L3-CMS1-22）

a) 测评指标

应制定工程实施方案控制安全工程实施过程；（本条款引用自 GB/T 22239.1-20XX 7.2.3.6 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查工程实施方案，查看其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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.6.3 测评单元（L3-CMS1-23）

a) 测评指标

应通过第三方工程监理控制项目的实施过程。（本条款引用自 GB/T 22239.1-20XX 7.2.3.6 c））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查第三方工程监理报告，查看是否明确了工程进展、时间计划、控制措施等方面内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.7 测试验收

8.2.3.7.1 测评单元（L3-CMS1-24）

a) 测评指标

在制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；（本条款引用自 GB/T 22239.1-20XX 7.2.3.7 a））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查是否具有工程测试验收方案，查看其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) 应核查是否具有测试验收报告，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.3.7.2 测评单元（L3-CMS1-25）

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。（本条款引用自 GB/T 22239.1-20XX 7.2.3.7 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.8 系统交付

8.2.3.8.1 测评单元（L3-CMS1-26）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.8 a））

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清单，查看交付清单是否说明交付的各类设备、软件、文档等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.8.2 测评单元（L3-CMS1-27）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.8 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.8.3 测评单元（L3-CMS1-28）

a) 测评指标

应确保提供建设过程中的文档和指导用户进行运行维护的文档。（本条款引用自 GB/T 22239.1-20XX 7.2.3.8 c））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查交付文档，查看是否有指导用户进行运维的文档等，提交的文档是否符合管理规定的要求。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.9 等级测评

8.2.3.9.1 测评单元（L3-CMS1-29）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.9 a））

b) 测评对象

运维负责人和记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，本次测评是否为首次，若非首次，以往进行过几次测评，是否根据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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.3.9.2 测评单元（L3-CMS1-30）

a) 测评指标

应在发生重大变更或系统级别发生变化时进行等级测评；（本条款引用自 GB/T 22239.1-20XX 7.2.3.9 b））

b) 测评对象

运维负责人和记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，系统是否过重大变更或级别发生过变化，若有，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.3.9.3 测评单元（L3-CMS1-31）

a) 测评指标

应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。（本条款引用自 GB/T 22239.1-20XX 7.2.3.9 c））

b) 测评对象

运维负责人。

c) 测评实施

应访谈运维负责人，以往等级测评的测评单位是否具有国家相关等级测评资质的单位。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.10 服务供应商管理

8.2.3.10.1 测评单元（L3-CMS1-32）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.3.10 a））

b) 测评对象

运维负责人。

c) 测评实施

应访谈建设负责人，询问等级保护对象选择的安全服务商有哪些，是否符合国家有关规定。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.10.2 测评单元（L3-CMS1-33）

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信息安全相关义务；（本条款引用自 GB/T 22239.1-20XX 7.2.3.10 b））

b) 测评对象

记录表单类文档

c) 测评实施

应核查是否具有与安全服务商签订的服务合同或安全责任合同书，查看是否明确了后期的技术支持和服务承诺等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.3.10.3 测评单元（L3-CMS1-34）

a) 测评指标

应定期监视、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。（本条款引用自 GB/T 22239.1-20XX 7.2.3.10 c））

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

1) 应核查是否具有安全服务商定期提交的安全服务报告；

2) 应核查是否定期审核评价安全服务供应商所提供的服务，是否具有服务审核报告；

3) 应核查是否具有安全服务商评价审核管理制度，明确针对服务商的评价指标和考核内容等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4 系统运维管理

8.2.4.1 环境管理

8.2.4.1.1 测评单元（L3-MMS1-01）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.1 a））

b) 测评对象

物理安全负责人、记录表单类文档。

c) 测评实施

1) 应访谈物理安全负责人，询问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，由何部门/何人负责；

2) 应核查部门或人员岗位职责文档，查看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，查看是否记录来访人员、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，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.1.2 测评单元（L3-MMS1-02）

a) 测评指标

应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；（本条款引用自 GB/T 22239.1-20XX 7.2.4.1 b））

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

1) 应核查机房安全管理制度，查看制度内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容；

2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录，是否与制度相符。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

8.2.4.1.3 测评单元（L3-MMS1-03）

a) 测评指标

应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等。（本条款引用自 GB/T 22239.1-20XX 7.2.4.1 c））

b) 测评对象

管理制度类文档、办公环境。

c) 测评实施

1) 应核查机房安全管理制度，查看是否明确来访人员的接待区域；

2) 应核查办公桌面上是否包含敏感信息的纸档文件、移动介质等。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.1.4 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应明确专人负责，并定期进行核查、维护和清洁工作。

b) 测评对象

室外控制设备。

c) 测评实施

1) 应询问管理员室外控制设备是否有专人负责；

2) 应核查相关记录是否定期对室外控制设备进行核查、维护和清洁工作的记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.2 资产管理

8.2.4.2.1 测评单元（L3-MMS1-04）

a) 测评指标

应编制并保存与等级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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.2 a））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查资产清单，查看其内容是否覆盖资产责任部门、重要程度和所处位置等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.2.2 测评单元（L3-MMS1-05）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.2 b））

b) 测评对象

资产管理员单、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问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，查看其是否具有相应标识，标识方法是否符合 2）相关要求。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.2.3 测评单元（L3-MMS1-06）

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。（本条款引用自 GB/T 22239.1-20XX 7.2.4.2 c））

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查信息分类文档，查看其内容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) 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。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.3 介质管理

8.2.4.3.1 测评单元（L3-MMS1-07）

a) 测评指标

应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，

并根据存档介质的目录清单定期盘点；（本条款引用自 GB/T 22239.1-20XX 7.2.4.3 a））

b) 测评对象

资产管理员、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理；

2) 应核查介质使用管理记录，查看其是否记录介质归档和使用等情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.3.2 测评单元（L3-MMS1-08）

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。（本条款引用自 GB/T 22239.1-20XX 7.2.4.3 b））

b) 测评对象

资产管理员、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问介质在物理传输过程中的人员、打包交付等情况是否进行控制；

2) 应核查是否有对介质的归档和查询等的登记记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.3.3 测评单元（L1-MMS1-03）

a) 测评指标

应建立隔离区域移动存储介质安全管理制度，对移动存储介质的使用进行限制。（新增）

b) 测评对象

资产管理员、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问是否建立隔离区域移动存储介质安全管理制度，是否对移动存储介质的使用进行限制；

2) 应查看是否有隔离区域移动存储介质安全管理制度是否有限制移动存储介质使用的内容；

3) 应核查隔离区与移动介质使用管理记录，查看其是否记录隔离区域移动存储介质归档和使用等情况。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.4 设备维护管理

8.2.4.4.1 测评单元（L3-MMS1-09）

a) 测评指标

应对等级保护对象相关的各种设备（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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.4 a））

b) 测评对象

设备管理员、管理制度类文档。

c) 测评实施

1) 应访谈设备管理员，询问是否对各类设施、设备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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.4.2 测评单元（L3-MMS1-10）

a) 测评指标

应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；（本条款引用自 GB/T 22239.1-20XX 7.2.4.4 b））

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

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

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

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.4.3 测评单元（L3-MMS1-11）

a) 测评指标

应确保信息处理设备必须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必须加密；（本条款引用自 GB/T 22239.1-20XX 7.2.4.4 c））

b) 测评对象

设备管理员、记录表单类文档。

c) 测评实施

1) 应访谈设备管理员，询问对带离机房的设备是否经过审批，由何人审批；

2) 应核查是否具有设备带离机房或办公地点的审批记录；

3) 应访谈设备管理员，询问含有重要数据的存储介质带出工作环境是否有加密措施，采取什么加密措施。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.4.4 测评单元（L3-MMS1-12）

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，确保该设备上的敏感数据和授权软件无法被恢复重用。（本条款引用自 GB/T 22239.1-20XX 7.2.4.4 d））

b) 测评对象

设备管理员。

c) 测评实施

应访谈设备管理员，询问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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.5 漏洞和风险管理

8.2.4.5.1 测评单元（L3-MMS1-13）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.5 a））

b) 测评对象

安全管理员、记录表单类文档。

c) 测评实施

1) 应访谈安全管理员，询问是否定期进行漏洞扫描，对发现的漏洞是否及时进行修补或评估可能的影响后进行修补；

2) 应核查漏洞扫描报告，查看内容是否描述了存在的漏洞、严重级别、原因分析和改

进意见等方面。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.5.2 **测评单元（L3-MMS1-14）**

a) **测评指标**

应按照国家标准定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。（本条款引用自 GB/T 22239.1-20XX 7.2.4.5 b））

b) **测评对象**

安全管理员、记录表单类文档。

c) **测评实施**

1) 应访谈安全管理员，询问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) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.6 **网络和系统安全管理**

8.2.4.6.1 **测评单元（L3-MMS1-15）**

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 a））

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，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）；

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.6.2 **测评单元（L3-MMS1-16）**

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；

（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 b））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问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，查看是否对申请账户、建立账户、删除账户等进行控制。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.6.3 测评单元（L3-MMS1-17）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 c））

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，查看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、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.6.4 测评单元（L3-MMS1-18）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 d））

b) 测评对象

操作规程类文档。

c) 测评实施

1) 应核查是否针对网络和系统制定了重要设备（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，查看是否明确操作步骤、维护记录、参

数配置等内容。

d) 单项判定

如果 1)）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.6.5 测评单元（L3-MMS1-19）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 e)）

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.6.6 测评单元（L3-MMS1-20）

a) 测评指标

应严格控制变更性运维，经过审批后才可改变系统连接、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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 f)）

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查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；

2) 应核查针对变更运维的操作过程记录；

3) 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。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.6.7 测评单元（L3-MMS1-21）

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系统进行操作，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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 g））

b) 测评对象

系统管理员、记录表单类文档。

c) 测评实施

1) 应核查是否具有运维工具接入系统的审批记录；

2) 应核查针对使用运维工具的操作过程记录，审计日志是否可以更改，并核查审计日志记录；

3) 应访谈系统管理员，询问使用运维工具结束后是否删除工具中的敏感数据。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.6.8 测评单元（L3-MMS1-22）

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。（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 h））

b) 测评对象

系统管理员、记录表单类文档。

c) 测评实施

1) 应访谈系统管理员，询问日常运维过程中是否存在远程运维；

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操作过程记录，查看审计日志是否可以更改；

4) 应访谈系统管理员远程运维结束后是否立即关闭了接口或通道。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.6.9 测评单元（L3-MMS1-23）

a) 测评指标

应保证所有与外部的连接均得到授权和批准， 应定期核查违反规定无线上网及其他违反网络安全策略的行为。（本条款引用自 GB/T 22239.1-20XX 7.2.4.6 i））

b) 测评对象

网络管理员、记录表单类文档。

c) 测评实施

1) 应访谈网络管理员，询问外联种类（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，由何人/何部门批准；

2) 应核查是否具有外联授权的记录文件；

3) 应访谈网络管理员，是否定期核查违规联网行为。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.7 **恶意代码防范管理**

8.2.4.7.1 **测评单元（L3-MMS1-24）**

a) **测评指标**

应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码核查等；（本条款引用自 GB/T 22239.1-20XX 7.2.4.7 a））

b) **测评对象**

运维负责人。

c) **测评实施**

应访谈运维负责人，询问是否采取告知方式提升员工的防病毒意识。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.7.2 **测评单元（L3-MMS1-25）**

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.7 b））

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，查看是否明确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) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.7.3 **测评单元（L3-MMS1-26）**

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。（本条款引用自 GB/T

22239.1-20XX 7.2.4.7 c））

b) 测评对象

安全管理员、记录表单类文档。

c) 测评实施

1) 应访谈安全管理员，询问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。

3) 应定期采用技术手段测试验证恶意代码防范技术措施的有效性。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.7.4 测评单元（L1-MMS1-09）

a) 测评指标

在更新恶意代码库、木马库以及 IDS 规则库前，应首先在测试环境中测试通过，对隔离区域恶意代码更新应有专人负责，更新操作应离线进行，并保存更新记录。（新增）

b) 测评对象

安全管理员、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈系统管理员，询问是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行，是否保存更新记录。

2) 应核查恶意代码防范管理制度，查看是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行等内容。

3) 应核查更新记录，查看是否有更新前在测试环境中测试通过的记录，隔离区域恶意代码更新是否为专人负责，更新操作是否离线的记录。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.8 配置管理

8.2.4.8.1 测评单元（L3-MMS1-27）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.8 a））

b) 测评对象

系统管理员。

c) 测评实施

3) 应访谈系统管理员，询问是否对基本配置信息进行记录和保存。

4) 查看记录表单类文档是否对基本配置信息进行记录

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.8.2 测评单元（L3-MMS1-28）

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。（本条款引用自 GB/T 22239.1-20XX 7.2.4.8 b））

b) 测评对象

系统管理员、记录表单类文档。

c) 测评实施

1) 应访谈配置管理人员，询问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，查看是否具有相应的申报审批程序。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.9 密码管理

8.2.4.9.1 测评单元（L3-MMS1-29）

a) 测评指标

应使用符合国家密码管理规定的密码技术和产品；（本条款引用自 GB/T 22239.1-20XX 7.2.4.9 a））

b) 测评对象

安全管理员。

c) 测评实施

应核查该是否获得有效的国家密码管理规定的检测报告或密码产品型号证书。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.10 变更管理

8.2.4.10.1 测评单元（L3-MMS1-31）

a) 测评指标

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；（本条款引用自 GB/T 22239.1-20XX 7.2.4.10 a））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应抽查变更方案，查看其是否包含变更类型、变更原因、变更过程、变更前评估等内容；

2) 应核查是否具有变更方案评审记录和变更过程记录文档。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.10.2 测评单元（L3-MMS1-32）

a) 测评指标

应建立变更的申报和审批控制程序，依据程序控制系统所有的变更，记录变更实施过程；（本条款引用自 GB/T 22239.1-20XX 7.2.4.10 b））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查变更控制的申报、审批程序，查看其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容；

2) 应核查变更实施过程的记录文档；

3) 应核查针对发生变更的事件进行影响分析。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.10.3 测评单元（L3-MMS1-33）

a) 测评指标

应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。（本条款引用自 GB/T 22239.1-20XX 7.2.4.10 c））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问变更失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练；

2) 应核查是否具有变更恢复演练记录；

3) 应核查变更失败恢复程序，查看其是否规定变更失败后的恢复流程。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.11 备份与恢复管理

8.2.4.11.1 测评单元（L3-MMS1-34）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.11 a））

b) 测评对象

系统管理员、数据库管理员和网络管理员、记录表单类文档。

c) 测评实施

1) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.11.2 测评单元（L3-MMS1-35）

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；（本条款引用自 GB/T 22239.1-20XX 7.2.4.11 b））

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，查看是否明确备份方式、频度、介质、保存期等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.11.3 测评单元（L3-MMS1-36）

a) 测评指标

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。（本条款引用自 GB/T 22239.1-20XX 7.2.4.11 c））

b) 测评对象

管理制度类文档。

c) 测评实施

应核查备份和恢复的策略，查看内容是否明确备份策略和恢复策略文档规范了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.12 安全事件处置

8.2.4.12.1 测评单元（L3-MMS1-37）

a) 测评指标

应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；（本条款引用自 GB/T 22239.1-20XX 7.2.4.12 a））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应进行及时报告；

2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.12.2 测评单元（L3-MMS1-38）

a) 测评指标

应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等；（本条款引用自 GB/T 22239.1-20XX 7.2.4.12 c））

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管理制度，查看内容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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.12.3 测评单元（L3-MMS1-39）

a) 测评指标

应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；（本条款引用自 GB/T 22239.1-20XX 7.2.4.12 d））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查安全事件报告和响应处置记录，查看其是否记录引发安全事件的系统弱点、不同安全事件发生的原因、处置过程、经验教训总结、补救措施等内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.12.4 测评单元（L3-MMS1-40）

a) 测评指标

对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。（本条款引用自 GB/T 22239.1-20XX 7.2.4.12 e））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问其不同安全事件的报告流程；

2) 应核查安全事件报告和处理程序文档，查看其是否根据不同安全事件制定不同的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.12.5 测评单元（L1-MMS1-13）

a) 测评指标

应建立工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件。（新

增）

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

1) 应核查安全事件报告和处置管理制度，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容；

2) 应核查安全事件报告和处理程序文档，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.13 应急预案管理

8.2.4.13.1 测评单元（L3-MMS1-41）

a) 测评指标

应规定统一的应急预案框架，并在此框架下制定不同事件的应急预案，包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；（本条款引用自 GB/T 22239.1-20XX 7.2.4.13 a））

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查应急预案框架，查看是否覆盖启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等方面；

2) 应核查是否具有根据应急预案框架制定不同事件的应急预案（如针对机房、系统、网络等各个层面）。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.13.2 测评单元（L3-MMS1-42）

a) 测评指标

应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；（本条款引用自 GB/T 22239.1-20XX 7.2.4.13 b））

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查应急预案框架或相关文档，查看是否明确应急小组、相关设备及资金保障。

d) 单项判定

如果 1）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.13.3 测评单元（L3-MMS1-43）

a) 测评指标

应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；（本条款引用自 GB/T 22239.1-20XX 7.2.4.13 c））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，是否定期对相关人员进行应急预案培训和演练；

2) 应核查应急预案培训记录，查看是否明确培训对象、培训内容、培训结果等；

3) 应核查应急预案演练记录，查看是否记录演练时间、主要操作内容、演练结果等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.13.4 测评单元（L3-MMS1-44）

a) 测评指标

应定期对原有的应急预案重新评估，修订完善。（本条款引用自 GB/T 22239.1-20XX 7.2.4.13 d））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查应急预案修订记录，查看是否明确修订时间、修订内容等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.14 外包运维管理

8.2.4.14.1 测评单元（L3-MMS1-45）

a) 测评指标

应确保外包运维服务商的选择符合国家的有关规定；（本条款引用自 GB/T 22239.1-20XX 7.2.4.14 a））

b) 测评对象

运维负责人。

c) 测评实施

1) 应访谈运维负责人，询问对等级保护对象进行运维是否有外包运维服务情况；

2) 应访谈运维负责人，询问对等级保护对象进行外包运维服务的服务单位是否符合国家有关规定。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

8.2.4.14.2 测评单元（L3-MMS1-46）

a) 测评指标

应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；（本条款引用自 GB/T 22239.1-20XX 7.2.4.14 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查外包运维服务协议，查看协议内容是否明确约定外包运维的范围和工作内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.14.3 测评单元（L3-MMS1-47）

a) 测评指标

应确保选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；（本条款引用自 GB/T 22239.1-20XX 7.2.4.14 c））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查与外包运维服务商签订的协议中是否明确其具有等级保护要求的服务能力要求。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

8.2.4.14.4 测评单元（L3-MMS1-48）

a) 测评指标

应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息

的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。（本条款引用自 GB/T 22239.1-20XX 7.2.4.14 d））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查外包运维服务协议，查看否明确安全要求，如是否包含可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9 第四级单项测评

9.1 安全技术测评

9.1.1 物理和环境安全

9.1.1.1 物理位置的选择

9.1.1.1.1 测评单元（L4-PES1-01）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.1.1 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 应核查是否存在雨水渗漏；

3) 应核查门窗是否因风导致的尘土严重；

4) 应核查屋顶、墙体、门窗和地面等是否破损开裂。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.1.2 测评单元（L4-PES1-02）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.1.1 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房是否不位于所在建筑物的顶层或地下室；

2) 如果机房位于所在建筑物的顶层或地下室，应核查机房是否采取了防水和防潮措施。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.2 物理访问控制

9.1.1.2.1 测评单元（L4-PES1-03）

a) 测评指标

机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；（本条款引用自 GB/T 22239.1-20XX 8.1.1.2 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查出入口是否配置电子门禁系统；

2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.2.2 测评单元（L4-PES1-04）

a) 测评指标

重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。（本条款引用自 GB/T 22239.1-20XX 8.1.1.2 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查重要区域出入口是否配置第二道电子门禁系统；

2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.3 防盗窃和防破坏

9.1.1.3.1 测评单元（L4-PES1-05）

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记；（本条款引用自 GB/T 22239.1-20XX 8.1.1.3 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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记。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.3.2 测评单元（L4-PES1-06）

a) 测评指标

应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；（本条款引用自 GB/T 22239.1-20XX 8.1.1.3 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房内通信线缆是否铺设在隐蔽处或桥架中。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.3.3 测评单元（L4-PES1-07）

a) 测评指标

应设置机房防盗报警系统或有专人值守的视频监控系统。（本条款引用自 GB/T 22239.1-20XX 8.1.1.3 c））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否配置防盗报警系统或有专人值守的视频监控系统；

2) 应核查防盗报警系统或视频监控系统是否启用。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.4 防雷击

9.1.1.4.1 测评单元（L4-PES1-08）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.1.4 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.4.2 测评单元（L4-PES1-09）

a) 测评指标

应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。（本条款引用自 GB/T 22239.1-20XX 8.1.1.4 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否设置防感应雷措施；

2) 应核查防雷装置是否通过验收或国家有关部门的技术检测。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.5 防火

9.1.1.5.1 测评单元（L4-PES1-10）

a) 测评指标

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；（（本条款引用自 GB/T 22239.1-20XX 8.1.1.5 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.5.2 测评单元（L4-PES1-11）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.1.5 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.5.3 测评单元（L4-PES1-12）

a) 测评指标

应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。（本条款引用自 GB/T 22239.1-20XX 8.1.1.5 c））

b) 测评对象

机房管理员和机房。

c) 测评实施

1) 应访谈机房管理员是否进行了区域划分；

2) 应核查各区域间是否采取了防火措施进行隔离。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.6 防水和防潮

9.1.1.6.1 测评单元（L4-PES1-13）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.1.6 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房的窗户、屋顶和墙壁是否采取了防雨水渗透的措施。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.6.2 测评单元（L4-PES1-14）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.1.6 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.6.3 测评单元（L4-PES1-15）

a) 测评指标

应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。（本条款引用自 GB/T 22239.1-20XX 8.1.1.6 c））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否安装了对水敏感的检测装置；

2) 应核查防水检测和报警装置是否启用。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.7 防静电

9.1.1.7.1 测评单元（L4-PES1-16）

a) 测评指标

应安装防静电地板并采用必要的接地防静电措施；（本条款引用自 GB/T 22239.1-20XX 8.1.1.7 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否安装了防静电地板；

2) 应核查机房内是否采用了接地防静电措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.7.2 测评单元（L4-PES1-17）

a) 测评指标

应采用措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。（本条款引用自 GB/T 22239.1-20XX 8.1.1.7 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房内是否配备了防静电设备。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.8 温湿度控制

9.1.1.8.1 测评单元（L4-PES1-18）

a) 测评指标

机房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。（本条款引用自 GB/T 22239.1-20XX 8.1.1.8）

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.9 电力供应

9.1.1.9.1 测评单元（L4-PES1-19）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.1.9 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

应核查机房供电线路上是否配置了稳压器和过电压防护设备。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.9.2 测评单元（L4-PES1-20）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.1.9 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查是否配备 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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.9.3 测评单元（L4-PES1-21）

a) 测评指标

应设置冗余或并行的电力电缆线路为计算机系统供电；（本条款引用自 GB/T 22239.1-20XX 8.1.1.9 c））

b) 测评对象

机房管理员和机房。

c) 测评实施

1) 应访谈机房管理员确认机房供电是否来自两个不同的变电站；

2) 应核查机房内是否设置了冗余或并行的电力电缆线路为计算机系统供电。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.9.4 测评单元（L4-PES1-22）

a) 测评指标

应建立应急供电设施。（本条款引用自 GB/T 22239.1-20XX 8.1.1.9 d））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查是否配置了应急供电设施；

2) 应核查应急供电设施是否可用。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.10 电磁防护

9.1.1.10.1 测评单元（L4-PES1-23）

a) 测评指标

电源线和通信线缆应隔离铺设，避免互相干扰；（本条款引用自 GB/T 22239.1-20XX 8.1.1.10 a））

b) 测评对象

数据中心机房、场站机房、现地机房。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.10.2 测评单元（L4-PES1-24）

a) 测评指标

应对关键设备或关键区域实施电磁屏蔽。（本条款引用自 GB/T 22239.1-20XX 8.1.1.10 b））

b) 测评对象

数据中心机房、场站机房、现地机房。

c) 测评实施

1) 应核查机房内是否划分了电磁屏蔽关键区域；

2) 应核查机房内是否为关键设备配备了电磁屏蔽装置。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.11 室外控制设备防护

9.1.1.11.1 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备是否放置于采用铁板或其他防火尽缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备是否安装在金属或其他尽缘板上(非木质板)，并紧固于箱体或装置中。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.1.11.2 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应远离极端天气环境，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行。

b) 测评对象

室外控制设备。

c) 测评实施

1) 应核查室外控制设备是否远离极端天气环境；

2) 应核查是否有极端天气时的检修维护记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.1.11.3 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备放置应远离强电磁干扰和热源。

b) 测评对象

室外控制设备。

c) 测评实施

应核查室外控制设备放置是否远离强电磁干扰和热源。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.2 网络和通信安全

9.1.2.1 网络架构

9.1.2.1.1 测评单元（L4-NCS1-01）

a) 测评指标

应保证网络设备的业务处理能力满足业务高峰期需要；（本条款引用自 GB/T 22239.1-20XX 8.1.2.1 a））

b) 测评对象

路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

1) 应访谈网络管理员了解系统的业务高峰时段，核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率；

2) 网络设备应未出现过宕机情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.1.2 测评单元（L4-NCS1-02）

a) 测评指标

应保证网络各个部分的带宽满足业务高峰期需要；（本条款引用自 GB/T 22239.1-20XX 8.1.2.1 b））

b) 测评对象

网络管理员或综合网管系统。

c) 测评实施

1) 应访谈网络管理员了解网络高峰时段；

2) 应核查综合网管系统，查看各通信链路带宽是否满足高峰时段的业务流量。

d) 单项判定

如果 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.1.3 测评单元（L4-NCS1-03）

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；（本条

款引用自 GB/T 22239.1-20XX 8.1.2.1 c））

b) 测评对象

路由器、交换机和防火墙等网络通信类设备。

c) 测评实施

1) 应访谈网络管理员依据何种原则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访谈结果一致。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.1.4 测评单元（L4-NCS1-04）

a) 测评指标

应避免将重要网络区域部署在网络边界处且没有边界防护措施；（本条款引用自 GB/T 22239.1-20XX 8.1.2.1 d））

b) 测评对象

网络管理员和网络拓扑图。

c) 测评实施

1) 应访谈网络管理员并查看网络拓扑图，核查重要网络区域不能部署在网络边界处且直接连接外部等级保护对象；

2) 应访谈网络管理员并查看网络拓扑图，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、ACL 等。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.1.5 测评单元（L4-NCS1-05）

a) 测评指标

应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性；（本条款引用自 GB/T 22239.1-20XX 8.1.2.1 e））

b) 测评对象

网络管理员和网络拓扑图。

c) 测评实施

应访谈管理员并查看网络拓扑图，核查系统是否有主要网络设备、安全设备和通信线路的硬件冗余。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

9.1.2.1.6 测评单元（L4-NCS1-06）

a) 测评指标

应可按照业务服务的重要程度分配带宽，优先保障重要业务。（本条款引用自 GB/T 22239.1-20XX 8.1.2.1 f））

b) 测评对象

路由器、交换机和流量控制设备等带宽控制设备。

c) 测评实施

应核查带宽控制设备是否按照业务服务的重要程度配置并启用了带宽策略。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.2.2 通信传输

9.1.2.2.1 测评单元（L4-NCS1-07）

a) 测评指标

应采用校验码技术或加解密技术保证通信过程中数据的完整性；（本条款引用自 GB/T 22239.1-20XX 8.1.2.2 a））

b) 测评对象

加解密设备或组件。

c) 测评实施

1) 应访谈安全管理员，询问是否在数据传输过程中使用校验码技术或其他加解密技术来保护其完整性；

2) 应核查加解密设备或组件，查看是否保证通信过程中数据的完整性。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.2.2 测评单元（L4-NCS1-08）

a) 测评指标

应采用加解密技术保证通信过程中敏感信息字段或整个报文的保密性。（本条款引用自 GB/T 22239.1-20XX 8.1.2.2 b））

b) 测评对象

加解密设备或组件。

c) 测评实施

1) 应访谈安全管理员，询问是否具有在通信过程中是否采取保密措施，具体措施有哪

些；

2) 应测试在通信过程中是否对敏感信息字段或整个报文进行加密。

d) **单项判定**

如果 1）-2)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.2.3 **测评单元（L4-NCS1-09）**

a) **测评指标**

应在通信前基于密码技术对通信的双方进行验证或认证。（本条款引用自 GB/T 22239.1-20XX 8.1.2.2 c））

b) **测评对象**

加解密设备或组件。

c) **测评实施**

应查看通信双方数据包的内容，查看是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证或认证。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.2.2.4 **测评单元（L4-NCS1-10）**

a) **测评指标**

应基于硬件设备对重要通信过程进行加解密运算和密钥管理。（本条款引用自 GB/T 22239.1-20XX 8.1.2.2 d））

b) **测评对象**

加解密设备或组件。

c) **测评实施**

1) 应核查是否基于硬件化的设备产生密钥，进行加解密运算；

2) 应核查相关证明材料（证书），查看采用的密码算法是否符合国家有关部门的要求。

d) **单项判定**

如果 1）-2)为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.3 **边界防护**

9.1.2.3.1 **测评单元（L4-NCS1-11）**

a) **测评指标**

应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；（本条款引用自 GB/T 22239.1-20XX 8.1.2.3 a））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应确认等级保护对象的网络边界位置，并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，该端口配置并启用了安全策略；

3) 应访谈安全管理员或核查设备配置信息，是否不存在其他未受控端口进行跨越边界的网络通信。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.3.2 测评单元（L4-NCS1-12）

a) 测评指标

应能够对内部用户非授权联到外部网络的行为进行限制或核查应能够对非授权设备私自联到内部网络的行为进行限制或核查，并对其进行有效阻断；（本条款引用自 GB/T 22239.1-20XX 8.1.2.3 b））

b) 测评对象

网络准入控制系统或设备。

c) 测评实施

1) 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断；

2) 应核查所有路由器和交换机闲置端口是否均已关闭。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.3.3 测评单元（L4-NCS1-13）

a) 测评指标

应能够对内部用户非授权联到外部网络的行为进行限制或核查；（本条款引用自 GB/T 22239.1-20XX 8.1.2.3 c））

b) 测评对象

网络准入控制系统或设备。

c) 测评实施

应核查是否采用技术措施防止内部用户非法外联行为。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

9.1.2.3.4 测评单元（L4-NCS1-14）

a) 测评指标

应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。（本条款引用自 GB/T 22239.1-20XX 8.1.2.3 d））

b) 测评对象

网络拓扑图和无线网络设备。

c) 测评实施

1) 应访谈网络管理员无线网络的部署方式，是否单独组网后再连接到有线网络；

2) 应确保无线网络通过受控的边界防护设备接入到内部有线网络。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.3.5 测评单元（L4-NCS1-14）

a) 测评指标

工控控制系统隔离区域内应避免使用无线网络，确需使用无线采集的数据，经过广域网进入隔离区域前应使用可信的网络信道、认证及加密方式确保无线网络数据安全可信。

b) 测评对象

安全接入设备、无线网络设备。

c) 测评实施

1) 应访谈网络管理员无线网络的部署方式，是否使用安全接入平台接入隔离区域；

2) 应确保使用可信的网络信道进行数据传输。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.3.6 测评单元（L4-NCS1-15）

a) 测评指标

应能够对连接到内部网络的设备进行可信验证，确保接入网络的设备真实可信。（本条款引用自 GB/T 22239.1-20XX 8.1.2.3 e））

b) 测评对象

网络准入控制设备或系统。

c) 测评实施

应访谈网络管理员是否采用技术措施对连接到内部网络的设备进行可信验证。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.2.4 访问控制

9.1.2.4.1 测评单元（L4-NCS1-16）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.4 a））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应核查在网络边界或区域之间是否部署网络访问控制设备，是否启用访问控制策略；

2) 应核查设备的访问控制策略，确保手工配置或设备默认的最后一条策略为禁止所有网络通信。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.4.2 测评单元（L4-NCS1-17）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.4 b））

b) 测评对象

网闸、防火墙、路由器和交换机等访问控制类设备。

c) 测评实施

1) 应核查设备访问控制策略，访谈安全管理员每一条策略的用途，查看是否不存在多余或无效的访问控制策略；

2) 应核查安全策略逻辑关系及访问控制策略排列顺序是否合理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.4.3 测评单元（L4-NCS1-18）

a) 测评指标

应不允许数据带通用协议通过；（本条款引用自 GB/T 22239.1-20XX 8.1.2.4 c））

b) 测评对象

网闸或协议转换类设备。

c) 测评实施

1) 应核查边界网络设备，查看是否采取协议转换或其他相应的控制措施来实现禁止数据带通用协议通过；

2) 应测试边界网络设备，可通过发送带通用协议的数据，测试访问控制措施是否有效阻断这种连接。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.4.4 测评单元（L2-NCS1-10）

a) 测评指标

工控控制系统隔离区域内不允许使用拨号访问服务。（新增）

b) 测评对象

拨号服务类设备。

c) 测评实施

1) 询问网络管理员，工控控制系统隔离区域内是否使用拨号访问服务；

2) 应核查工控控制系统隔离区域是否有拨号服务类设备。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.5 入侵防范

9.1.2.5.1 测评单元（L4-NCS1-19）

a) 测评指标

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；（本条款引用自 GB/T 22239.1-20XX 8.1.2.5 a））

b) 测评对象

IPS、IDS、抗 APT 攻击、防 DDoS 和网络回溯等系统或设备。

c) 测评实施

3) 应核查相关系统或设备，查看能否检测从外部发起的网络攻击行为；

4) 应核查相关系统或设备的规则库版本，查看是否及时更新；

5) 应测试相关系统或设备，验证其策略有效性；

6) 应核查相关系统或设备的防护策略，是否能够覆盖网络所有关键节点。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.5.2 测评单元（L4-NCS1-20）

a) 测评指标

应在关键网络节点处检测和限制从内部发起的网络攻击行为；（本条款引用自 GB/T 22239.1-20XX 8.1.2.5 b））

b) 测评对象

IPS、IDS、抗 APT 攻击、防 DDoS 和网络回溯等系统或设备。

c) 测评实施

1) 应核查相关系统或设备，查看能否检测从内部发起的网络攻击行为；

2) 应核查相关系统或设备的规则库版本，查看是否及时更新；

3) 应测试相关系统或设备，验证其策略有效性；

4) 应核查相关系统或设备的防护策略，是否能够覆盖网络所有关键节点。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.5.3 测评单元（L4-NCS1-21）

a) 测评指标

应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；（本条款引用自 GB/T 22239.1-20XX 8.1.2.5 c））

b) 测评对象

网络回溯和抗 APT 攻击等系统或设备。

c) 测评实施

1) 应核查是否部署网络回溯系统或抗 APT 攻击系统用来检测新型网络攻击；

2) 应核查系统能否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

d) 单项判定

如果 1）- 2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.2.5.4 测评单元（L4-NCS1-22）

a) 测评指标

当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。（本条款引用自 GB/T 22239.1-20XX 8.1.2.5 d））

b) 测评对象

IPS、IDS、抗 APT 攻击、防 DDoS 和网络回溯等系统或设备。

c) 测评实施

1) 应核查相关系统或设备，查看记录中是否包括：入侵源 IP、攻击类型、攻击目的、攻击时间等；

2) 应测试相关系统或设备验证其报警策略的有效性。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.6 恶意代码防范

9.1.2.6.1 测评单元（L4-NCS1-23）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.6 a））

b) **测评对象**

防病毒网关和 UTM 等防恶意代码设备。

c) **测评实施**

1) 应核查在关键网络节点处是否有相应的防恶意代码措施；

2) 应核查防恶意代码产品，查看其运行是否正常，恶意代码库是否及时更新。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.6.2 测评单元（L4-NCS1-24）

a) **测评指标**

应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。（本条款引用自 GB/T 22239.1-20XX 8.1.2.6 b））

b) **测评对象**

防垃圾邮件网关等设备。

c) **测评实施**

1) 应核查在关键网络节点处是否部署了防垃圾邮件类产品；

2) 应核查防垃圾邮件产品，查看其运行是否正常，防垃圾邮件规则库是否及时更新。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.6.3 测评单元（L4-NCS1-24）

a) **测评指标**

工控控制系统隔离区域内不允许使用邮件服务。

b) 测评对象

终端和服务器设备中的操作系统开启的服务。

c) 测评实施

应核查工控控制系统隔离区域内的终端和服务器是否开启了邮件服务。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.2.7 安全审计

9.1.2.7.1 测评单元（L4-NCS1-25）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.7 a））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否开启了日志记录或安全审计功能；

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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.7.2 测评单元（L4-NCS1-26）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.7 b））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 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) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.7.3 测评单元（L4-NCS1-27）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.7 c））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制和备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.7.4 测评单元（L4-NCS1-28）

a) 测评指标

审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；（本条款引用自 GB/T 22239.1-20XX 8.1.2.7 d））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查是否统一使用系统范围内唯一确定的时钟，以确保审计分析的正确性。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.8 集中管控

9.1.2.8.1 测评单元（L4-NCS1-29）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.2.8 a））

b) 测评对象

安全管理员和网络拓扑图。

c) 测评实施

1) 应访谈安全管理员并核查网络拓扑，查看是否划分单独网络区域用于部署安全管理系统；

2) 应核查各安全管理系统是否集中部署在安全管理区域。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.8.2 测评单元（L4-NCS1-30）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.8 b））

b) 测评对象

路由器、交换机和防火墙等设备。

c) 测评实施

1) 应核查网络是否建立安全的路由控制策略，如使用静态路由，或对动态路由协议启用加密认证机制；

2) 应核查网络中是否划分单独的管理 VLAN 用于对安全设备或安全组件进行管理；

3) 应核查网络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) 单项判定

如果 1）-3）其中之一为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.2.8.3 测评单元（L4-NCS1-31）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.8 c））

b) 测评对象

集中安全管控系统、IPS、IDS 等。

c) 测评实施

1) 应核查是否在网络中部署具备状态监控功能的集中安全管控系统，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) 应核查监测系统能否根据网络链路、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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.8.4 测评单元（L4-NCS1-32）

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；（本条款引用自 GB/T

22239.1-20XX 8.1.2.8 d））

b) 测评对象

综合安全审计系统、数据库审计系统或集中安全管控系统等。

c) 测评实施

1) 应核查网络中各设备是否配置独立于设备的集中安全管控系统，用于收集、存储设备日志；

2) 应核查是否部署统一的集中安全管控系统，统一收集、存储各设备日志，并根据需要进行集中审计分析。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.8.5 测评单元（L4-NCS1-33）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.2.8 e））

b) 测评对象

集中安全管控系统等。

c) 测评实施

1) 应核查是否通过安全管理区对网络安全策略（如防火墙访问控制策略、IPS 防护策略、WAF 防护策略等）进行统一管理；

2) 应核查是否实现对主机操作系统的防病毒软件及网络恶意代码防护设备的统一管理，实现病毒库的实时、统一升级；

3) 应核查是否实现网络中各设备统一、及时的补丁升级。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.2.8.6 测评单元（L4-NCS1-34）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.2.8 f））

b) 测评对象

集中安全管控系统等。

c) 测评实施

1) 应核查网络中是否在网络边界及关键节点，部署集中安全管控系统，并通过声光方

式实时报警；

2) 应核查集中安全管控系统的检测范围是否能够覆盖网络所有关键路径。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3 设备和计算安全

9.1.3.1 身份鉴别

9.1.3.1.1 测评单元（L4-ECS1-01）

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，用户名和口令不得相同，禁止明文存储口令。（增强）。（本条款引用自 GB/T 22239.1-20XX 8.1.3.1 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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，查看所有用户身份标识是否具有唯一性；

3) 应核查用户配置信息或访谈系统管理员，查看是否存在空密码用户；

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.1.2 测评单元（L4-ECS1-02）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.3.1 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

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达到一定次数后实现账户锁定功能；

3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.1.3 测评单元（L4-ECS1-03）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.3.1 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.1.4 测评单元（L4-ECS1-04）

a) 测评指标

应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。（本条款引用自 GB/T 22239.1-20XX 8.1.3.1 e））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别；

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.1.5 测评单元（L4-ECS1-08）

i) 测评指标

应能够对控制设备控制及操作指令进行加密传输及认证鉴别。

j) 测评对象

控制设备。

k) 测评实施

5) 应核查控制设备控制及操作指令在进行远程传输时，是否进行加密处理；

6) 应查看智能控制装置，核查当现场设备层向控制装置发起会话连接时，是否使用认证措施进行会话认证（非身份认证）。

l) 单项判定

如果 1）-2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.1.6 测评单元（L4-ECS1-36）

m) 测评指标

应能够对登录控制设备进行密码认证。

n) 测评对象

控制设备。

o) 测评实施

核查控制设备访问时是否提供密码认证选项。

p) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.2 访问控制

9.1.3.2.1 测评单元（L4-ECS1-05）

a) 测评指标

应对登录的用户分配账号和权限。（本条款引用自 GB/T 22239.1-20XX 8.1.3.2 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查或访谈用户账户和权限设置情况；

2) 应核查是否已禁用或限制匿名、默认账户的访问权限。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.2.2 测评单元（L4-ECS1-06）

a) 测评指标

应重命名默认账号或修改默认口令。（本条款引用自 GB/T 22239.1-20XX 8.1.3.2 b））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全

设备。

c) 测评实施

1) 应核查是否不存在默认账号或默认账号已重命名；

2) 应核查是否已修改默认账号的默认口令。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.2.3 测评单元（L4-ECS1-07）

a) 测评指标

应及时删除或停用多余的、过期的账号，避免共享账号的存在。（本条款引用自 GB/T 22239.1-20XX 8.1.3.2 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否不存在多余或过期账号；

2) 应访谈了解是否不同用户采用不同登录账号登录系统。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.2.4 测评单元（L4-ECS1-08）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.3.2 d））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查访问控制策略，查看管理用户的权限是否已进行分离；

2) 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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.2.5 测评单元（L4-ECS1-09）

a) 测评指标

应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。（本条款引用自 GB/T 22239.1-20XX 8.1.3.2 e））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否有管理用户负责配置访问控制策略；

2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则；

3) 应测试用户是否有可越权访问情形。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.2.6 测评单元（L4-ECS1-10）

a) 测评指标

访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。（本条款引用自 GB/T 22239.1-20XX 8.1.3.2 f））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.2.7 测评单元（L4-ECS1-11）

a) 测评指标

应对所有主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。（本条款引用自 GB/T 22239.1-20XX 8.1.3.2 g））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。

c) 测评实施

1) 应核查是否依据安全策略对所有主体、客体设置安全标记；

2) 应测试依据主体、客体安全标记控制主体对客体访问的强制访问控制功能。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.3 安全审计

9.1.3.3.1 测评单元（L4-ECS1-12）

a) 测评指标

应启用安全审计功能，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。（本条款引用自 GB/T 22239.1-20XX 8.1.3.3 a））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应核查是否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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.3.2 测评单元（L4-ECS1-13）

a) 测评指标

审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。（本条款引用自 GB/T 22239.1-20XX 8.1.3.3 b））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

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、主体标识、客体标识、事件类型、事件是否成功及其他与审计相关的信息。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.3.3 测评单元（L4-ECS1-14）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.3.3 c））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制及备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.3.4 测评单元（L4-ECS1-15）

a) 测评指标

应对审计进程进行保护，防止未经授权的中断。（本条款引用自 GB/T 22239.1-20XX 8.1.3.3 d））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应测试可否通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.3.5 测评单元（L4-ECS1-16）

a) 测评指标

审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。（本条款引用自 GB/T 22239.1-20XX 8.1.3.3 e））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应核查是否统一使用系统范围内唯一确定的时钟，以确保审计分析的正确性。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.3.6 测评单元（L4-ECS1-25）

i) 测评指标

控制设备应具备日志收集功能。

j) 测评对象

控制设备。

k) 测评实施

应核查控制设备是否具有日志收集功能。

l) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.3.7 测评单元（L4-ECS1-26）

i) 测评指标

控制设备的时钟保持应与时钟服务器同步。

j) 测评对象

控制设备。

k) 测评实施

应核查控制设备的时钟，确认其与时钟服务器是否同步。

l) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.4 入侵防范

9.1.3.4.1 测评单元（L4-ECS1-17）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.3.4 a））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否遵循最小安装原则；

2) 应确认是否已经关闭非必要的组件和应用程序。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.4.2 测评单元（L4-ECS1-18）

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。（本条款引用自 GB/T 22239.1-20XX

8.1.3.4 b））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员是否定期对系统服务进行梳理，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.4.3 测评单元（L4-ECS1-19）

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。（本条款引用自 GB/T 22239.1-20XX 8.1.3.4 c））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

应核查配置文件是否对终端接入范围进行限制。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.4.4 测评单元（L4-ECS1-20）

a) 测评指标

应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自 GB/T 22239.1-20XX 8.1.3.4 d））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应进行漏洞扫描，核查是否不存在高风险漏洞；

2) 应访谈系统管理员，查看是否在经过充分测试评估后及时修补漏洞。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.4.5 测评单元（L4-ECS1-21）

a) 测评指标

应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。（本条款引用自 GB/T 22239.1-20XX 8.1.3.4 e））

b) 测评对象

终端、控制设备和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈并查看入侵检测的措施，访谈是否部署了入侵检测工具；

2) 应查看重要节点的入侵行为记录和报警情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.4.6 测评单元（L4-ECS1-36）

m) 测评指标

应使用专用设备或专用软件对控制设备进行更新。

n) 测评对象

控制设备。

o) 测评实施

应核查控制设备更新设备是否为专用设备或专用软件。

p) 单项判定

如果以上内容均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.4.7 测评单元（L4-ECS1-30）

m) 测评指标

应关闭控制设备中不必要的端口和服务。

n) 测评对象

控制设备。

o) 测评实施

7) 应访谈管理员是否关闭了非必要的服务和端口；

8) 采用工控扫描设备对控制设备进行扫描。

p) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.5 恶意代码防范

9.1.3.5.1 测评单元（L4-ECS1-22）

a) 测评指标

应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。（本条款引用自 GB/T 22239.1-20XX 8.1.3.5））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应查看防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库，或查看是否采用可信计算技术建立从系统到应用的信任链；

2) 应访谈管理员，查看是否有保护重要系统程序或文件完整性的措施；

3) 应当检测到程序或文件受到破坏后，是否具备恢复的措施。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.5.2 测评单元（L4-ECS1-41）

i) 测评指标

应保证控制设备在入网前经过国家相关测评机构的安全性检测，确保控制设备固件中不存在恶意代码程序。

j) 测评对象

控制设备。

k) 测评实施

应核查控制设备经过国家相关测评机构检测的检测报告，明确控制设备固件中是否不存在恶意代码程序。若检测报告显示控制设备固件存在恶意代码程序，则询问终端管理员是否对恶意代码进行过处理，查看相关的处理报告和记录，并确认目前是否已不存在恶意代码程序。

l) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.6 资源控制

9.1.3.6.1 测评单元（L4-ECS1-23）

a) 测评指标

应限制单个用户或进程对系统资源的最大使用限度。（本条款引用自 GB/T 22239.1-20XX 8.1.3.6 a））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员核查系统资源控制的管理措施，如核查配置参数是否设置最大进程数；

2) 应引用产品（应用）测试结果，确认目前系统资源利用率在允许范围之内或者查看数据库表空间，目前总体数据库表空间占用率是否超过阀值，是否存在对数据库资源过大或最小的用户的限制措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.6.2 测评单元（L4-ECS1-24）

a) 测评指标

应提供重要节点设备的硬件冗余，保证系统的可用性。（本条款引用自 GB/T 22239.1-20XX 8.1.3.6 b））

b) 测评对象

终端、控制设备和服务器等设备。

c) 测评实施

查看重要节点设备是否有硬件冗余。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.3.6.3 测评单元（L4-ECS1-25）

a) 测评指标

应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况。（本条款引用自 GB/T 22239.1-20XX 8.1.3.7 c））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员，核查重要节点的系统 CPU、硬盘、内存、磁盘容量、网络服务等系统监控的手段和措施；

2) 应询问管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.6.4 测评单元（L4-ECS1-26）

a) 测评指标

应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。（本条款引用自 GB/T 22239.1-20XX 8.1.3.7 d））

b) 测评对象

终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件。

c) 测评实施

1) 应访谈管理员，查看是否有报警机制；

2) 应询问管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.3.6.5 测评单元（L2-ECS1-16）

a) 测评指标

应关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等，确需保留的必须通过相关的技术措施实施严格的监控管理。（新增）

b) 测评对象

终端和服务器等设备物理接口。

c) 测评实施

1) 应核查终端和服务器是否关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等；

2) 应访谈管理员对确需保留的软盘驱动、光盘驱动、USB 接口、串行口等是否通过相关的技术措施实施严格的监控管理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4 应用和数据安全

9.1.4.1 身份鉴别

9.1.4.1.1 测评单元（L4-ADS1-01）

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，鉴别信息具有复杂度要求并定期更换；（本条款引用自 GB/T 22239.1-20XX 8.1.4.1 a））

b) 测评对象

应用系统管理员和业务应用系统。

c) **测评实施**

1) 应核查用户在登录时是否采用了身份鉴别措施；

2) 应核查用户登录时是否使用唯一性身份标识；

3) 应测试应用系统对用户身份标识有效性是否进行鉴别；

4) 应核查鉴别信息是否具有复杂度要求并定期更换；

5) 应核查用户配置信息或访谈应用系统管理员，查看是否不存在空密码用户。

d) **单项判定**

如果 1）-5）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.1.2 **测评单元（L4-ADS1-02）**

a) **测评指标**

应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；（本条款引用自 GB/T 22239.1-20XX 8.1.4.1 b））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应测试是否进行用户登录失败处理；

2) 应核查登录失败反馈信息是否进行模糊处理；

3) 应测试用户连续多次登录失败时应用系统是否采取必要的保护措施。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.1.3 **测评单元（L4-ADS1-03）**

a) **测评指标**

应强制用户首次登录时修改初始口令；（本条款引用自 GB/T 22239.1-20XX 8.1.4.1 c））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应测试用户首次登录时是否被强制修改初始口令。

d) **单项判定**

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.1.4 测评单元（L4-ADS1-04）

a) 测评指标

用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。（本条款引用自 GB/T 22239.1-20XX 8.1.4.1 d））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试管理员是否能够对用户鉴别信息进行重置；

2) 应核查用户身份鉴别信息丢失或失效时，是否采取其他技术措施保证应用系统安全。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.1.5 测评单元（L4-ADS1-05）

a) 测评指标

应采用两种或两种以上组合的鉴别技术实现用户身份鉴别；（本条款引用自 GB/T 22239.1-20XX 8.1.4.1 e））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.1.6 测评单元（L4-ADS1-06）

a) 测评指标

登录用户执行重要操作时应再次进行身份鉴别。（本条款引用自 GB/T 22239.1-20XX 8.1.4.1 f））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查用户执行重要操作时应用系统是否再次进行身份鉴别。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.2 访问控制

9.1.4.2.1 测评单元（L4-ADS1-07）

a) 测评指标

应提供访问控制功能，对登录的用户分配帐号和权限；（本条款引用自 GB/T 22239.1-20XX 8.1.4.2 a））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否提供访问控制功能；

2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理；

3) 应测试不同岗位用户是否具有不同的权限。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.2.2 测评单元（L4-ADS1-08）

a) 测评指标

应重命名默认账户或修改默认口令；（本条款引用自 GB/T 22239.1-20XX 8.1.4.2 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否不存在默认账户或默认账户已重命名；

2) 应核查是否已修改默认账户的默认口令。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.2.3 测评单元（L4-ADS1-09）

a) 测评指标

应及时删除或停用多余的、过期的帐户，避免共享帐户的存在；（本条款引用自 GB/T 22239.1-20XX 8.1.4.2 c））

b) 测评对象

应用系统管理员和业务应用系统。

c) 测评实施

1) 应核查是否不存在多余账户或过期账户；

2) 应访谈了解是否不同用户采用不同登录账户登录应用系统。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.2.4 测评单元（L4-ADS1-10）

a) 测评指标

应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；（本条款引用自 GB/T 22239.1-20XX 8.1.4.2 d））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查不同岗位用户是否仅拥有其工作任务所需的最小权限；

2) 应核查业务岗位与管理岗位用户操作权限相互之间是否相互制约；

3) 应核查关键业务岗位用户操作权限相互之间是否相互制约；

4) 应核查关键管理岗位用户操作权限相互之间是否相互制约。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.2.5 测评单元（L4-ADS1-11）

a) 测评指标

应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；（本条款引用自 GB/T 22239.1-20XX 8.1.4.2 e））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否由管理用户负责配置访问控制策略；

2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则；

3) 应测试用户是否不存在可越权访问情形。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.2.6 测评单元（L4-ADS1-12）

a) 测评指标

访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；（本条款引用自 GB/T 22239.1-20XX 8.1.4.2 f））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.2.7 测评单元（L4-ADS1-13）

a) 测评指标

应对所有主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。（本条款引用自 GB/T 22239.1-20XX 8.1.4.2 g））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否依据安全策略对所有主体和客体设置了安全标记；

2) 应测试是否依据安全标记和强制访问控制规则确定主体对客体的访问。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.3 安全审计

9.1.4.3.1 测评单元（L4-ADS1-14）

a) 测评指标

应提供并启用安全审计功能，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；（本条款引用自 GB/T 22239.1-20XX 8.1.4.3 a））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否提供并启用了安全审计功能；

2) 应核查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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.3.2 测评单元（L4-ADS1-15）

a) 测评指标

审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；（本条款引用自 GB/T 22239.1-20XX 8.1.4.3 b））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查审计记录信息是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.3.3 测评单元（L4-ADS1-16）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.4.3 c））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否采取了保护措施对审计记录进行保护；

2) 应核查审计记录的备份机制及备份策略。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.3.4 测评单元（L4-ADS1-17）

a) 测评指标

应对审计进程进行保护，防止未经授权的中断；（本条款引用自 GB/T 22239.1-20XX 8.1.4.3 d））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试应用系统，可试图通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.3.5 测评单元（L4-ADS1-18）

a) 测评指标

审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；（本条款引用自 GB/T 22239.1-20XX 8.1.4.3 e））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应核查是否统一使用系统范围内唯一确定的时钟，以确保审计分析的正确性。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.4 软件容错

9.1.4.4.1 测评单元（L4-ADS1-19）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.4.4 a））

b) 测评对象

业务应用系统和系统设计文档等。

c) 测评实施

1) 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；

2) 应审核应用系统的源代码，在应用系统在人机接口或通信接口处是否对输入的数据进行有效性验证和处理；

3) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.4.2 测评单元（L4-ADS1-20）

a) 测评指标

在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；（本条款引用自 GB/T 22239.1-20XX 8.1.4.4 b））

b) 测评对象

系统设计文档和维护文档等。

c) 测评实施

1) 应核查应用系统设计文档和维护文档，应用系统有故障发生时是否能继续提供一部分功能；

2) 应核查应用系统设计文档和维护文档，应用系统有故障发生后，是否能够实施必要的措施使系统恢复功能。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.4.3 测评单元（L4-ADS1-21）

a) 测评指标

应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。（本条款引用自 GB/T 22239.1-20XX 8.1.4.4 c））

b) 测评对象

系统设计文档和维护文档等。

c) 测评实施

1) 应核查应用系统设计文档和维护文档，当故障发生时应用系统是否能自动保护当前所有状态；

2) 应核查应用系统设计文档和维护文档，应用系统发生故障后能够恢复故障时的状态。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.5 资源控制

9.1.4.5.1 测评单元（L4-ADS1-22）

a) 测评指标

当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；（本条款引用自 GB/T 22239.1-20XX 8.1.4.5 a））

b) 测评对象

业务应用系统。

c) 测评实施

1) 应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。

d) 单项判定

如果 1） 为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.5.2 测评单元（L4-ADS1-23）

a) 测评指标

应能够对系统的最大并发会话连接数进行限制；（本条款引用自 GB/T 22239.1-20XX 8.1.4.5 b））

b) 测评对象

业务应用系统或中间件等。

c) 测评实施

1) 应核查应用系统配置信息是否对最大并发会话连接数进行限制；

2) 应核查中间件配置信息是否对最大并发会话连接数进行限制。

d) 单项判定

如果 1）或 2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.5.3 测评单元（L4-ADS1-24）

a) 测评指标

应能够对单个账户的多重并发会话进行限制；（本条款引用自 GB/T 22239.1-20XX 8.1.4.5 c））

b) 测评对象

业务应用系统。

c) 测评实施

应测试是否能够正确地限制单个账户的多重并发会话数。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.4.5.4 测评单元（L4-ADS1-25）

a) 测评指标

应能够对并发进程的每个进程占用的资源分配最大限额。（本条款引用自 GB/T 22239.1-20XX 8.1.4.5 d））

b) 测评对象

业务应用系统或中间件等。

c) 测评实施

1) 应核查是否对并发进程的每个进程占用的资源设置最大限额；

2) 应测试应用系统，验证并发进程的每个进程占用资源是否被限制在最大限额内。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

9.1.4.6 数据完整性

9.1.4.6.1 测评单元（L4-ADS1-26）

a) 测评指标

应采用校验码技术或加解密技术保证重要数据在传输过程中的完整性；（本条款引用自GB/T 22239.1-20XX 8.1.4.6 a））

b) 测评对象

系统设计文档和业务应用系统。

c) 测评实施

1) 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码技术或加解密技术保证完整性；

2) 应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.6.2 测评单元（L4-ADS1-27）

a) 测评指标

应采用校验码技术或加解密技术保证重要数据在存储过程中的完整性；（本条款引用自GB/T 22239.1-20XX 8.1.4.6 b））

b) 测评对象

系统设计文档、业务应用系统和数据加解密系统。

c) 测评实施

1) 应核查设计文档，是否采用校验码技术或加解密技术保证重要配置数据、重要业务数据在存储过程中的完整性；

2) 应核查数据加解密系统是否能够保证重要配置数据、重要业务数据在存储过程中的完整性；

3) 应测试在存储过程中对重要配置数据、重要业务数据进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.6.3 测评单元（L4-ADS1-28）

a) 测评指标

应对重要数据传输提供专用通信协议或安全通信协议，避免来自基于通用通信协议的攻击破坏数据完整性。（本条款引用自 GB/T 22239.1-20XX 8.1.4.6 c））

b) 测评对象

系统设计文档和业务应用系统。

c) 测评实施

1) 应核查系统设计文档，查看是否为重要业务数据传输提供专用通信协议或安全通信协议保证数据完整性。

2) 应通过嗅探等方式抓取传输过程中的数据包，查看重要管理数据、重要业务数据在传输过程中是否能够被通用的网络嗅探工具抓取。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.7 数据保密性

9.1.4.7.1 测评单元（L4-ADS1-29）

a) 测评指标

应采用加解密技术保证重要数据在传输过程中的保密性；（本条款引用自 GB/T 22239.1-20XX 8.1.4.7 a））

b) 测评对象

系统设计文档和业务应用系统。

c) 测评实施

1) 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加解密技术保证保密性；

2) 应通过嗅探等方式抓取传输过程中的数据包，查看重要管理数据、重要业务数据在传输过程中是否进行了加密处理。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.7.2 测评单元（L4-ADS1-30）

a) 测评指标

应采用加解密技术保证重要数据在存储过程中的保密性；（本条款引用自 GB/T 22239.1-20XX 8.1.4.7 b））

b) 测评对象

系统设计文档、业务应用系统和数据加解密系统。

c) 测评实施

1) 应核查是否采用加解密技术保证重要配置数据、重要业务数据在存储过程中的保密性；

2) 应核查数据加解密系统是否能够保证重要配置数据、重要业务数据在存储过程中的保密性。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.7.3 **测评单元（L4-ADS1-31）**

a) **测评指标**

应对重要数据传输提供专用通信协议或安全通信协议，避免来自基于通用通信协议的攻击破坏数据保密性。（本条款引用自 GB/T 22239.1-20XX 8.1.4.7 c））

b) **测评对象**

系统设计文档和业务应用系统。

c) **测评实施**

1) 应核查系统设计文档，查看是否为重要业务数据传输提供专用通信协议或安全通信协议保证数据保密性；

2) 应通过嗅探等方式抓取传输过程中的数据包，查看重要管理数据、重要业务数据在传输过程中是否能够被通用的网络嗅探工具抓取。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.8 **数据备份恢复**

9.1.4.8.1 **测评单元（L4-ADS1-32）**

a) **测评指标**

应提供重要数据的本地数据备份与恢复功能；（本条款引用自 GB/T 22239.1-20XX 8.1.4.8 a））

b) **测评对象**

配置数据和业务数据。

c) **测评实施**

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，查看是否能够进行正常的数据恢复。

d) **单项判定**

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.8.2 测评单元（L4-ADS1-33）

a) 测评指标

应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；（本条款引用自 GB/T 22239.1-20XX 8.1.4.8 b））

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实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.4.8.3 测评单元（L4-ADS1-34）

a) 测评指标

应提供重要数据处理系统的热冗余，保证系统的高可用性；（本条款引用自 GB/T 22239.1-20XX 8.1.4.8 c））

b) 测评对象

重要数据处理系统。

c) 测评实施

应核查重要数据处理系统（包括边界交换机、边界防火墙、核心路由器、应用服务器和数据库服务器等）是否采用热冗余方式部署。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.1.4.8.4 测评单元（L4-ADS1-35）

a) 测评指标

应建立异地灾难备份中心，提供业务应用的实时切换。（本条款引用自 GB/T 22239.1-20XX 8.1.4.8 d））

b) 测评对象

灾难备份中心及相关组件。

c) 测评实施

1) 应核查是否建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数

据处理设备；

2) 应核查是否提供业务应用的实时切换功能。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.9 剩余信息保护

9.1.4.9.1 测评单元（L4-ADS1-36）

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；（本条款引用自 GB/T 22239.1-20XX 8.1.4.9 a））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应核查相关配置信息或访谈应用系统管理员，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) **单项判定**

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.9.2 测评单元（L4-ADS1-37）

a) **测评指标**

应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。（本条款引用自 GB/T 22239.1-20XX 8.1.4.9 b））

b) **测评对象**

业务应用系统。

c) **测评实施**

1) 应核查相关配置信息或访谈应用系统管理员，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除。

d) **单项判定**

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.10 个人信息保护

9.1.4.10.1 测评单元（L4-ADS1-38）

a) **测评指标**

应仅采集和保存业务必需的用户信息；（本条款引用自 GB/T 22239.1-20XX 8.1.4.10 a））

b) 测评对象

用户数据和业务应用系统。

c) 测评实施

1) 应核查采集的用户信息是否是业务应用必需的。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.1.4.10.2 测评单元（L4-ADS1-39）

a) 测评指标

应禁止未授权访问和使用用户信息。（本条款引用自 GB/T 22239.1-20XX 8.1.4.10 b））

b) 测评对象

用户数据和业务应用系统。

c) 测评实施

1) 应核查是否通过访问控制限制对用户信息的访问和使用。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2 安全管理测评

9.2.1 安全策略和管理制度

9.2.1.1 安全策略

9.2.1.1.1 测评单元（L4-PSS1-01）

a) 测评指标

应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。本条款引用自 GB/T 22239.1-20XX 8.2.1.1）

b) 测评对象

总体方针策略类文档。

c) 测评实施

应核查信息安全工作的总体方针和安全策略文件，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.1.2 管理制度

9.2.1.2.1 测评单元（L4-PSS1-02）

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。本条款引用自 GB/T 22239.1-20XX 8.2.1.2 a））

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，查看是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.1.2.2 测评单元（L4-PSS1-03）

a) 测评指标

应对要求管理人员或操作人员执行的日常管理操作建立操作规程。本条款引用自 GB/T 22239.1-20XX 8.2.1.2 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.1.2.3 测评单元（L4-PSS1-04）

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信息安全管理制度体系。本条款引用自 GB/T 22239.1-20XX 8.2.1.1 c））

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是否形成体系化。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级

保护对象不符合本单项测评指标要求。

9.2.1.2.4 测评单元(L1-PSS1-02）

a) 测评指标

应按照“谁主管谁负责，谁运营谁负责”的原则，建立工控系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。（新增）

b) 测评对象

安全管理制度类文档。

c) 测评实施

应核查工控系统安全管理制度，查看是否按照“谁主管谁负责，谁运营谁负责”的原则，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将工控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.1.3 制定和发布

9.2.1.3.1 测评单元（L4-PSS1-05）

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。本条款引用自 GB/T 22239.1-20XX 8.2.1.3 a））

b) 测评对象

安全主管。

c) 测评实施

应访谈安全主管，询问是否由专门的部门或人员负责制定安全管理制度。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.1.3.2 测评单元（L4-PSS1-06）

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。本条款引用自 GB/T 22239.1-20XX 8.2.1.3 b））

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

1) 应核查制度制定和发布要求管理文档，查看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，查看是否通过正式、有效的方式收发（如正式发文、领导签署和单位盖章等），是否注明发布范围。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.1.4 评审和修订

9.2.1.4.1 测评单元（L4-PSS1-07）

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。（本条款引用自 GB/T 22239.1-20XX 8.2.2.4）

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈安全主管，询问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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2 安全管理机构和人员

9.2.2.1 岗位设置

9.2.2.1.1 测评单元（L4-ORS1-01）

a) 测评指标

应成立指导和管理信息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委任或授权，并定期组织开展信息安全工作。（本条款引用自 GB/T 22239.1-20XX 8.2.2.1 a））

b) 测评对象

信息安全主管、管理制度类文档和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否成立了指导和管理信息安全工作的委员会或领导小组；

2) 应核查部门职责文档，查看信息安全工作的委员会或领导小组构成情况和相关职责；

3) 应核查信息安全工作的委员会或领导小组开展工作的会议纪要或相关记录。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.1.2 **测评单元（L4-ORS1-02）**

a) **测评指标**

应设立信息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。（本条款引用自 GB/T 22239.1-20XX 8.2.2.1 a））

b) **测评对象**

信息安全主管和管理制度类文档。

c) **测评实施**

1) 应访谈信息安全主管，确认是否进行了信息安全管理职能部门的划分；

2) 应核查部门职责文档，查看是否明确信息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，查看岗位划分情况和岗位职责。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.1.3 **测评单元（L4-ORS1-03）**

a) **测评指标**

应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。（本条款引用自 GB/T 22239.1-20XX 8.2.2.1 c））

b) **测评对象**

信息安全主管和管理制度类文档。

c) **测评实施**

1) 应访谈信息安全主管，确认是否进行了信息安全管理岗位的划分；

2) 应核查岗位职责文档，查看是否明确了各岗位职责。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.1.4 **测评单元（L1-ORS1-02）**

a) **测评指标**

应明确由主管安全生产的领导作为工控系统安全防护的主要责任人。（新增）

b) **测评对象**

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否由主管安全生产的领导作为工控系统安全防护的主要责任人；

2) 应核查岗位职责文档，查看是明确由主管安全生产的领导作为工控系统安全防护的主要责任人。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.2 资金保障

9.2.2.2.1 测评单元（L1-ORS1-01）

a) 测评指标

应保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金。（新增）

b) 测评对象

信息安全主管和管理制度类文档。

c) 测评实施

1) 应访谈信息安全主管，是否能够保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金；

2) 应核查安全管理制度中是否有保障工控控制系统安全建设、运维、核查、等级保护测评及其它信息安全资金的内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.3 人员配备

9.2.2.3.1 测评单元（L4-ORS1-04）

a) 测评指标

应配备一定数量的系统管理员、网络管理员、安全管理员等。（本条款引用自 GB/T 22239.1-20XX 8.2.2.2 a））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认各岗位人员配备情况；

2) 应核查人员配备文档，查看各岗位人员配备情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.3.2 测评单元（L4-ORS1-05）

a) 测评指标

应配备专职安全管理员，不可兼任。（本条款引用自 GB/T 22239.1-20XX 8.2.2.2 b））

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，查看是否配备了专职安全管理员。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.2.3.3 测评单元（L4-ORS1-06）

a) 测评指标

关键事务岗位应配备多人共同管理。（本条款引用自 GB/T 22239.1-20XX 8.2.2.2 c））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，询问是否对关键岗位配备了多人；

2) 应核查人员配备文档，查看关键岗位是否配备多人。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.4 授权和审批

9.2.2.4.1 测评单元（L4-ORS1-07）

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。（本条款引用自 GB/T 22239.1-20XX 8.2.2.3 a））

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

1) 应核查部门职责文档，查看各部门的职责和授权范围；

2) 应核查岗位职责文档，查看各岗位的职责和授权范围；

3) 应核查审批记录，查看审批事项、审批部门和批准人等内容是否与相关制度一致。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.4.2 **测评单元（L4-ORS1-08）**

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。本条款引用自 GB/T 22239.1-20XX 8.2.2.3 b））

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**

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，查看相关操作过程中是否建立了逐级审批程序。

2) 应核查审批记录、操作记录，查看审批结果是否与相关制度一致。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.4.3 **测评单元（L4-ORS1-09）**

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。本条款引用自 GB/T 22239.1-20XX 8.2.2.3 c））

b) **测评对象**

信息安全主管。

c) **测评实施**

应访谈信息安全主管，询问是否对各类审批事项进行更新。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.2.5 **沟通和合作**

9.2.2.5.1 **测评单元（L4-ORS1-10）**

a) **测评指标**

应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题。本条款引用自 GB/T 22239.1-20XX 8.2.2.4 a））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否建立了各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通机制；

2) 应核查会议记录，查看各类管理人员之间、组织内部机构之间以及信息安全职能部门内部是否开展了合作与沟通。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.5.2 测评单元（L4-ORS1-11）

a) 测评指标

应加强与兄弟单位、公安机关、各类供应商、业界专家及安全组织的合作与沟通。本条款引用自 GB/T 22239.1-20XX 8.2.2.4 b））

b) 测评对象

信息安全主管和记录表单类文档。

c) 测评实施

1) 应访谈信息安全主管，确认是否建立了与兄弟单位、公安机关、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，查看与兄弟单位、公安机关、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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.5.3 测评单元（L4-ORS1-12）

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。本条款引用自 GB/T 22239.1-20XX 8.2.2.4 c））

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.2.6 **审核和核查**

9.2.2.6.1 **测评单元（L4-ORS1-13）**

a) **测评指标**

应定期进行常规安全核查，核查内容包括系统日常运行、系统漏洞和数据备份等情况。本条款引用自 GB/T 22239.1-20XX 8.2.2.5 a））

b) **测评对象**

信息安全主管和记录表单类文档。

c) **测评实施**

1) 应访谈信息安全主管，确认是否定期进行了常规安全核查；

2) 应核查常规安全核查记录，查看记录内容是否包括了系统日常运行、系统漏洞和数据备份等情况。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.6.2 **测评单元（L4-ORS1-14）**

a) **测评指标**

应定期进行全面安全核查，核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。本条款引用自 GB/T 22239.1-20XX 8.2.2.5 b））

b) **测评对象**

信息安全主管和记录表单类文档。

c) **测评实施**

1) 应访谈信息安全主管，确认是否定期进行了全面安全核查；

2) 应核查全面安全核查记录，查看记录内容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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.6.3 **测评单元（L4-ORS1-15）**

a) **测评指标**

应制定安全核查表格实施安全核查，汇总安全核查数据，形成安全核查报告，并对安全核查结果进行通报。本条款引用自 GB/T 22239.1-20XX 8.2.2.5 c））

b) **测评对象**

记录表单类文档。

c) 测评实施

1) 应核查安全核查表格、安全核查记录、安全核查报告、安全核查结果通报记录，以此确认是否开展了安全核查，记录了核查数据，形成了核查报告，并对安全核查结果进行了通报。

d) 单项判定

如果 1）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.7 人员录用

9.2.2.7.1 测评单元（L4-ORS1-16）

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；本条款引用自（GB/T 22239.1-20XX 9.2.2.6 a））

b) 测评对象

信息安全主管。

c) 测评实施

应访谈安全主管，询问是否由专门的部门或人员负责人员的录用工作。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.2.7.2 测评单元（L4-ORS1-17）

a) 测评指标

应对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；本条款引用自（GB/T 22239.1-20XX 9.2.2.6 b））

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

1) 应核查人员安全管理文档，查看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、背景、专业资格和资质等进行审查的相关文档或记录，查看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，查看是否记录考核内容和考核结果等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

9.2.2.7.3 测评单元（L4-ORS1-18）

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；本条款引用自（GB/T 22239.1-20XX 9.2.2.6 c））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查保密协议，查看是否有保密范围、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，查看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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.7.4 测评单元（L4-ORS1-19）

a) 测评指标

应从内部人员中选拔从事关键岗位的人员。本条款引用自（GB/T 22239.1-20XX 9.2.2.6 d））

b) 测评对象

人事负责人。

c) 测评实施

应访谈人事负责人，询问从事关键岗位的人员是否是从内部人员选拔担任。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.2.8 人员离岗

9.2.2.8.1 测评单元（L4-ORS1-20）

a) 测评指标

应及时终止离岗员工的所有访问权限，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；本条款引用自（GB/T 22239.1-20XX 9.2.2.7 a））

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交还身份证件、设备等的登记记录。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.2.8.2 测评单元（L4-ORS1-21）

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。本条款引用自（GB/T 22239.1-20XX 9.2.2.7 b））

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

1) 应核查人员离岗的管理文档，查看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，查看是否有调离人员的签字。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.9 安全意识教育和培训

9.2.2.9.1 测评单元（L4-ORS1-22）

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；本条款引用自（GB/T 22239.1-20XX 9.2.2.8 a））

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查信息安全教育及技能培训文档，查看是否明确培训周期、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，查看是否包含具体的安全责任和惩戒措施。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.9.2 测评单元（L4-ORS1-23）

a) 测评指标

应针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。

本条款引用自（GB/T 22239.1-20XX 9.2.2.8 b））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查安全教育和培训计划文档，查看是否具有不同岗位的培训计划；查看培训内容是否包含信息安全基础知识、岗位操作规程等；

2) 应核查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.10 外部人员访问管理

9.2.2.10.1 测评单元（L4-ORS1-24）

a) 测评指标

应确保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；本条款引用自（GB/T 22239.1-20XX 9.2.2.9 a））

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

1) 应核查外部人员访问管理文档，查看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，查看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，查看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) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.10.2 测评单元（L4-ORS1-25）

a) 测评指标

应确保在外部人员接入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；本条款引用自（GB/T 22239.1-20XX 9.2.2.9 b））

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

1) 应核查外部人员访问管理文档，查看是否明确外部人员接入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，查看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，查看是否记录了外部人员访问的权限、时限、账户等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.10.3 测评单元（L4-ORS1-26）

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；本条款引用自（GB/T 22239.1-20XX 9.2.2.9 c））

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

1) 应核查外部人员访问管理文档，查看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，查看是否记录了访问权限清除时间。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.2.10.4 测评单元（L4-ORS1-27）

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；本条款引用自（GB/T 22239.1-20XX 9.2.2.9 d））

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.2.10.5 测评单元（L4-ORS1-28）

a) 测评指标

对关键区域或关键系统不允许外部人员访问。本条款引用自（GB/T 22239.1-20XX 9.2.2.9 e））

b) 测评对象

管理制度类文档。

c) 测评实施

应核查外部人员访问管理文档，查看是否明确不允许外部人员访问关键区域或关键业务系统。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3 安全建设管理

9.2.3.1 定级和备案

9.2.3.1.1 测评单元（L4-CMS1-01）

a) 测评指标

应以书面的形式说明保护对象的边界、安全保护等级及确定等级的方法和理由；（本条款引用自 GB/T 22239.1-20XX 8.2.3.1a））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查定级文档，查看文档是否明确保护对象的边界和安全保护等级，是否说明定级的方法和理由。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.1.2 测评单元（L4-CMS1-02）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.1 b））

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.1.3 测评单元（L4-CMS1-03）

a) 测评指标

应确保定级结果经过相关部门的批准；（本条款引用自 GB/T 22239.1-20XX 8.2.3.1 c））

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，查看是否有上级主管部门或本单位相关部门的审批意见。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.1.4 测评单元（L4-CMS1-04）

a) 测评指标

应将备案材料报主管部门和相应公安机关备案。（本条款引用自 GB/T 22239.1-20XX 8.2.3.1 d））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.2 安全方案设计

9.2.3.2.1 测评单元（L4-CMS1-05）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.2 a））

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，查看是否根据安全等级选择安全措施，是否根据安全需求调整安

全措施。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.2.2 测评单元（L4-CMS1-06）

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，并形成配套文件；（本条款引用自 GB/T 22239.1-20XX 8.2.3.2 b））

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。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.2.3 测评单元（L4-CMS1-07）

a) 测评指标

应组织相关部门和有关安全专家对安全总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。（本条款引用自 GB/T 22239.1-20XX 8.2.3.2 c））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查配套文件的论证评审记录或文档，查看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论证意见；

2) 应核查是否有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.3.3 产品采购和使用

9.2.3.3.1 测评单元（L4-CMS1-08）

a) 测评指标

应确保信息安全产品采购和使用符合国家的有关规定；（本条款引用自 GB/T 22239.1-20XX 8.2.3.3 a））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.3.2 测评单元（L4-CMS1-09）

a) 测评指标

应确保密码产品采购和使用符合国家密码主管部门的要求；（本条款引用自 GB/T 22239.1-20XX 8.2.3.3 b））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求；

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.3.3 测评单元（L4-CMS1-10）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.3 c））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.3.4 测评单元（L4-CMS1-11）

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。（本条

款引用自 GB/T 22239.1-20XX 8.2.3.3 d））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.3.5 测评单元（L1-CMS1-03）

a) 测评指标

工控控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用。（新增）

b) 测评对象

建设负责人、检测报告类文档。

c) 测评实施

1) 应访谈建设负责人，询问系统使用的工控控制系统重要设备及专用信息安全产品是否通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测；

2) 应核查工控控制系统通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测的检测报告。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.3.4 自行软件开发

9.2.3.4.1 测评单元（L4-CMS1-12）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.4 a））

b) 测评对象

建设负责人。

c) 测评实施

3) 应访谈建设负责人，询问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；

4) 应核查测试数据和结果是否受控使用。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.3.4.2 测评单元（L4-CMS1-13）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.4 b））

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，查看文件是否明确软件设计、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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.4.3 测评单元（L4-CMS1-14）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.4 c））

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，查看规范中是否明确代码安全编写规则；

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.4.4 测评单元（L4-CMS1-15）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.4 d））

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。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.4.5 测评单元（L4-CMS1-16）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.4 e））

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，明确软件存在的安全问题及可能存在的恶意代码。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.4.6 测评单元（L4-CMS1-17）

a) 测评指标

应确保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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.4 f））

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，查看是否有批准人的签字；

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.4.7 测评单元（L4-CMS1-18）

a) 测评指标

应确保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。（本条款引用自 GB/T 22239.1-20XX 8.2.3.4 g））

b) 测评对象

建设负责人。

c) 测评实施

应访谈建设负责人，询问开发人员是否为专职，是否对开发人员活动进行控制等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.5 外包软件开发

9.2.3.5.1 测评单元（L4-CMS1-19）

a) 测评指标

应在软件交付前检测软件质量和其中可能存在的恶意代码；（本条款引用自 GB/T 22239.1-20XX 8.2.3.5 a））

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软件质量和恶意代码检测报告。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.5.2 测评单元（L4-CMS1-20）

a) 测评指标

应要求开发单位提供软件设计文档和使用指南；（本条款引用自 GB/T 22239.1-20XX 8.2.3.5 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.5.3 测评单元（L4-CMS1-21）

a) 测评指标

应要求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。（本条款引用自 GB/T 22239.1-20XX 8.2.3.5 c））

b) 测评对象

建设负责人和记录表单类文档。

c) 测评实施

1) 应访谈建设负责人，询问是否具有软件源代码；

2) 应核查软件测试报告，查看是否明确审查了软件可能存在的后门和隐蔽信道并记录。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.3.5.4 **测评单元（L2-CMS1-13）**

a) **测评指标**

应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。（新增）

b) **测评对象**

外包合同。

c) **测评实施**

应核查外包开发合同中是否包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.6 **工程实施**

9.2.3.6.1 **测评单元（L4-CMS1-22）**

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.6 a））

b) **测评对象**

建设负责人。

c) **测评实施**

应访谈建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.6.2 **测评单元（L4-CMS1-23）**

a) **测评指标**

应制定工程实施方案控制安全工程实施过程；（本条款引用自 GB/T 22239.1-20XX 8.2.3.6 b））

b) **测评对象**

记录表单类文档。

c) 测评实施

应核查工程实施方案，查看其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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.6.3 测评单元（L4-CMS1-24）

a) 测评指标

应通过第三方工程监理控制项目的实施过程。（本条款引用自 GB/T 22239.1-20XX 8.2.3.6 c））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查第三方工程监理报告，查看是否明确了工程进展、时间计划、控制措施等方面内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.7 测试验收

9.2.3.7.1 测评单元（L4-CMS1-25）

a) 测评指标

在制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；（本条款引用自 GB/T 22239.1-20XX 8.2.3.7 a））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查是否具有工程测试验收方案，查看其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) 应核查是否具有测试验收报告，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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.3.7.2 测评单元（L4-CMS1-26）

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。（本条款引用自 GB/T 22239.1-20XX 8.2.3.7 b））

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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.8 系统交付

9.2.3.8.1 测评单元（L4-CMS1-27）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.8 a））

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清单，查看交付清单是否说明系统交付的各类设备、软件、文档等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.8.2 测评单元（L4-CMS1-28）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.8 b））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查是否有交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.8.3 测评单元（L4-CMS1-29）

a) 测评指标

应确保提供建设过程中的文档和指导用户进行运行维护的文档。（本条款引用自 GB/T 22239.1-20XX 8.2.3.8 c））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查交付文档，查看是否有指导用户进行运维的文档等，提交的文档是否符合管理规定的要求。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.9 等级测评

9.2.3.9.1 测评单元（L4-CMS1-30）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.9 a））

b) 测评对象

运维负责人和记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，本次测评是否为首次，若非首次，以往进行过几次测评，是否根据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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.3.9.2 测评单元（L4-CMS1-31）

a) 测评指标

应在发生重大变更或系统级别发生变化时进行等级测评；（本条款引用自 GB/T 22239.1-20XX 8.2.3.9 b））

b) 测评对象

运维负责人和记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，系统是否过重大变更或级别发生过变化，若有，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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.3.9.3 **测评单元（L4-CMS1-32）**

a) **测评指标**

应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。（本条款引用自 GB/T 22239.1-20XX 8.2.3.9 c））

b) **测评对象**

运维负责人。

c) **测评实施**

应访谈运维负责人，以往等级测评的测评单位是否具有国家相关等级测评资质的单位。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.10 **服务供应商管理**

9.2.3.10.1 **测评单元（L4-CMS1-33）**

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；（本条款引用自 GB/T 22239.1-20XX 8.2.3.10 a））

b) **测评对象**

运维负责人。

c) **测评实施**

应访谈建设负责人，询问等级保护对象选择的安全服务商有哪些，是否符合国家有关规定。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.10.2 **测评单元（L4-CMS1-34）**

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信息安全相关义务；（本条款引用自 GB/T 22239.1-20XX 8.2.3.10 b））

b) **测评对象**

记录表单类文档。

c) 测评实施

应核查是否具有与安全服务商签订的服务合同或安全责任合同书，查看是否明确了后期的技术支持和服务承诺等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.3.10.3 测评单元（L4-CMS1-35）

a) 测评指标

应定期监视、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。（本条款引用自 GB/T 22239.1-20XX 8.2.3.10 c））

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

1) 应核查是否具有安全服务商定期提交的安全服务报告；

2) 应核查是否定期审核评价安全服务供应商所提供的服务，是否具有服务审核报告；

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

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4 系统运维管理

9.2.4.1 环境管理

9.2.4.1.1 测评单元（L4-MMS1-01）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.1 a））

b) 测评对象

物理安全负责人、记录表单类文档。

c) 测评实施

1) 应访谈物理安全负责人，询问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，由何部门/何人负责；

2) 应核查部门或人员岗位职责文档，查看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，查看是否记录来访人员、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，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。

d) **单项判定**

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.1.2 **测评单元（L4-MMS1-02）**

a) **测评指标**

应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；（本条款引用自 GB/T 22239.1-20XX 8.2.4.1 b）

b) **测评对象**

管理制度类文档、记录表单类文档。

c) **测评实施**

1) 应核查机房安全管理制度，查看制度内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容；

2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录，是否与制度相符。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.1.3 **测评单元（L4-MMS1-03）**

a) **测评指标**

应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等；（本条款引用自 GB/T 22239.1-20XX 8.2.4.1 c）

b) **测评对象**

管理制度类文档、办公环境。

c) **测评实施**

1) 应核查机房安全管理制度，查看是否明确来访人员的接待区域；

2) 应核查办公桌面上是否包含敏感信息的纸档文件、移动介质等。

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.1.4 **测评单元（L4-MMS1-04）**

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。（本条款引用自 GB/T 22239.1-20XX 8.2.4.1 d））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查出入人员授权审批记录，查看是否明确对人员有不同的授权；

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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.1.5 测评单元（L4-PES1-24）

a) 测评指标

室外控制设备应明确专人负责，并定期进行核查、维护和清洁工作。

b) 测评对象

室外控制设备。

c) 测评实施

1) 应询问管理员室外控制设备是否有专人负责；

2) 应核查相关记录是否定期对室外控制设备进行核查、维护和清洁工作的记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.2 资产管理

9.2.4.2.1 测评单元（L4-MMS1-05）

a) 测评指标

应编制并保存与等级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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.2 a））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查资产清单，查看其内容是否覆盖资产责任部门、重要程度和所处位置等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.2.2 测评单元（L4-MMS1-06）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.2 b）

b) 测评对象

资产管理员单、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问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，查看其是否具有相应标识，标识方法是否符合 2）中相关要求。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.2.3 测评单元（L4-MMS1-07）

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。（本条款引用自 GB/T 22239.1-20XX 8.2.4.2 c）

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查信息分类文档，查看其内容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) 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。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.3 介质管理

9.2.4.3.1 测评单元（L4-MMS1-08）

a) 测评指标

应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；（本条款引用自 GB/T 22239.1-20XX 8.2.4.3 a）

b) 测评对象

资产管理员、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理；

2) 应核查介质使用管理记录，查看其是否记录介质归档和使用等情况。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.3.2 测评单元（L4-MMS1-09）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.3 b）

b) 测评对象

资产管理员、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问介质在物理传输过程中的人员、打包交付等情况是否进行控制；

2) 应核查是否有对介质的归档和查询等的登记记录。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.3.3 测评单元（L1-MMS1-03）

a) 测评指标

应建立隔离区域移动存储介质安全管理制度，对移动存储介质的使用进行限制。（新增）

b) 测评对象

资产管理员、管理制度类文档、记录表单类文档。

c) 测评实施

1) 应访谈资产管理员，询问是否建立隔离区域移动存储介质安全管理制度，是否对移动存储介质的使用进行限制；

2) 应查看是否有隔离区域移动存储介质安全管理制度是否有限制移动存储介质使用的内容；

3) 应核查隔离区与移动介质使用管理记录，查看其是否记录隔离区域移动存储介质归档和使用等情况。

d) 单项判定

如果 1）3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对

象不符合或部分符合本单项测评指标要求。

9.2.4.4 设备维护管理

9.2.4.4.1 测评单元（L4-MMS1-10）

a) 测评指标

应对等级保护对象相关的各种设备（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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.4 a）

b) 测评对象

设备管理员、管理制度类文档。

c) 测评实施

1) 应访谈设备管理员，询问是否对各类设施、设备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) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.4.2 测评单元（L4-MMS1-11）

a) 测评指标

应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；（本条款引用自 GB/T 22239.1-20XX 8.2.4.4 b）

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

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

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

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.4.3 测评单元（L4-MMS1-12）

a) 测评指标

应确保信息处理设备必须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必须加密；（本条款引用自 GB/T 22239.1-20XX 8.2.4.4 c）

b) 测评对象

设备管理员、记录表单类文档。

c) 测评实施

1) 应访谈设备管理员，询问对带离机房的设备是否经过审批，由何人审批；

2) 应核查是否具有设备带离机房或办公地点的审批记录；

3) 应访谈设备管理员，询问含有重要数据的存储介质带出工作环境是否有加密措施，采取什么加密措施。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.4.4 测评单元（L4-MMS1-13）

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，确保该设备上的敏感数据和授权软件无法被恢复重用。（本条款引用自 GB/T 22239.1-20XX 8.2.4.4 d））

b) 测评对象

设备管理员。

c) 测评实施

应访谈设备管理员，询问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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.5 漏洞和风险管理

9.2.4.5.1 测评单元（L4-MMS1-14）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.5 a））

b) 测评对象

安全管理员、记录表单类文档。

c) 测评实施

1) 应访谈安全管理员，询问是否定期进行漏洞扫描，对发现的漏洞是否及时进行修补或评估可能的影响后进行修补；

2) 应核查漏洞扫描报告，查看内容是否描述了存在的漏洞、严重级别、原因分析和改进意见等方面。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.5.2　测评单元（L4-MMS1-15）

a)　测评指标

应按照国家标准定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。（本条款引用自 GB/T 22239.1-20XX 8.2.4.5 b））

b)　测评对象

安全管理员、记录表单类文档。

c)　测评实施

1)　应访谈安全管理员，询问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)　单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.5.3　测评单元（L4-MMS1-15）

a)　测评指标

应按照工控控制系统类别，建立控制设备漏洞台账或漏洞库，通过扫描机制或情报共享机制定期更新；通过漏洞台账或漏洞库，建立漏洞测试验证机制，定期对不影响生产环境的高危漏洞进行修补；对特别严重但又不能修复的漏洞，应建立补偿措施，弥补漏洞对工控系统带来的风险。

b)　测评对象

安全管理员、控制设备、漏洞台账、漏洞库系统。

c)　测评实施

1)　应访谈安全管理员，询问是否建设了漏洞台账或漏洞库；

2)　应核查漏洞台账或漏洞库内容是否更新；

3)　应核查是否对漏洞有测试验证机制；

4)　应核查是否对控制设备做过漏洞修复，提供相关变更文档；

5)　应核查存在高危漏洞的控制设备，询问是否采用了相关弥补措施。

d)　单项判定

如果 1）-5）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.6 网络和系统安全管理

9.2.4.6.1 测评单元（L4-MMS1-16）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.6 a））

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文档，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.6.2 测评单元（L4-MMS1-17）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.6 b））

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问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，查看是否对申请账户、建立账户、删除账户等进行控制。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.6.3 测评单元（L4-MMS1-18）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.6 c））

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，查看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、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.6.4 测评单元（L4-MMS1-19）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.6 d）

b) 测评对象

操作规程类文档。

c) 测评实施

应核查是否针对网络和系统制定了重要设备（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，查看是否明确操作步骤、维护记录、参数配置等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.6.5 测评单元（L4-MMS1-20）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.6 e）

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，查看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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.6.6 测评单元（L4-MMS1-21）

a) 测评指标

应严格控制变更性运维，经过审批后才可改变系统连接、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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.6 f）

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查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；

2) 应核查针对变更运维的操作过程记录；

3) 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。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.6.7 测评单元（L4-MMS1-22）

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系统进行操作，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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.6 g）

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查是否具有运维工具接入系统的审批记录；

2) 应核查针对使用运维工具的操作过程记录，审计日志是否可以更改，并核查审计日志记录；

3) 应访谈系统相关人员，询问使用运维工具结束后是否删除工具中的敏感数据。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.6.8 测评单元（L4-MMS1-23）

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；（本条款引用自 GB/T

22239.1-20XX 8.2.4.6 h）)

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应访谈系统相关人员，询问日常运维过程中是否存在远程运维；

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操作过程记录，查看审计日志是否可以更改；

4) 应访谈系统相关人员远程运维结束后是否立即关闭了接口或通道。

d) 单项判定

如果 1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.6.9 测评单元（L4-MMS1-24）

a) 测评指标

应保证所有与外部的连接均得到授权和批准， 应定期核查违反规定无线上网及其他违反网络安全策略的行为。（本条款引用自 GB/T 22239.1-20XX 8.2.5.6 j）)

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应访谈系统相关人员，询问外联种类（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，由何人/何部门批准；

2) 应核查是否具有外联授权的记录文件；

3) 应访谈系统相关人员，是否定期核查违规联网行为。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.7 恶意代码防范管理

9.2.4.7.1 测评单元（L4-MMS1-25）

a) 测评指标

应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码核查等；（本条款引用自 GB/T 22239.1-20XX 8.2.4.7 a）)

b) 测评对象

运维负责人。

c) 测评实施

应访谈运维负责人，询问是否采取告知方式提升员工的防病毒意识。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.7.2 测评单元（L4-MMS1-26）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.7 b））

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，查看是否明确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) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.7.3 测评单元（L4-MMS1-27）

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。（本条款引用自 GB/T 22239.1-20XX 8.2.4.7 c））

b) 测评对象

安全管理员、记录表单类文档。

c) 测评实施

1) 应访谈安全管理员，询问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。

3) 应定期采用技术手段测试验证恶意代码防范技术措施的有效性。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.7.4 测评单元（L1-MMS1-09）

a) 测评指标

在更新恶意代码库、木马库以及 IDS 规则库前，应首先在测试环境中测试通过，对隔离区域恶意代码更新应有专人负责，更新操作应离线进行，并保存更新记录。（新增）

b) **测评对象**

安全管理员、管理制度类文档、记录表单类文档。

c) **测评实施**

1) 应访谈系统管理员，询问是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行，是否保存更新记录。

2) 应核查恶意代码防范管理制度，查看是否在更新恶意代码库、木马库以及 IDS 规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行等内容。

3) 应核查更新记录，查看是否有更新前在测试环境中测试通过的记录，隔离区域恶意代码更新是否为专人负责，更新操作是否离线的记录。

d) **单项判定**

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.8 配置管理

9.2.4.8.1 测评单元（L4-MMS1-28）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.8 a））

b) **测评对象**

系统管理员。

c) **测评实施**

5) 应访谈系统管理员，询问是否对基本配置信息进行记录和保存。

6) 查看记录表单类文档是否对基本配置信息进行记录

d) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.8.2 测评单元（L4-MMS1-29）

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。（本条款引用自 GB/T 22239.1-20XX 8.2.4.8 b））

b) **测评对象**

系统管理员、记录表单类文档。

c) 测评实施

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，查看是否具有相应的申报审批程序。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.9 密码管理

9.2.4.9.1 测评单元（L4-MMS1-30）

a) 测评指标

应使用符合国家密码管理规定的密码技术和产品；（本条款引用自 GB/T 22239.1-20XX 8.2.4.9 a））

b) 测评对象

安全管理员。

c) 测评实施

应核查该是否获得有效的国家密码管理规定的检测报告或密码产品型号证书。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.10 变更管理

9.2.4.10.1 测评单元（L4-MMS1-32）

a) 测评指标

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；（本条款引用自 GB/T 22239.1-20XX 8.2.4.10 a））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应抽查变更方案，查看其是否包含变更类型、变更原因、变更过程、变更前评估等内容；

2) 应核查是否具有变更方案评审记录和变更过程记录文档。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.10.2 测评单元（L4-MMS1-33）

a) 测评指标

应建立变更的申报和审批控制程序，依据程序控制系统所有的变更，记录变更实施过程；（本条款引用自 GB/T 22239.1-20XX 8.2.4.10 b））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查变更控制的申报、审批程序，查看其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容；

2) 应核查变更实施过程的记录文档；

3) 应核查针对发生变更的事件进行影响分析。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.10.3 测评单元（L4-MMS1-34）

a) 测评指标

应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。（本条款引用自 GB/T 22239.1-20XX 8.2.4.10 c））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问变更失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练；

2) 应核查是否具有变更恢复演练记录；

3) 应核查变更失败恢复程序，查看其是否规定变更失败后的恢复流程。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.11 备份与恢复管理

9.2.4.11.1 测评单元（L4-MMS1-35）

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.11 a））

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别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) **单项判定**

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.11.2 **测评单元（L4-MMS1-36）**

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；（本条款引用自 GB/T 22239.1-20XX 8.2.4.11 b）

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，查看是否明确备份方式、频度、介质、保存期等内容。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.11.3 **测评单元（L4-MMS1-37）**

a) **测评指标**

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。（本条款引用自 GB/T 22239.1-20XX 8.2.4.11 c）

b) **测评对象**

管理制度类文档。

c) **测评实施**

应核查备份和恢复的策略，查看内容是否明确备份策略和恢复策略文档规范了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面。

d) **单项判定**

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.12 **安全事件处置**

9.2.4.12.1 **测评单元（L4-MMS1-38）**

a) **测评指标**

应报告所发现的安全弱点和可疑事件；（本条款引用自 GB/T 22239.1-20XX 8.2.4.12 a）

b) **测评对象**

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应进行及时报告；

2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.12.2 测评单元（L4-MMS1-39）

a) 测评指标

应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等；（本条款引用自 GB/T 22239.1-20XX 8.2.4.12 c）

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管理制度，查看内容是否明确了与安全事件有关的工作职责，各类事件的处置相应流程等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.12.3 测评单元（L4-MMS1-40）

a) 测评指标

应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；（本条款引用自 GB/T 22239.1-20XX 8.2.4.12 d）

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应核查安全事件报告和响应处置记录，查看其是否记录引发安全事件的系统弱点、不同安全事件发生的原因、处置过程、经验教训总结、补救措施等内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.12.4 测评单元（L4-MMS1-41）

a) 测评指标

对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。（本条款引用自 GB/T 22239.1-20XX 8.2.4.12 e）

b) 测评对象

记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，询问其不同安全事件的报告流程；

2) 应核查安全事件报告和处理程序文档，查看其是否根据不同安全事件制定不同的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.12.5 测评单元（L1-MMS1-13）

a) 测评指标

应建立工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件。（新增）

b) 测评对象

管理制度类文档、记录表单类文档。

c) 测评实施

1) 应核查安全事件报告和处置管理制度，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容；

2) 应核查安全事件报告和处理程序文档，查看是否含有工控控制系统联合防护和应急机制，负责处置跨部门工控控制系统安全事件的相关内容。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.13 应急预案管理

9.2.4.13.1 测评单元（L4-MMS1-42）

a) 测评指标

应规定统一的应急预案框架，并在此框架下制定不同事件的应急预案，包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；（本条款引用自 GB/T 22239.1-20XX 8.2.4.13 a）

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查应急预案框架，查看是否覆盖启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等方面；

2) 应核查是否具有根据应急预案框架制定不同事件的应急预案（如针对机房、系统、网络等各个层面）。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.13.2 测评单元（L4-MMS1-43）

a) 测评指标

应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；（本条款引用自 GB/T 22239.1-20XX 8.2.4.13 b）

b) 测评对象

管理制度类文档。

c) 测评实施

1) 应核查应急预案框架或相关文档，查看是否明确应急小组、相关设备及资金保障。

d) 单项判定

如果 1）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.13.3 测评单元（L4-MMS1-44）

a) 测评指标

应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；（本条款引用自 GB/T 22239.1-20XX 8.2.4.13 c）

b) 测评对象

运维负责人、记录表单类文档。

c) 测评实施

1) 应访谈运维负责人，是否定期对相关人员进行应急预案培训和演练；

2) 应核查应急预案培训记录，查看是否明确培训对象、培训内容、培训结果等；

3) 应核查应急预案演练记录，查看是否记录演练时间、主要操作内容、演练结果等。

d) 单项判定

如果 1）-3）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.13.4 测评单元（L4-MMS1-45）

a) 测评指标

应定期对原有的应急预案重新评估，修订完善。（本条款引用自 GB/T 22239.1-20XX 8.2.4.13 d）

b) 测评对象

记录表单类文档。

c) 测评实施

应核查应急预案修订记录，查看是否明确修订时间、修订内容等。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.14 外包运维管理

9.2.4.14.1 测评单元（L4-MMS1-46）

a) 测评指标

应确保外包运维服务商的选择符合国家的有关规定；（本条款引用自 GB/T 22239.1-20XX 8.2.4.14 a）

b) 测评对象

运维负责人。

c) 测评实施

1) 应访谈运维负责人，询问对等级保护对象进行运维是否有外包运维服务情况；

2) 应访谈运维负责人，询问对等级保护对象进行外包运维服务的服务单位是否符合国家有关规定。

d) 单项判定

如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

9.2.4.14.2 测评单元（L4-MMS1-47）

a) 测评指标

应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；（本条款引用自 GB/T 22239.1-20XX 8.2.4.14 b）

b) 测评对象

记录表单类文档。

c) 测评实施

应核查外包运维服务协议，查看协议内容是否明确约定外包运维的范围和工作内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.14.3 测评单元（L4-MMS1-48）

a) 测评指标

应确保选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；（本条款引用自 GB/T 22239.1-20XX 8.2.4.14 c））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查与外包运维服务商签订的协议中是否明确其具有等级保护要求的服务能力要求。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

9.2.4.14.4 测评单元（L4-MMS1-49）

a) 测评指标

应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。（本条款引用自 GB/T 22239.1-20XX 8.2.4.14 d））

b) 测评对象

记录表单类文档。

c) 测评实施

应核查外包运维服务协议，查看否明确安全要求，如是否包含可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等内容。

d) 单项判定

如果以上测评实施内容为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。

10 第五级单项测评

（略）。

11 整体测评

11.1 概述

国标 GB/T 22239.1-20XX 中的要求项，是为了对抗相应等级的威胁或具备相应等级的恢复能力而设计的，但由于安全措施的实现方式多种多样，安全技术也在不断发展，等级保护对象的运行使用单位所采用的安全措施和技术并不一定和 GB/T 22239.1-20XX 的要求项完

全一致。因此，需要从等级保护对象整体上是否能够对抗相应等级威胁的角度，对单项测评中的不符合项和部分符合项进行综合分析，分析这些不符合项或部分符合项是否会影响到等级保护对象整体安全保护能力的缺失。等级保护对象的整体测评就是在单项测评的基础上，评价等级保护对象的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。

等级保护对象整体测评应从安全控制点、安全控制点间和层面间等方面进行测评和综合安全分析，从而给出等级测评结论。整体测评包括安全控制点测评、安全控制点间测评和层面间测评。

安全控制点测评是指对单个控制点中所有要求项的符合程度进行分析和判定。

安全控制点间安全测评是指对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

层面间安全测评是指对同一区域内的两个或者两个以上不同层面安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

11.2 安全控制点测评

在单项测评完成后，如果该安全控制点下的所有要求项为符合，则该安全控制点符合，否则为不符合或部分符合。

11.3 安全控制点间测评

在单项测评完成后，如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合，应进行安全控制点间测评，应分析在同一层面内，是否存在其他安全控制点对该安全控制点具有补充作用（如物理访问控制和防盗窃、身份鉴别和访问控制等）。同时，分析是否存在其他的安全措施或技术与该要求项具有相似的安全功能。

根据测评分析结果，综合判断该安全控制点所对应的系统安全保护能力是否缺失，如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失，则该安全控制点的测评结论应调整为符合。

11.4 层面间测评

在单项测评完成后，如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合，应进行层面间安全测评，重点分析其他层面上功能相同或相似的安全控制点是否对该安全控制点存在补充作用（如应用和数据层加密与网络和通信层加密、设备和计算层与应用和数据层上的身份鉴别等），以及技术与管理上各层面的关联关系（如设备和计算安全与安全运维管理、应用和数据安全与安全运维管理等）。

根据测评分析结果，综合判断该安全控制点所对应的系统安全保护能力是否缺失，如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失，则该安全控制点的测评结论应调整为符合。

12 测评结论

12.1 各层面的测评结论

通过汇总安全控制点的测评结果，等级测评报告可以给出等级保护对象在安全技术和安全管理各个层面的等级测评结论。

在安全技术四个层面的等级测评结论中，通常物理和环境安全测评结论应重点给出等级保护对象在防范各种自然灾害和人为物理破坏方面安全控制措施的落实情况；网络和通信安全测评结论应重点给出等级保护对象在网络结构安全、通信传输、边界保护、访问控制、入侵防范、恶意代码防范、安全审计和集中管控等方面安全控制措施的落实情况；设备和计算安全测评结论应重点给出身份鉴别、访问控制、安全审计入侵防范、恶意代码防范和资源控制等方面安全控制措施的落实情况；应用和数据安全测评结论应重点给出身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人隐私保护等方面的安全控制措施的落实情况。

在安全管理四个方面的等级测评结论中，通常安全策略和管理制度应重点给出安全策略及管理制度体系的完备性和制修订的及时性等方面的测评结论；安全管理机构和人员应重点给出机构、岗位设置、人员配备、人员录用、离岗和培训等方面的测评结论；安全建设管理可重点给出系统定级与备案、安全方案设计、产品采购与使用、系统的测试验收和交付等方面的测评结论；安全运维管理可重点给出设备维护管理、网络与系统安全管理、漏洞和风险管理、恶意代码防范管理、安全事件处置以及应急预案管理等方面的测评结论。

不同等级等级保护对象在不同层面上会有不同的关注点，应反映到相应层面的等级测评结论中。

12.2 风险分析和评价

等级测评报告中应对整体测评之后单项测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法对单项测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，综合评价这些不符合项或部分符合项对等级保护对象造成的安全风险。

12.3 等级测评结论

等级测评报告应给出等级保护对象安全等级保护测评结论，确认等级保护对象达到相应等级保护要求的程度。

应结合各层面的测评结论和对单项测评结果的风险分析给出等级测评结论：

a) 如果单项测评结果中没有不符合项或部分符合项，则测评结论为“符合”；

b) 如果单项测评结果存在不符合项或部分符合项，但所产生的安全问题不会导致等级保护对象存在高等级安全风险，则测评结论为“基本符合”；

c) 如果单项测评结果存在不符合项或部分符合项，且所产生的安全问题导致等级保护

对象存在高等级安全风险，则测评结论为“不符合”。

附录 A
（资料性附录）
测评力度

A.1 概述

本部分在第5章到第8章描述了第一级到第四级等级保护对象的单项测评的具体测评实施过程要求。为了便于理解、对比不同测评方法的测评力度以及不同级别等级保护对象单项测评的测评力度增强情况，分别编制表 A.1 测评方法的测评力度描述和表 A.2 不同安全保护等级的等级保护对象的测评力度要求表。

A.2 测评力度描述

测评方法是测评人员依据测评内容选取的、实施特定测评操作的具体方法。本部分涉及访谈、核查和测试等三种基本测评方法。访谈、核查和测试等三种基本测评方法的测评力度可以通过其测评的深度和广度来描述，如表 A.1。

表 A.1 测评方法的测评力度

测评方法	深度	广度
访谈	访谈的深度体现在访谈过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要访谈只包含通用和高级的问题；充分访谈包含通用和高级的问题以及一些较为详细的问题；较全面访谈包含通用和高级的问题以及一些有难度和探索性的问题；全面访谈包含通用和高级的问题以及较多有难度和探索性的问题。	访谈的广度体现在访谈人员的构成和数量上。访谈覆盖不同类型的人员和同一类人的数量多少，体现出访谈的广度不同。
核查	核查的深度体现在核查过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要核查主要是对功能级上的文档、机制和活动，使用简要的评审、观察或核查以及核查列表和其他相似手段的简短测评；充分核查有详细的分析、观察和研究，除了功能级上的文档、机制和活动外，还适当需要一些总体/概要设计信息；较全面核查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和一些详细设计以及实现上的相关信息；全面核查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和详细设计以及实现上的相关信息。	核查的广度体现在核查对象的种类（文档、机制等）和数量上。核查覆盖不同类型的对象和同一类对象的数量多少，体现出对象的广度不同。
测试	测试的深度体现在执行的测试类型上：功能/性能测试和渗透测试。功能/性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入等级保护对象。	测试的广度体现在被测试的机制种类和数量上。测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出

		对象的广度不同。

A.3 等级测评力度

测评力度是在测评过程中实施测评工作的力度，反映测评的广度和深度，体现为测评工作的实际投入程度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多；测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的投入。投入越多，测评力度就越强，测评就越有保证。测评的广度和深度落实到访谈、核查和测试三种不同的测评方法上，能体现出测评实施过程中访谈、核查和测试的投入程度的不同。

网络安全等级保护要求不同安全保护等级的等级保护对象应具有不同的安全保护能力，满足相应等级的保护要求。为了检验不同安全保护等级的等级保护对象是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。第一级到第四级等级保护对象的测评力度反映在访谈、核查和测试等三种基本测评方法的测评广度和深度上，落实在不同单单项测评中具体的测评实施上。

为了进一步理解不同等级等级保护对象在测评力度上的不同，表 A.2 在表 A.1 的基础上，从测评对象数量和种类以及测评深度等方面详细分析了不同测评方法的测评力度在不同等级保护对象安全测评中的具体体现。

表 A.2 不同等级保护对象的测评力度要求

测评力度		等级保护对象安全保护等级			
		第一级	第二级	第三级	第四级
访谈	广度	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	简要	充分	较全面	全面
核查	广度	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	简要	充分	较全面	全面
测试	广度	测评对象在种类和数量、范围上抽样，种类和数量都较少，范围小	测评对象在种类和数量、范围上抽样，种类和数量都较多，范围大	测评对象在数量和范围上抽样，在种类上基本覆盖	测评对象在数量、范围上抽样，在种类上基本覆盖
	深度	功能测试/性能测试	功能测试/性能测试	功能测试/性能测试，渗透测试	功能测试/性能测试，渗透测试

从表 A.2 可以看到，对不同等级的等级保护对象进行等级测评时，选择的测评对象的种

类和数量是不同的，随着等级保护对象安全保护等级的增高，抽查的测评对象的种类和数量也随之增加。

对不同安全保护等级等级保护对象进行等级测评时，实际抽查测评对象的种类和数量，应当达到表 A.2 的要求，以满足相应等级的测评力度要求。在具体测评对象选择工作过程中，可参照遵循以下原则：

a） 完整性原则，选择的设备、措施等应能满足相应等级的测评力度要求；

b） 重要性原则，应抽查重要的服务器、数据库和网络设备等；

c） 安全性原则，应抽查对外暴露的网络边界；

d） 共享性原则，应抽查共享设备和数据交换平台/设备；

e） 代表性原则，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统的类型。

f） 稳定性原则，应在确保工控控制系统稳定运行的的前提下，分时段优先抽查相应的备用或测试设备进行等级测评。

附录 B

（规范性附录）

测评单元编号说明

B.1 测评指标编码规则

测评单元编号为三组数据，格式为 XX-XXXX-XX，各组含义和编码规则如下：

第 1 组由两位组成，第 1 位为字母 L，第 2 位为数字，其中数字 1 为第一级，2 为第二级，3 为第三级，4 为第四级，5 为第五级。

第 2 组由 4 位组成，前 3 位为字母，第 3 位为数字。字母代表层面：PES 为物理和环境安全， NCS 为网络和通信安全，ECS 为设备和计算安全，ADS 为应用和数据安全，PSS 为安全策略和管理制度，ORS 为安全管理机构和人员，CMS 为安全建设管理，MMS 为安全运维管理。数字代表标准分册：1 为第一分册，2 为第二分册，3 为第三分册，4 为第四分册，5 为第五分册，6 为第六分册。

第 3 组由 2 位数字组成，按层面对基本要求中的要求项进行顺序编号。

示例：测评单元编号为 L1-PES1-01，代表源自基本要求第 1 部分的第一级物理和环境安全类的第 1 个指标。

B.2 专用缩略语

物理和环境安全为 PES（Physical and Enviornment Security）

网络和通信安全 NCS（Network and Communication Security）

设备和计算安全 ECS（Equipment and Computing Security）

应用和数据安全 ADS（Application and Data Security）

安全策略和管理制度 PSS（Policy and System Security）

安全管理机构和人员 ORS（Organization and Resource Security）

安全建设管理 CMS（Construction Management Security）

安全运维管理 MMS（Maintenance Management Security）

附录 C

（资料性附录）

测评要求与设计要求对应表

适用范围	功能要求	设计要求	测评要求
安全计算环境	用户身份鉴别	应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可替代的，并对鉴别数据进行保密性和完整性保护。	测评单元（L4-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施；应核查用户列表，查看所有用户身份标识是否具有唯一性。 测评单元（L4- ECS1-02） 应核查用户配置或访谈系统管理员，查看是否存在空密码用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L4-ECS1-05） 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别； 测评单元（L4-ADS1-26） 应核查开发文档，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码技术或加解密技术保证完整性；应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
	自主访问控制	应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。	测评单元（L4-ECS1-06） 应核查或访谈用户账户和权限设置情况；应核查是否已禁用或限制匿名、默认账户的访问权限。 测评单元（L4-ADS1-11） 应核查是否由管理用户负责配置访问控制策略；应核查授权主体是否依据安全策略配置了主体对客体的访问规则；应测试用户是否有可越权访问情形。 测评单元（L4-ADS1-12）

			应核查访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级。
	标记与强制访问控制	在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记，将强制访问控制扩展到所有主体与客体；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。	测评单元（L4-ADS1-13） 应核查是否依据安全策略对所有主体和客体设置了安全标记； 应测试是否依据安全标记和强制访问控制规则确定主体对客体的访问。
	系统安全审计	应记录系统相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警，终止违例进程等；确保审计记录不被破坏或非授权访问以及防止审计记录丢失等。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。	测评单元（L4-NCS1-25） 应核查是否开启了日志记录或安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行审计。 测评单元（L4-NCS1-26） 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。 测评单元（L4-NCS1-27） 应核查是否采取了保护措施对审计记录进行保护；应核查审计记录的备份机制和备份策略。 测评单元（L4-NCS1-34） 应核查网络中是否在网络边界及关键节点，部署集中安全管控系统，并通过声光方式实时报警；应核查集中安全管控系统的检测范围是否能够覆盖网络所有关键路径。
	用户数据	应采用密码等技术支持的完	测评单元（L4-ADS1-26）

	完整性保护	整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。	应核查开发文档，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码技术或加解密技术保证完整性；应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。 测评单元（L4-ADS1-27） 应核查开发文档，是否采用校验码技术或加解密技术保证重要配置数据、重要业务数据在存储过程中的完整性；应测试在存储过程中对重要配置数据、重要业务数据进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。 测评单元（L4-ADS1-28） 应核查系统开发文档，查看是否为重要业务数据传输提供专用通信协议或安全通信协议保证数据完整性。
	用户数据保密性保护	采用密码等技术支持的保密性保护机制，对在安全计算环境中的用户数据进行保密性保护。	测评单元（L4-ADS1-29） 应核查开发文档，重要管理数据、重要业务数据在传输过程中是否采用加解密技术保证保密性；应通过嗅探等方式抓取传输过程中的数据包，查看重要管理数据、重要业务数据在传输过程中是否进行了加密处理。 测评单元（L4-ADS1-30） 应核查是否采用加解密技术保证重要配置数据、重要业务数据在存储过程中的保密性。 测评单元（L4-ADS1-31） 应核查系统开发文档，查看是否为重要业务数据传输提供专用通信协议或安全通信协议保证数据保密性。
	客体安全重用	应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体	测评单元（L4-ADS1-37） 应核查相关配置信息或访谈应用系统管理员，用户的鉴别信息所在的存储空间被释放

		资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。	或重新分配前是否得到完全清除。 测评单元（L4-ADS1-38） 应核查相关配置信息或访谈应用系统管理员，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除。
	程序可信执行保护	应构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。	测评单元（L3-ECS1-23） 应查看防恶意代码工具的安装和使用情况，或查看是否采用可信计算技术建立从系统到应用的信任链；应访谈管理员，查看是否有保护重要系统程序或文件完整性的措施；应当检测到程序或文件受到破坏后，是否具备恢复的措施。
	网络可信连接保护	应采用具有网络可信连接保护功能的系统软件或具有相应功能的信息技术产品，在设备连接网络时，对源和目标进行平台身份鉴别、平台完整性校验、数据传输的保密性和完整性保护等。	测评单元（L4-NCS1-15） 应访谈网络管理员是否采用技术措施对连接到内部网络的设备进行可信验证。
	配置可信核查	应将系统的安全配置信息形成基准库，实时监控或定期核查配置信息的修改行为，及时修复和基准库中内容不符的配置信息。	测评单元（L4-ADS1-27） 应核查开发文档，是否采用校验码技术或加解密技术保证重要配置数据、重要业务数据在存储过程中的完整性； 应测试在存储过程中对重要配置数据、重要业务数据进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
安全区域边界	区域边界访问控制	应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。	测评单元（L4-NCS1-16） 应核查在网络边界或区域之间是否部署网络访问控制设备，是否启用访问控制策略；应核查设备的访问控制策略，确保手工配置或设备默认的最后一条策略为禁止所有网络通信。
	区域边界包过滤	应根据区域边界安全控制策略，通过核查数据包的源地址、目	测评单元（L3-NCS1-14） 应核查访问控制设备，查看是否对源地址、

		的地址、传输层协议、请求的服务等，确定是否允许该数据包进出受保护的区域边界。	目的地址、源端口、目的端口和协议等进行核查。 测评单元（L3-NCS1-15） 应核查访问控制策略查看是否有明确的源地址、目的地址、源端口、目的端口和协议，访问控制粒度是否为端口级。
	区域边界安全审计	应在安全区域边界设置审计机制，通过安全管理中心集中管理，对确认的违规行为及时报警并做出相应处置。	测评单元（L4-NCS1-25） 应核查是否开启了日志记录或安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行审计。 测评单元（L4-NCS1-26） 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。
	区域边界完整性保护	应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。	测评单元（L4-NCS1-12） 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断； 测评单元（L4-NCS1-13） 应核查是否采用技术措施防止非法外联行为，进行核查并有效阻断。
安全通信网络	通信网络安全审计	应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警，且做出相应处置。	测评单元（L4-NCS1-25） 应核查是否开启了日志记录或安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行审计。 测评单元（L4-NCS1-26） 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。
	通信网络数据传输完整性保	应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完	测评单元（L4-NCS1-07） 应访谈安全管理员，询问是否具有在数据传输过程中保护其完整性的措施，具体措施是

	护	整性被破坏时进行恢复。	什么；应核查设计/验收文档，查看其是否有关于保护通信完整性的说明。
	通信网络数据传输保密性保护	采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。	测评单元（L4-NCS1-08） 应访谈安全管理员，询问是否具有在通信过程中是否采取保密措施，具体措施有哪些； 应测试在通信过程中是否对敏感信息字段或整个报文进行加密。
	通信网络可信接入保护	应采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。	测评单元（L4-NCS1-12） 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断； 应核查所有路由器和交换机闲置端口是否均已关闭。
安全管理中心	系统管理	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，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和异地灾难备份与恢复等。 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。	测评单元（L4-MMS1-16） 应核查网络和系统安全管理文档，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L4-MMS1-17） 应访谈系统运维负责人，询问是否指定专门的部门或人员进行账户管理；应核查申请账户、建立账户、删除账户的审批记录或流程。 测评单元（L4-MMS1-18） 应核查网络和系统安全管理制度，查看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、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。 测评单元（L4-ADS1-14） 应核查是否提供并开启了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进

			行审计。
	安全管理	应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略，并确保标记、授权和安全策略的数据完整性。 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，并进行审计。	测评单元（L4-ORS1-04） 应访谈信息安全主管，确认各岗位人员配备情况；应核查人员配备文档，查看各岗位人员配备情况。 测评单元（L4-ORS1-05） 应核查人员配备文档，查看是否配备了专职安全管理员。 测评单元（L4-MMS1-18） 应核查网络和系统安全管理制度，查看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、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。 测评单元（L4-ADS1-14） 应核查是否提供并开启了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行审计。
	审计管理	应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。 应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。	测评单元（L4-ORS1-04） 应访谈信息安全主管，确认各岗位人员配备情况；应核查人员配备文档，查看各岗位人员配备情况。 测评单元（L4-MMS1-16） 应核查网络和系统安全管理文档，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L4-ADS1-14） 应核查是否提供并开启了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查

			是否对重要的用户行为和重要安全事件进行审计。

参考文献

[1] GB/T 20269-2006 信息安全技术 信息系统安全管理要求

[2] GB/T 20270-2006 信息安全技术 网络基础安全技术要求

[3] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

[4] GB/T 20272-2006 信息安全技术 操作系统安全技术要求

[5] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求

[6] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求

[7] GB/T 18336-2008 信息安全技术 信息技术安全性评估准则

[8] Information technology-Security techniques - Information security management systems requirements（ISO/IEC 27001：2005）

[9] Information technology-Security techniques - Code of practice forinformation security management（ISO/IEC 17799：2005）