ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28448—2019
代替 GB/T 28448—2012

信息安全技术
网络安全等级保护测评要求

Information security technology—
Evaluation requirement for classified protection of cybersecurity

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 28448—2012《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，主要变化如下：

——将标准名称变更为《信息安全技术　网络安全等级保护测评要求》；

——每个级别增加了云计算安全测评扩展要求、移动互联安全测评扩展要求、物联网安全测评扩展要求和工业控制系统安全测评扩展要求等内容；

——增加了等级测评、测评对象、云服务商和云服务客户等相关术语和定义（见第 3 章，2012 年版的第 3 章）；

——将针对控制点的单元测评细化调整为针对要求项的单项测评，删除了“测评框架”（见 2012 年版的 4.1）和“等级测评内容”（见 2012 年版的 4.2）；

——增加了大数据可参考安全评估方法（见附录 B）和测评单元编号说明（见附录 C）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：公安部第三研究所（公安部信息安全等级保护评估中心）、中国电子技术标准化研究院、国家信息中心、中国科学院信息工程研究所（信息安全国家重点实验室）、北京大学、新华三技术有限公司、成都科来软件有限公司、中国移动通信集团有限公司、北京鼎普科技股份有限公司、北京微步在线科技有限公司、北京梆梆安全科技有限公司、北京迅达云成科技有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、公安部第一研究所、北京信息安全测评中心、国家能源局信息中心（电力行业信息安全等级保护测评中心）、全球能源互联网研究院、北京卓识网安技术股份有限公司、中国电力科学研究院、南京南瑞集团公司、国电南京自动化股份有限公司、南方电网科学研究院、中国电子信息产业集团公司第六研究所、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、启明星辰信息技术集团股份有限公司、北京烽云互联科技有限公司、华普科工（北京）有限公司。

本标准主要起草人：陈广勇、李明、黎水林、马力、曲洁、于东升、艾春迪、郭启全、葛波蔚、祝国邦、陆磊、张宇翔、毕马宁、沙淼淼、李升、胡红升、陈雪鸿、袁静、章恒、张益、毛澍、王斌、尹湘培、王勇、高亚楠、焦安春、赵劲涛、于俊杰、徐衍龙、马晓波、江雷、黄顺京、朱建兴、苏艳芳、禄凯、何申、霍珊珊、于运涛、陈震、任卫红、孙惠平、万晓兰、马红霞、薛锋、赵林林、刘金刚、胡越宁、周晓雪、李亚军、杨洪起、孟召瑞、李飞、王江波、阚志刚、刘健、陶源、李秋香、许凤凯、王绍杰、李晨旸、李凌、朱世顺、张五一、陈华军、张洁昕、张彪、李汪蔚、王雪、蔡学琳、胡娟、刘静、周峰、郝鑫、马闽、段伟恒。

本标准所代替标准的历次版本发布情况为：

——GB/T 28448—2012。

引　言

为了配合《中华人民共和国网络安全法》的实施，同时适应云计算、移动互联、物联网和工业控制等新技术、新应用情况下网络安全等级保护工作的开展，需对 GB/T 28448—2012 进行修订。同时，作为测评指标进行引用的 GB/T 22239—2008 也启动了修订工作。修订的思路和方法依据 GB/T 22239 调整的内容，针对共性安全保护需求提出安全测评通用要求，针对云计算、移动互联、物联网和工业控制等新技术、新应用领域的个性安全保护需求提出安全测评扩展要求，形成新的《信息安全技术　网络安全等级保护测评要求》标准。

本标准是网络安全等级保护相关系列标准之一。

与本标准相关的标准包括：

——GB/T 25058　信息安全技术　信息系统安全等级保护实施指南；

——GB/T 22240　信息安全技术　信息系统安全等级保护定级指南；

——GB/T 22239　信息安全技术　网络安全等级保护基本要求；

——GB/T 25070　信息安全技术　网络安全等级保护安全设计技术要求；

——GB/T 28449　信息安全技术　网络安全等级保护测评过程指南。

信息安全技术
网络安全等级保护测评要求

1 范围

本标准规定了不同级别的等级保护对象的安全测评通用要求和安全测评扩展要求。

本标准适用于安全测评服务机构、等级保护对象的运营使用单位及主管部门对等级保护对象的安全状况进行安全测评并提供指南，也适用于网络安全职能部门进行网络安全等级保护监督检查时参考使用。

注：第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全测评要求，所以不在本标准中进行描述。

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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

3 术语和定义

GB 17859—1999、GB/T 25069、GB/T 22239—2019、GB/T 25070—2019、GB/T 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 31167—2014 和 GB/T 31168—2014 中的一些术语和定义。

3.1

访谈 interview

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 examine

测评人员通过对测评对象(如制度文档、各类设备及相关安全配置等)进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

3.3

测试 test

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

评估　evaluate

对测评对象可能存在的威胁及其可能产生的后果进行综合评价和预测的过程。

3.5

测评对象　target of testing and evaluation

等级测评过程中不同测评方法作用的对象，主要涉及相关配套制度文档、设备设施及人员等。

3.6

等级测评　testing and evaluation for classified cybersecurity protection

测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密的网络安全等级保护状况进行检测评估的活动。

3.7

云服务商　cloud service provider

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。

[GB/T 31167—2014，定义 3.3]

3.8

云服务客户　cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31168—2014，定义 3.4]

3.9

虚拟机监视器　hypervisor

运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

3.10

宿主机　host machine

运行虚拟机监视器的物理服务器。

4　缩略语

下列缩略语适用于本文件。

AP：无线访问接入点(Wireless Access Point)

APT：高级持续性威胁(Advanced Persistent Threat)

DDoS：分布式拒绝服务(Distributed Denial of Service)

SSID：服务集标识(Service Set Identifier)

WEP：有线等效加密(Wired Equivalent Privacy)

WiFi：无线保真(Wireless Fidelity)

WPS：WiFi 保护设置(Wi-Fi Protected Setup)

5　等级测评概述

5.1　等级测评方法

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见

GB/T 28449—2018。

本标准中针对每一个要求项的测评就构成一个单项测评，针对某个要求项的所有具体测评内容构成测评实施。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、核查和测试三种测评方法，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—2019及GB/T 25070—2019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—2019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。

根据调研结果，分析等级保护对象的业务流程和数据流，确定测评工作的范围。结合等级保护对象的安全级别，综合分析系统中各个设备和组件的功能和特性，从等级保护对象构成组件的重要性、安全性、共享性、全面性和恰当性等几方面属性确定技术层面的测评对象，并将与其相关的人员及管理文档确定为管理层面的测评对象。测评对象可以根据类别加以描述，包括机房、业务应用软件、主机操作系统、数据库管理系统、网络互联设备、安全设备、访谈人员及安全管理文档等。

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）。安全保护等级较高的测评实施应选择覆盖面更广的测评对象和更强的测评手段，可以获得可信度更高的测评证据，测评力度的具体描述参见附录A。

每个级别测评要求都包括安全测评通用要求、云计算安全测评扩展要求、移动互联安全测评扩展要求、物联网安全测评扩展要求和工业控制系统安全测评扩展要求5个部分。大数据可参考安全评估方法参见附录B。

5.2 单项测评和整体测评

等级测评包括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。本标准中单项测评由测评指标、测评对象、测评实施和单元判定结果构成。为方便使用针对每个测评单元进行编号，具体描述见附录C。

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两个角度评判。

6 第一级测评要求

6.1 安全测评通用要求

6.1.1 安全物理环境

6.1.1.1 物理访问控制

6.1.1.1.1 测评单元（L1-PES1-01）

该测评单元包括以下要求：

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

b） 测评对象：机房电子门禁系统和值守记录。

c） 测评实施：应核查是否安排专人值守或配置电子门禁系统。

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

6.1.1.2 防盗窃和防破坏

6.1.1.2.1 测评单元(L1-PES1-02)

该测评单元包括以下要求：

a) 测评指标：应将设备或主要部件进行固定，并设置明显的不易除去的标识。

b) 测评对象：机房设备或主要部件。

c) 测评实施包括以下内容：

1) 应核查机房内设备或主要部件是否固定；

2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标识。

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

6.1.1.3 防雷击

6.1.1.3.1 测评单元(L1-PES1-03)

该测评单元包括以下要求：

a) 测评指标：应将各类机柜、设施和设备等通过接地系统安全接地。

b) 测评对象：机房。

c) 测评实施：应核查机房内机柜、设施和设备等是否进行接地处理。

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

6.1.1.4 防火

6.1.1.4.1 测评单元(L1-PES1-04)

该测评单元包括以下要求：

a) 测评指标：机房应设置灭火设备。

b) 测评对象：机房灭火设备。

c) 测评实施：应核查机房内是否配备灭火设备。

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

6.1.1.5 防水和防潮

6.1.1.5.1 测评单元(L1-PES1-05)

该测评单元包括以下要求：

a) 测评指标：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b) 测评对象：机房。

c) 测评实施：应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施。

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

6.1.1.6 温湿度控制

6.1.1.6.1 测评单元(L1-PES1-06)

该测评单元包括以下要求：

a) 测评指标：应设置必要的温湿度调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

b) 测评对象：机房温湿度控制设施。

c) 测评实施包括以下内容：

1) 应核查机房内是否配备了温湿度调节设施；

2) 应核查温湿度是否在设备运行所允许的范围之内。

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

6.1.1.7 电力供应

6.1.1.7.1 测评单元(L1-PES1-07)

该测评单元包括以下要求：

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。

b) 测评对象：机房供电设施。

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

6.1.2 安全通信网络

6.1.2.1 通信传输

6.1.2.1.1 测评单元(L1-CNS1-01)

该测评单元包括以下要求：

a) 测评指标：应采用校验技术保证通信过程中数据的完整性。

b) 测评对象：提供校验技术功能的设备或组件。

c) 测评实施：应核查是否在数据传输过程中使用校验技术来保护其完整性。

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

6.1.2.2 可信验证

6.1.2.2.1 测评单元(L1-CNS1-02)

该测评单元包括以下要求：

a) 测评指标：可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

b) 测评对象：提供可信验证的设备或组件。

c) 测评实施包括以下内容：

1) 应核查是否基于可信根对通信设备的系统引导程序、系统程序等进行可信验证；

2） 应核查当检测到通信设备的可信性受到破坏后是否进行报警。

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

6.1.3 安全区域边界

6.1.3.1 边界防护

6.1.3.1.1 测评单元（L1-ABS1-01）

该测评单元包括以下要求：

a） 测评指标：应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

b） 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c） 测评实施包括以下内容：

1） 应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，指定端口是否配置并启用了安全策略；

3） 应采用其他技术手段（如非法无线网络设备定位、核查设备配置信息等）核查是否不存在其他未受控端口进行跨越边界的网络通信。

d） 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.2 访问控制

6.1.3.2.1 测评单元（L1-ABS1-02）

该测评单元包括以下要求：

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。

b） 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c） 测评实施包括以下内容：

1） 应核查在网络边界是否部署访问控制设备并启用访问控制策略；

2） 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。

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

6.1.3.2.2 测评单元（L1-ABS1-03）

该测评单元包括以下要求：

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。

b） 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c） 测评实施包括以下内容：

1） 应核查是否不存在多余或无效的访问控制策略；

2） 应核查不同的访问控制策略之间的逻辑关系及前后排列顺序是否合理。

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

6.1.3.2.3 测评单元（L1-ABS1-04）

该测评单元包括以下要求：

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检查，以允许/拒绝数据包进出。

b） 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c） 测评实施：应核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数。

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

6.1.3.3 可信验证

6.1.3.3.1 测评单元（L1-ABS1-05）

该测评单元包括以下要求：

a） 测评指标：可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

b） 测评对象：提供可信验证的设备或组件。

c） 测评实施包括以下内容：

1） 应核查是否基于可信根对边界设备的系统引导程序、系统程序等进行可信验证；

2） 应核查当检测到边界设备的可信性受到破坏后是否进行报警。

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

6.1.4 安全计算环境

6.1.4.1 身份鉴别

6.1.4.1.1 测评单元（L1-CES1-01）

该测评单元包括以下要求：

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。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c） 测评实施包括以下内容：

1） 应核查用户在登录时是否采用了身份鉴别措施；

2） 应核查用户列表确认用户身份标识是否具有唯一性；

3） 应核查用户配置信息是否不存在空口令用户；

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) 单元判定：如果 1)和 4)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.1.2 测评单元(L1-CES1-02)

该测评单元包括以下要求：

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。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

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功能，非法登录达到一定次数后采取特定动作，如账户锁定等；

3) 应核查是否配置并启用了登录连接超时及自动退出功能。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.2 访问控制

6.1.4.2.1 测评单元(L1-CES1-03)

该测评单元包括以下要求：

a) 测评指标：应对登录的用户分配账户和权限。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查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) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.2.2 测评单元(L1-CES1-04)

该测评单元包括以下要求：

a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施包括以下内容：

1） 应核查是否已经重命名默认账户或默认账户已被删除；

2） 应核查是否已修改默认账户的默认口令。

d） 单元判定：如果 1)或 2)为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.2.3 测评单元（L1-CES1-05）

该测评单元包括以下要求：

a） 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c） 测评实施包括以下内容：

1） 应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应；

2） 应核查多余的、过期的账户是否被删除或停用。

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

6.1.4.3 入侵防范

6.1.4.3.1 测评单元（L1-CES1-06）

该测评单元包括以下要求：

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。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。

c） 测评实施包括以下内容：

1） 应核查是否遵循最小安装原则；

2） 应确认是否未安装非必要的组件和应用程序。

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

6.1.4.3.2 测评单元（L1-CES1-07）

该测评单元包括以下要求：

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。

b） 测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等。

c） 测评实施包括以下内容：

1） 应核查是否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） 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.4 恶意代码防范

6.1.4.4.1 测评单元(L1-CES1-08)

该测评单元包括以下要求：

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。

b) 测评对象：终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)和移动终端等。

c) 测评实施内容包括以下：

1) 应核查是否安装了防恶意代码软件或相应功能的软件；

2) 应核查是否定期进行升级和更新防恶意代码库。

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

6.1.4.5 可信验证

6.1.4.5.1 测评单元(L1-CES1-09)

该测评单元包括以下要求：

a) 测评指标：可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

b) 测评对象：提供可信验证的设备或组件。

c) 测评实施包括以下内容：

1) 应核查是否基于可信根对计算设备的系统引导程序、系统程序等进行可信验证；

2) 应核查当检测到计算设备的可信性受到破坏后是否进行报警。

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

6.1.4.6 数据完整性

6.1.4.6.1 测评单元(L1-CES1-10)

该测评单元包括以下要求：

a) 测评指标：应采用校验技术保证重要数据在传输过程中的完整性。

b) 测评对象：业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

c) 测评实施：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技术或密码技术保证完整性。

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

6.1.4.7 数据备份恢复

6.1.4.7.1 测评单元(L1-CES1-11)

该测评单元包括以下要求：

a) 测评指标：应提供重要数据的本地数据备份与恢复功能。

b) 测评对象：配置数据和业务数据。

c) 测评实施包括以下内容：

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，是否能够进行正常的数据恢复。

d） 单元判定：如果1）～4）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.5 安全管理制度

6.1.5.1 管理制度

6.1.5.1.1 测评单元（L1-PSS1-01）

该测评单元包括以下要求：

a） 测评指标：应建立日常管理活动中常用的安全管理制度。
b） 测评对象：安全管理制度类文档。
c） 测评实施：应核查各项安全管理制度是否覆盖日常管理活动中的管理内容。
d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.6 安全管理机构

6.1.6.1 岗位设置

6.1.6.1.1 测评单元（L1-ORS1-01）

该测评单元包括以下要求：

a） 测评指标：应设立系统管理员等岗位，并定义各个工作岗位的职责。
b） 测评对象：信息/网络安全主管和管理制度类文档。
c） 测评实施包括以下内容：
1） 应访谈信息/网络安全主管是否进行了系统管理员等岗位的划分；
2） 应核查岗位职责文档是否明确了各岗位职责。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.6.2 人员配备

6.1.6.2.1 测评单元（L1-ORS1-02）

该测评单元包括以下要求：

a） 测评指标：应配备一定数量的系统管理员。
b） 测评对象：信息/网络安全主管和记录表单类文档。
c） 测评实施包括以下内容：
1） 应访谈信息/网络安全主管是否配备一定数量的系统管理员；
2） 应核查人员配备文档是否有各岗位人员配备情况。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.6.3 授权和审批

6.1.6.3.1 测评单元(L1-ORS1-03)

该测评单元包括以下要求：

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

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查部门职责文档是否明确各部门审批事项；

2) 应核查岗位职责文档是否明确各岗位审批事项。

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

6.1.7 安全管理人员

6.1.7.1 人员录用

6.1.7.1.1 测评单元(L1-HRS1-01)

该测评单元包括以下要求：

a) 测评指标：应指定或授权专门的部门或人员负责人员录用。

b) 测评对象：信息/网络安全主管。

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

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

6.1.7.2 人员离岗

6.1.7.2.1 测评单元(L1-HRS1-02)

该测评单元包括以下要求：

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

b) 测评对象：记录表单类文档。

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

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

6.1.7.3 安全意识教育和培训

6.1.7.3.1 测评单元(L1-HRS1-03)

该测评单元包括以下要求：

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

b) 测评对象：管理制度类文档。

c) 测评实施包括以下内容：

1) 应核查安全意识教育及岗位技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容；
2) 应核查安全责任和惩戒措施管理文档或培训文档是否包含具体的安全责任和惩戒措施。

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

6.1.7.4 外部人员访问管理

6.1.7.4.1 测评单元(L1-HRS1-04)

该测评单元包括以下要求：

a) 测评指标：应保证在外部人员访问受控区域前得到授权或审批。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围(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是否具有批准人允许访问的批准签字等。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8 安全建设管理

6.1.8.1 定级和备案

6.1.8.1.1 测评单元(L1-CMS1-01)

该测评单元包括以下要求：

a) 测评指标：应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.8.2 安全方案设计

6.1.8.2.1 测评单元(L1-CMS1-02)

该测评单元包括以下要求：

a) 测评指标：应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。
b) 测评对象：安全规划设计类文档。
c) 测评实施：应核查安全设计文档是否根据安全保护等级选择安全措施，是否根据安全需求调整安全措施。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。