ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0072—2020
代替 JR/T 0072—2012

金融行业网络安全等级保护测评指南

Testing and evaluation guidelines for classified protection of cybersecurity of financial industry

2020－11－11 发布　　2020－11－11 实施

中国人民银行　发布

目　　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 5
5 等级测评概述 5
5.1 等级测评方法 5
5.2 单项测评和整体测评 5
6 第二级测评要求 6
6.1 安全测评通用要求 6
6.2 云计算安全测评扩展要求 54
6.3 移动互联安全测评扩展要求 61
6.4 物联网安全测评扩展要求 64
7 第三级测评要求 70
7.1 安全测评通用要求 70
7.2 云计算安全测评扩展要求 149
7.3 移动互联安全测评扩展要求 165
7.4 物联网安全测评扩展要求 171
8 第四级测评要求 181
8.1 安全测评通用要求 181
8.2 云计算安全测评扩展要求 267
8.3 移动互联安全测评扩展要求 288
8.4 物联网安全测评扩展要求 295
9 整体测评 305
9.1 概述 305
9.2 安全控制点测评 305
9.3 安全控制点间测评 305
9.4 区域间测评 305
10 测评结论 305
10.1 风险分析和评价 305
10.2 等级测评结论 306
附录 A（资料性附录）测评力度 307
附录 B（资料性附录）大数据可参考安全评估方法 309
附录 C（规范性附录）测评单元编号说明 330
参考文献 331

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替JR/T 0072—2012《金融行业信息系统信息安全等级保护测评指南》，与JR/T 0072—2012相比，主要技术变化如下：

——修改了“等级测评概述”（见第5章，2012年版第3章）；

——删除了“等级测评过程”（见2012年版第4章）；

——删除了“测评准备”（见2012年版第5章）；

——删除了“测评方案”（见2012年版第6章）；

——修改了“第二级测评要求”的“安全测评通用要求”中“安全物理环境”“安全通信网络”“安全区域边界”“安全计算环境”“安全管理中心”“安全管理制度”“安全管理机构”“安全管理人员”“安全建设管理”“安全运维管理”相关要求项（见6.1，2012年版7.1.1）；

——增加了“第二级测评要求”中“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”（见第6章）；

——修改了“第三级测评要求”的“安全测评通用要求”中“安全物理环境”“安全通信网络”“安全区域边界”“安全计算环境”“安全管理中心”“安全管理制度”“安全管理机构”“安全管理人员”“安全建设管理”“安全运维管理”相关要求项（见7.1，2012年版7.1.2）；

——增加了“第三级测评要求”中“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”（见第7章）；

——修改了“第四级测评要求”的“安全测评通用要求”中“安全物理环境”“安全通信网络”“安全区域边界”“安全计算环境”“安全管理中心”“安全管理制度”“安全管理机构”“安全管理人员”“安全建设管理”“安全运维管理”相关要求项（见8.1，2012年版7.1.3）；

——增加了“第四级测评要求”中“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”（见第8章）；

——删除了“分析与报告编制”（见2012年版第8章）；

——删除了“现场单元测评检查表”（见2012年版附录A）；

——增加了“测评力度”（见附录A）；

——增加了“大数据可参考安全评估方法”，对金融行业大数据平台提出分级要求（见附录B）；

——增加了“测评单元编号说明”（见附录C）。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、中国银行保险监督管理委员会统计信息与风险监测部、中国金融电子化公司、北京中金国盛认证有限公司、银行卡检测中心、中国平安保险（集团）股份有限公司、北京天融信网络安全技术有限公司、华为技术有限公司。

本标准主要起草人：李伟、陈立吾、沈筱彦、车珍、眷新、夏磊、方怡、张海燕、唐辉、李凡、王海涛、张璐、潘丽扬、邓昊、侯漫丽、孙国栋、刘文娟、赵方萌、马成龙、杜巍、崔莹、陈雪峰、渠韶光、高强裔、李博文、李金华、金朝、任勇强、岳源、朱京城、赵江、于惊涛、胡珊、谢虹、杨剑、李建彬、于国强、肖松、白阳、张宇、赵华。

本标准所代替标准的历次版本发布情况为：

——JR/T 0072—2012。

引　言

网络安全等级保护是国家网络安全保障工作的一项基本制度，金融行业重要系统关系到国计民生，是国家网络安全重点保护对象，因此需要一系列适合金融行业的等级保护标准体系作为支撑，以规范和指导金融行业等级保护工作的实施。随着云计算、移动互联、物联网、大数据等新技术的广泛应用，金融机构正根据自身发展的需要，持续推进IT架构的转型。为适应新技术、新应用和新架构情况下金融行业网络安全等级保护工作的开展，对JR/T 0071进行了修订，同时，作为测评指标进行引用的JR/T 0072也启动了修订工作。修订后的JR/T 0072依据JR/T 0071基本要求调整的内容，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。

金融行业网络安全等级保护测评指南

1 范围

本标准规定了金融行业对第二级、第三级和第四级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。

本标准适用于指导金融机构、测评机构和金融行业网络安全等级保护主管部门对等级保护对象的安全状况进行安全测评。

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。凡是不注日期的文件，其最新版本（包括所有的修改版）适用于本文件。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

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 32400—2015 云计算概览与词汇

GM/T 0054—2018 信息系统密码应用基本要求

JR/T 0071.2—2020 金融行业网络安全等级保护实施指引 第2部分：基本要求

JR/T 0171—2020 个人金融信息保护技术规范

3 术语和定义

下列术语和定义适用于本文件。

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。

[GB/T 28448—2019，定义3.1]

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。

[GB/T 28448—2019，定义 3.2]

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。

[GB/T 28448—2019，定义 3.3]

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。
[GB/T 28448—2019，定义 3.4]

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。
[GB/T 28448—2019，定义 3.5]

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。
[GB/T 28448—2019，定义 3.6]

3.7

云计算 cloud computing
通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。
注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。
[GB/T 31167—2014，定义3.1]

3.8

云服务 cloud service
通过云计算已定义的接口提供的一种或多种能力。
[GB/T 32400—2015，定义 3.2.8]

3.9

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]

3.10

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]

3.11

云计算平台/系统 cloud computing platform/system
云服务商提供的云计算基础设施及其上的服务软件的集合。
[GB/T 22239—2019，定义 3.6]

3.12

团体云 community cloud
由一组特定的云服务客户使用和共享，且资源被云服务商或使用者控制的一种云部署和云服务模式。

3.13

虚拟机 virtual machine
通过各种虚拟化技术，为用户提供的与原有物理服务器相同的操作系统和应用程序运行环境的统称。
注：虚拟机通常使用物理服务器的资源，在用户看来它与物理服务器的使用方式完全相同。

3.14

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。

[GB/T 22239—2019，定义 3.7]

3.15

资源池 resource pool

按照一定规则可从中获取、释放、或回收资源的物理资源或虚拟资源的集合。

注：资源包括物理机、虚拟机、物理存储资源、虚拟存储资源、物理网络资源和虚拟网络资源等。

3.16

宿主机 host machine

运行虚拟机监视器的物理服务器。

[GB/T 22239—2019，定义 3.8]

3.17

敏感数据 sensitive data

一旦泄露可能会对用户或金融机构造成损失的数据。

[JR/T 0071.2—2020，定义 3.24]

3.18

个人金融信息 personal financial information

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

注：本标准中的个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

[JR/T 0171—2020，定义 3.2]

3.19

个人金融信息主体 personal financial data subject

个人金融信息所标识的自然人。

[JR/T 0171—2020，定义3.4]

3.20

移动互联 mobile communication

采用无线通信技术将移动终端接入有线网络的过程。

[GB/T 22239—2019，定义 3.9]

3.21

移动终端 mobile device

在移动业务中使用的终端设备，包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

[GB/T 22239—2019，定义 3.10]

3.22

无线接入设备 wireless access device

采用无线通信技术将移动终端接入有线网络的通信设备。

[GB/T 22239—2019，定义 3.11]

3.23

无线接入网关 wireless access gateway

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

[GB/T 22239—2019，定义 3.12]

3.24

移动应用软件 mobile application

针对移动终端开发的应用软件。

[GB/T 22239—2019，定义 3.13]

3.25

移动终端管理系统 mobile device management system

用于进行移动终端设备管理、应用管理和内容管理的专用软件，包括客户端软件和服务端软件。

[GB/T 22239—2019，定义 3.14]

3.26

物联网 internet of things；IOT

将感知节点设备（含 RFID）通过互联网等网络连接起来构成的一个应用系统，其融合信息系统和物理世界实体，是虚拟世界与现实世界的结合。

注：改写 GB/T 22239—2019，定义 3.15。

3.27

网关节点设备 The sensor layer gateway

将感知节点设备所采集的数据传输到数据处理中心的关键出口，连接传统信息网络（有线网、移动网等）和传感网的设备。

注：简单的感知层网关只是对感知数据的转发（因电力充足），而智能的感知层网关可以包括对数据进行适当处理、数据融合等业务。

3.28

感知节点设备 sensor node

物联网系统的最终端设备或器件，能够通过有线、无线方式发起或终结通信，采集物理信息和/或接受控制的实体设备。

注：感知节点设备也叫感知终端设备（end sensor）、终端感知节点设备（end sensor node）。

3.29

感知网关节点设备 sensor layer gateway

将感知节点所采集的数据进行汇总、适当处理或数据融合，并进行转发的装置。

[GB/T 22239—2019，定义 3.17]

3.30

动态口令 one-time-password（OTP），dynamic password

基于时间、事件等方式动态生成的一次性口令。

[GM/T 0054—2018，定义 3.1]

3.31

安全单元 security element；SE

负责关键数据的安全存储的部件。

3.32

大数据 big data

具有数量巨大、种类多样、流动速度快、特征多变等特性，并且难以用传统数据体系结构和数据处理技术进行有效组织、存储、计算、分析和管理的数据集。

3.33

大数据平台 big data platform

采用分布式存储和计算技术，提供大数据的访问和处理，支持大数据应用安全高效运行的软硬件集合。

注：大数据平台通常包括监视大数据的存储、输入/输出、操作控制等大数据服务软硬件基础设施。

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）

CPU：中央处理单元（Central Processing Unit）

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

DoS：拒绝服务（Denial of Service）

HTTPS：安全超文本传输协议（HyperText Transfer Protocol Secure）

IP：互联网协议（Internet Protocol）

IT：信息技术（Information Technology）

RFID：射频识别（Radio Frequency Identification）

SQL：结构化查询语言（Structured Query Language）

SSID：服务集标识（Service Set Identifier）

VPN：虚拟专用网络（Virtual Private Network）

WEP：有线等效加密（Wired Equivalent Privacy）

WPS：WiFi 保护设置（WiFi Protected Setup）

XSS：跨站脚本攻击（Cross-Site Scripting）

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JR/T 0071.2—2020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JR/T 0071.2—2020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和物联网安全测评扩展要求4个部分，大数据可参考安全评估方法参见附录B。与金融机构系统特色相结合，新增金融行业增强安全保护类（F类）要求，F2表示第二级增强安全保护要求，F3表示第三级增强安全保护要求，F4表示第四级增强安全保护要求。

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 第二级测评要求

6.1 安全测评通用要求

6.1.1 安全物理环境

6.1.1.1 物理位置选择

测评单元（L2-PES1-01）

该测评单元包括以下要求：

a) 测评指标：机房场地应选择在具有防震、防风和防雨等能力的建筑内。
b) 测评对象：记录表单类文档和机房。
c) 测评实施包括以下内容：
   1) 应核查所在建筑物是否具有建筑物抗震设防审批文档。
   2) 应核查机房是否不存在雨水渗漏。
   3) 应核查机房门窗是否不存在因风导致尘土严重的情况。
   4) 应核查屋顶、墙体、门窗和地面等是否没有破损开裂。
d) 单元判定：如果1）～4）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-PES1-02）

该测评单元包括以下要求：

a) 测评指标：机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
b) 测评对象：机房。
c) 测评实施：应核查机房是否不位于所在建筑物的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.2 物理访问控制

测评单元（L2-PES1-03）

该测评单元包括以下要求：

a) 测评指标：机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
b) 测评对象：机房电子门禁系统和值守记录。
c) 测评实施包括以下内容：
   1) 应核查是否安排专人值守或配置电子门禁系统。
   2) 应核查相关记录是否能够控制、鉴别和记录进入的人员。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-PES1-04）

该测评单元包括以下要求：

a) 测评指标：**可对机房划分区域进行管理，并根据各区域特点提出相应的访问控制要求。（F2）**
b) 测评对象：机房。
c) 测评实施包括以下内容：

1） 应核查机房区域划分是否合理，是否根据各区域特点提出相应的访问控制要求。
2） 应核查相关记录是否能够控制、鉴别和记录进入的人员。

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

6.1.1.3 防盗窃和防破坏

测评单元（L2-PES1-05）

该测评单元包括以下要求：

a） 测评指标：应将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。

测评单元（L2-PES1-06）

该测评单元包括以下要求：

a） 测评指标：应将通信线缆铺设在隐蔽安全处。
b） 测评对象：机房通信线缆。
c） 测评实施：应核查机房内通信线缆是否铺设在隐蔽安全处，如桥架中等。
d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-PES1-07）

该测评单元包括以下要求：

a） 测评指标：**应建立机房视频监控系统和动环监控系统，对机房风冷水电设备、消防设施、门禁系统等重要设施实行全面监控，视频监控记录和门禁系统出入记录至少保存3个月。（F2）**
b） 测评对象：机房视频监控系统和动环监控系统。
c） 测评实施包括以下内容：
1） 应核查机房是否配置视频监控系统和动环监控系统。
2） 应核查视频监控系统和动环监控系统是否启用。
3） 应核查视频监控系统和动环监控系统是否对机房风冷水电设备、消防设施、门禁系统等重要设施实行全面监控，并核查视频监控记录和门禁系统出入记录是否至少保存3个月。
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。

6.1.1.4 防雷击

测评单元（L2-PES1-08）

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。

6.1.1.5 防火

测评单元（L2-PES1-09）

该测评单元包括以下要求：

a) 测评指标：机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。
b) 测评对象：机房防火设施。
c) 测评实施包括以下内容：
   1) 应核查机房内是否设置火灾自动消防系统。
   2) 应核查火灾自动消防系统是否可以自动检测火情、自动报警，并自动灭火。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-PES1-10）

该测评单元包括以下要求：

a) 测评指标：机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
b) 测评对象：机房验收类文档。
c) 测评实施：应核查机房验收文档是否明确相关建筑材料的耐火等级。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-PES1-11）

该测评单元包括以下要求：

a) 测评指标：**机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收。（F2）**
b) 测评对象：机房验收类文档。
c) 测评实施：应核查机房验收类文档，是否明确内部通道设置、装修装饰材料、设备线缆等满足消防验收要求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.6 防水和防潮

测评单元（L2-PES1-12）

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。

测评单元（L2-PES1-13）

该测评单元包括以下要求：

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。
b) 测评对象：机房。
c) 测评实施包括以下内容：
   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 防静电

测评单元（L2-PES1-14）

该测评单元包括以下要求：

a) 测评指标：应采用防静电地板或地面并采用必要的接地防静电措施。
b) 测评对象：机房。
c) 测评实施包括以下内容：
   1) 应核查机房内是否安装了防静电地板或地面。
   2) 应核查机房内是否采用了接地防静电措施。
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。

6.1.1.8 温湿度控制

测评单元（L2-PES1-15）

该测评单元包括以下要求：
a) 测评指标：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。
b) 测评对象：机房温湿度调节设施。
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。

6.1.1.9 电力供应

测评单元（L2-PES1-16）

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。

测评单元（L2-PES1-17）

该测评单元包括以下要求：
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。
b) 测评对象：机房备用供电设施。
c) 测评实施包括以下内容：
   1) 应核查机房是否配备 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。

测评单元（L2-PES1-18）

该测评单元包括以下要求：
a) 测评指标：**机房重要区域、重要设备应提供 UPS 供电。（F2）**
b) 测评对象：机房备用供电设施。
c) 测评实施包括以下内容：
   1) 应核查机房重要区域、重要设备是否配备 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。

6.1.1.10 电磁防护

测评单元（L2-PES1-19）

该测评单元包括以下要求：

a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰。
b) 测评对象：机房线缆。
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 网络架构

测评单元（L2-CNS1-01）

该测评单元包括以下要求：

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。
b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否依据重要性、部门等因素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划分原则一致。
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。

测评单元（L2-CNS1-02）

该测评单元包括以下要求：

a) 测评指标：应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
b) 测评对象：网络拓扑。
c) 测评实施包括以下内容：
   1) 应核查网络拓扑图是否与实际网络运行环境一致。
   2) 应核查重要网络区域是否未部署在网络边界处。
   3) 应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、防火墙和设备访问控制列表（ACL）等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2.2 通信传输

测评单元（L2-CNS1-03）

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证其完整性。
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。

6.1.2.3 可信验证

测评单元（L2-CNS1-04）

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、重要配置参数和通信应用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，并将验证结果形成审计记录送至安全管理中心。

b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。
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、重要配置参数和通信应用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。
   3) 应核查验证结果是否以审计记录的形式送至安全管理中心。
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 安全区域边界

6.1.3.1 边界防护

测评单元（L2-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

测评单元（L2-ABS1-02）

该测评单元包括以下要求：
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。
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) 应核查在网络边界或区域之间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。

测评单元（L2-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。

测评单元（L2-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。

测评单元（L2-ABS1-05）

该测评单元包括以下要求：

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，**控制粒度为网段级。（F2）**
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：应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力，且控制粒度为网段级。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.3 入侵防范

测评单元（L2-ABS1-06）

该测评单元包括以下要求：

a) 测评指标：应在关键网络节点处监视网络攻击行为。
b) 测评对象：抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统、入侵保护系统和入侵检测系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够检测到以下攻击行为：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是否已经更新到最新版本。
   3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。
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。

6.1.3.4 恶意代码和垃圾邮件防范

测评单元（L2-ABS1-07）

该测评单元包括以下要求：

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。
b) 测评对象：防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查在关键网络节点处是否部署防恶意代码产品等技术措施。
   2) 应核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新。

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

测评单元（L2-ABS1-08）

该测评单元包括以下要求：

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。（F2）**

b) 测评对象：提供防垃圾邮件功能的系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查在关键网络节点处是否部署防垃圾邮件产品等技术措施。

2) 应核查防垃圾邮件策略是否更新到最新版本。

3) 应核查防垃圾邮件产品运行是否正常。

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。

6.1.3.5 安全审计

测评单元（L2-ABS1-09）

该测评单元包括以下要求：

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。

b) 测评对象：综合安全审计系统等。

c) 测评实施包括以下内容：

1) 应核查是否部署了综合安全审计系统或类似功能的系统平台。

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了审计。

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。

测评单元（L2-ABS1-10）

该测评单元包括以下要求：

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。

b) 测评对象：综合安全审计系统等。

c) 测评实施：应核查审计记录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。

测评单元（L2-ABS1-11）

该测评单元包括以下要求：

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。

b) 测评对象：综合安全审计系统等。

c) 测评实施包括以下内容：

1) 应核查是否采取了技术措施对审计记录进行保护。

2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

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

6.1.3.6 可信验证

测评单元（L2-ABS1-12）

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、重要配置参数和边界防护应用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，并将验证结果形成审计记录送至安全管理中心。
b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。
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、重要配置参数和边界防护应用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。
   3) 应核查验证结果是否以审计记录的形式送至安全管理中心。
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 安全计算环境

6.1.4.1 身份鉴别

测评单元（L2-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，**静态口令应在8位以上，由字母、数字、符号等混合组成**并定期更换。**（F2）**
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不存在空口令用户。
   4) 应核查用户静态口令是否在8位以上，由字母、数字、符号等混合组成并定期更换。
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。

测评单元（L2-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。

测评单元（L2-CES1-03）

该测评单元包括以下要求：

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。

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：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。

6.1.4.2 访问控制

测评单元（L2-CES1-04）

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) 应核查是否为用户分配了账户和权限及相关设置情况。

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。

测评单元（L2-CES1-05）

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，修改默认账户或**预设账户**的默认口令。**（F2）**

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或删除默认账户。

2) 应核查是否已修改默认账户或预设账户的默认口令。

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。

测评单元（L2-CES1-06）

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) 应核查并测试多余的、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。

测评单元（L2-CES1-07）

该测评单元包括以下要求：

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。

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) 应核查是否进行角色划分。

2) 应核查管理用户的权限是否已进行分离。

3) 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。

测评单元（L2-CES1-08）

该测评单元包括以下要求：

a) 测评指标：**应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。（F2）**

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：应核查是否严格限制默认账户或预设账户的权限，如将默认账户或预设账户的权限设置为空权限或某单一功能专用权限等。

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

6.1.4.3 安全审计

测评单元（L2-CES1-09）

该测评单元包括以下要求：

a) 测评指标：应提供安全审计功能，审计应覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

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) 应核查是否提供并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。

测评单元（L2-CES1-10）

该测评单元包括以下要求：

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。
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：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。

测评单元（L2-CES1-11）

该测评单元包括以下要求：
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，**审计记录保存时间应不少于6个月。（F2）**
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) 应核查是否采取了保护措施对审计记录进行保护。
   2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。
   3) 应核查审计记录保存时间是否不少于6个月。
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。

测评单元（L2-CES1-12）

该测评单元包括以下要求：
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，以确保审计分析的一致性与正确性。（F2）**
b) 测评对象：时钟服务器、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) 应核查是否具有唯一确定的时钟同步服务器。
   2) 应核查系统的时间与时钟同步服务器时间是否一致。
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 入侵防范

测评单元（L2-CES1-13）

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） 应核查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。

测评单元（L2-CES1-14）

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。

测评单元（L2-CES1-15）

该测评单元包括以下要求：

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。

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：应核查配置文件或参数是否对终端接入范围进行限制。

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

测评单元（L2-CES1-16）

该测评单元包括以下要求：

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。

b） 测评对象：业务应用系统、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的内容是否包括数据有效性检验功能的内容或模块。

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。

测评单元（L2-CES1-17）

该测评单元包括以下要求：

a） 测评指标：应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

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、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等。

c） 测评实施包括以下内容：

1） 应核查是否不存在高风险漏洞，如通过漏洞扫描、渗透测试等方式。

2） 应核查是否在经过充分测试评估后及时修补漏洞。

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。

测评单元（L2-CES1-18）

该测评单元包括以下要求：

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。（F2）**
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、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等。
c) 测评实施包括以下内容：
   1) 应核查是否采取技术措施对重要节点进行入侵检测。
   2) 应核查是否能对严重入侵事件进行报警，如通过声音、邮件、短信等方式。
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。

测评单元（L2-CES1-19）

该测评单元包括以下要求：
a) 测评指标：**所有安全计算环境设备应全部专用化，不得进行与业务不相关的操作。（F2）**
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等。
c) 测评实施包括以下内容：
   1) 应核查各安全计算环境设备的业务用途是否专用化。
   2) 应核查各安全计算环境设备是否未进行过与业务用途不相关的操作。
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。

测评单元（L2-CES1-20）

该测评单元包括以下要求：
a) 测评指标：**应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F2）**
b) 测评对象：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等。
c) 测评实施：应通过给系统人为制造一些故障（如系统异常），测试验证系统是否未在故障发生时将技术错误信息直接或间接反馈到前台界面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.5 恶意代码防范

测评单元（L2-CES1-21）

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**统一**进行升级和更新防恶意代码库。**（F2）**
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) 测评实施包括以下内容：
   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) 应核查是否定期统一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。

6.1.4.6 可信验证

测评单元（L2-CES1-22）

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、重要配置参数和应用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，并将验证结果形成审计记录送至安全管理中心。
b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。
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、重要配置参数和应用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。
   3) 应核查验证结果是否以审计记录的形式送至安全管理中心。
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。

6.1.4.7 数据完整性

测评单元（L2-CES1-23）

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**和存储**过程中的完整性。**（F2）**
b) 测评对象：业务应用系统。
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和存储过程中是否采用了校验技术保证完整性。
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。

6.1.4.8 数据保密性

测评单元（L2-CES1-24）

该测评单元包括以下要求：

a) 测评指标：**应采用加密或其他保护措施保证鉴别信息在传输和存储过程中的保密性。（F2）**
b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。
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和存储过程中是否采用了加密或其他保护措施保证保密性。
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。

6.1.4.9 数据备份恢复

测评单元（L2-CES1-25）

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：业务系统、网络设备，操作系统、数据库等配置数据。
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。

测评单元（L2-CES1-26）

该测评单元包括以下要求：

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。
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。

6.1.4.10 剩余信息保护

测评单元（L2-CES1-27）

该测评单元包括以下要求：

a) 测评指标：应保证**操作系统、数据库系统和应用系统用户**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，**无论这些信息是存放在硬盘上还是内存中。（F2）**
b) 测评对象：终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统等。
c) 测评实施：应核查相关配置信息或系统设计文档，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。

6.1.4.11 个人信息保护

测评单元（L2-CES1-28）

该测评单元包括以下要求：

a) 测评指标：**金融机构在收集、使用个人金融信息时，应当遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F2）**
b) 测评对象：隐私政策。
c) 测评实施包括以下内容：
   1) 应核查是否具有隐私政策。
   2) 应核查隐私政策中是否向个人金融信息主体明示收集、使用信息的目的、方式和范围。
   3) 应核查隐私政策是否获得个人信息主体的明示同意。
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。

测评单元（L2-CES1-29）

该测评单元包括以下要求：

a) 测评指标：应仅采集和保存业务必需的用户个人**金融**信息。**（F2）**
b) 测评对象：业务应用系统和数据库管理系统等。
c) 测评实施包括以下内容：
   1) 应核查采集和保存的用户个人金融信息是否是业务应用必需的。
   2) 应核查是否制定了有关用户个人金融信息保护的管理制度和流程。
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。

测评单元（L2-CES1-30）

该测评单元包括以下要求：

a) 测评指标：**应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限，**应禁止未授权访问和非法使用用户个人**金融**信息。**（F2）**
b) 测评对象：业务应用系统和数据库管理系统等。

c) 测评实施包括以下内容：
   1) 应核查是否采用技术措施限制对用户个人金融信息的访问和使用。
   2) 应核查是否根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理。
   3) 应核查是否制定了有关用户个人金融信息保护的管理制度和流程。
   4) 应验证未经授权是否不能访问用户个人金融信息。
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。

测评单元（L2-CES1-31）

该测评单元包括以下要求：
a) 测评指标：**金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F2）**
b) 测评对象：个人金融信息、个人金融信息全生命周期管理相关规范、个人金融信息生命周期过程进行安全检查与评估的相关文档等。
c) 测评实施包括以下内容：
   1) 应访谈是否对个人金融信息生命周期过程进行安全检查与评估。
   2) 应核查是否具备对个人金融信息生命周期过程进行安全检查与评估的报告。
   3) 应核查是否对个人金融信息生命周期过程的安全检查与评估中发现的高风险问题进行补充测试。
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。

测评单元（L2-CES1-32）

该测评单元包括以下要求：
a) 测评指标：**金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F2）**
b) 测评对象：计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等可能展示个人金融信息的界面。
c) 测评实施包括以下内容：
   1) 应访谈和核查个人金融信息以何种方式展示，如计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等。
   2) 应核查展示个人金融信息的界面是否采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。
d) 单元判定：如果 2）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。

测评单元（L2-CES1-33）

该测评单元包括以下要求：
a) 测评指标：**应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F2）**
b) 测评对象：隐私政策和个人金融信息。
c) 测评实施包括以下内容：
   1) 应访谈并核查是否存在个人金融信息共享、转让的情况。
   2) 应核查用户隐私政策，是否明确告知个人金融信息主体共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力。
   3) 应核查隐私政策是否获得个人金融信息主体的明示同意。

4) 应核查共享、转让的个人金融信息是否经去标识化处理，且数据接收方无法重新识别个人金融信息主体。

d) 单元判定：如果1）为否定，则不适用本测评单元指标要求，如果1）～3）均为肯定或4）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。

测评单元（L2-CES1-34）

该测评单元包括以下要求：

a) 测评指标：**开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F2）**

b) 测评对象：开发环境、测试环境、开发和测评环境中使用的数据。

c) 测评实施包括以下内容：

1) 应核查系统开发环境和测试环境中的数据是否使用虚构的个人金融信息。

2) 如果使用真实的个人金融信息，是否对真实的个人金融信息进行去标识化处理，账号、卡号、协议号、支付指令等测试确需除外。

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，否则不符合本测评单元指标要求。

6.1.5 安全管理中心

6.1.5.1 系统管理

测评单元（L2-SMC1-01）

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：提供集中系统管理功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否对系统管理员进行身份鉴别。

2) 应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作。

3) 应核查是否对系统管理的操作进行审计。

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。

测评单元（L2-SMC1-02）

该测评单元包括以下要求：

a) 测评指标：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、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

b) 测评对象：提供集中系统管理功能的系统。

c) 测评实施：应核查是否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、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

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

测评单元（L2-SMC1-03）

该测评单元包括以下要求：

a) 测评指标：**应每月对设备的配置文件进行备份，发生变动时应及时备份。（F2）**

b) 测评对象：提供集中系统管理功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否每月对设备的配置文件进行备份。

2) 应核查系统发生变动时是否及时备份。

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。

测评单元（L2-SMC1-04）

该测评单元包括以下要求：

a) 测评指标：**应定期对设备运行状况进行监测。（F2）**
b) 测评对象：系统管理员、监测记录。
c) 测评实施：应核查是否定期对设备运行状况进行监测。
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。

测评单元（L2-SMC1-05）

该测评单元包括以下要求：

a) 测评指标：**应定期检验设备的软件版本信息，并留存记录。（F2）**
b) 测评对象：系统管理员、测试验证记录。
c) 测评实施：应核查是否对设备的版本进行定期更新，并核查测试验证记录，判断是否定期对版本进行有效测试验证。
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。

测评单元（L2-SMC1-06）

该测评单元包括以下要求：

a) 测评指标：**应提供数据备份与恢复功能，增量数据备份至少每天一次。（F2）**
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施：
   1) 应核查是否提供数据备份与恢复功能。
   2) 应核查增量数据备份是否至少每天一次。
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。

6.1.5.2 审计管理

测评单元（L2-SMC1-07）

该测评单元包括以下要求：

a) 测评指标：应对审计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审计操作，并对这些操作进行审计。
b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否对审计管理员进行身份鉴别。
   2) 应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作。
   3) 应核查是否对审计管理员的操作进行审计。
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。

测评单元（L2-SMC1-08）

该测评单元包括以下要求：

a) 测评指标：应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。

c) 测评实施：应核查是否通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.6 安全管理制度

6.1.6.1 安全策略

测评单元（L2-PSS1-01）

该测评单元包括以下要求：
a) 测评指标：应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
b) 测评对象：总体方针策略类文档。
c) 测评实施：应核查网络安全工作的总体方针和安全策略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。

6.1.6.2 管理制度

测评单元（L2-PSS1-02）

该测评单元包括以下要求：
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。
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物理、网络、主机系统、数据、应用、建设和运维等管理内容。
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。

测评单元（L2-PSS1-03）

该测评单元包括以下要求：
a) 测评指标：应对安全管理人员或操作人员执行的日常管理操作建立操作规程。
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。

6.1.6.3 制定和发布

测评单元（L2-PSS1-04）

该测评单元包括以下要求：
a) 测评指标：**金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应制定适用辖内的安全管理制度。（F2）**
b) 测评对象：部门/人员职责文件等。
c) 测评实施包括以下内容：
   1) 应核查适用全机构范围的安全管理制度是否在金融机构总部的总体负责下统一制定。
   2) 应核查各分支机构是否制定了适用辖内的安全管理制度。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-PSS1-05）

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安全管理制度的制定。
b) 测评对象：部门/人员职责文件等。
c) 测评实施：应核查是否由专门的部门或人员负责制定安全管理制度。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-PSS1-06）

该测评单元包括以下要求：

a) 测评指标：安全管理制度应通过正式、有效的方式发布，并进行版本控制。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容。
   2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.6.4 评审和修订

测评单元（L2-PSS1-07）

该测评单元包括以下要求：

a) 测评指标：应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期对安全管理制度体系的合理性和适用性进行审定。
   2) 应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.7 安全管理机构

6.1.7.1 岗位设置

测评单元（L2-ORS1-01）

该测评单元包括以下要求：

a) 测评指标：**网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F2）**
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/网络安全主管网络安全管理工作是否实行统一领导、分级管理。
   2) 应核查相关制度文档是否明确了总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。
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。

测评单元（L2-ORS1-02）

该测评单元包括以下要求：

a) 测评指标：**除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开展本部门的网络安全管理工作。（F2）**
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/网络安全主管网络安全管理部门外的其他部门是否指定至少一名部门网络安全员。
   2) 应核查岗位职责文档是否明确了部门网络安全员需协助网络安全管理部门开展本部门的网络安全管理工作。
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。

测评单元（L2-ORS1-03）

该测评单元包括以下要求：
a) 测评指标：应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。
b) 测评对象：信息/网络安全主管和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否设立网络安全管理工作的职能部门。
   2) 应核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责。
   3) 应核查岗位职责文档是否有岗位划分情况和岗位职责。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-ORS1-04）

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

6.1.7.2 人员配备

测评单元（L2-ORS1-05）

该测评单元包括以下要求：
a) 测评指标：应配备一定数量的系统管理员、审计管理员和安全管理员等。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否配备了系统管理员、审计管理员和安全管理员。
   2) 应核查人员配备文档是否明确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。

测评单元（L2-ORS1-06）

该测评单元包括以下要求：
a) 测评指标：**安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。（F2）**
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：应访谈信息/网络安全主管安全管理员是否没有兼任网络管理员、系统管理员、数据库管理员等。
d) 单元判定：如果上述条款均为肯定，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 授权和审批

测评单元（L2-ORS1-07）

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，**对系统投入运行、系统变更、网络系统接入和重要资源（如敏感数据等资源）的访问等关键活动应执行审批过程。（F2）**
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，尤其是是否对系统投入运行、系统变更、网络系统接入和重要资源（如敏感数据等资源）的访问等关键活动执行审批过程。
   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。

6.1.7.4 沟通和合作

测评单元（L2-ORS1-08）

该测评单元包括以下要求：
a) 测评指标：应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否建立了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制。
   2) 应核查会议记录是否明确在各类管理人员、组织内部机构和网络安全管理部门之间开展了合作与沟通。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-ORS1-09）

该测评单元包括以下要求：
a) 测评指标：应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否建立了与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制。
   2) 应核查会议记录是否明确了与网络安全职能部门、各类供应商、业界专家及安全组织开展了合作与沟通。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-ORS1-10）

该测评单元包括以下要求：
a) 测评指标：应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
b) 测评对象：记录表单类文档。

c) 测评实施：应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息。
d) 单元判定：如果以上测评实施内容为肯定，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。

6.1.7.5 审核和检查

测评单元（L2-ORS1-11）

该测评单元包括以下要求：
a) 测评指标：应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期进行了常规安全检查。
   2) 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8 安全管理人员

6.1.8.1 人员录用

测评单元（L2-HRS1-01）

该测评单元包括以下要求：
a) 测评指标：应指定或授权专门的部门或人员负责人员录用。
b) 测评对象：信息/网络安全主管。
c) 测评实施：应访谈信息/网络安全主管是否由专门的部门或人员负责人员的录用工作。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-HRS1-02）

该测评单元包括以下要求：
a) 测评指标：应对被录用人员的身份、安全背景、专业资格或资质等进行审查。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）。
   2) 应核查是否具有人员录用时对录用人身份、安全背景、专业资格或资质等进行审查的相关文档或记录，是否记录审查内容和审查结果等。
   3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-HRS1-03）

该测评单元包括以下要求：
a) 测评指标：**应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否有网络安全管理人员的备案制度。
   2) 应核查相关备案记录，网络安全管理人员的配备变更情况是否报上一级科技部门备案，金融机构总部网络安全管理人员是否在总部科技部门备案。

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

测评单元（L2-HRS1-04）

该测评单元包括以下要求：

a) 测评指标：**凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不应从事网络安全管理工作。（F2）**
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：应核查网络安全管理人员是否无因违反国家法律法规和金融机构有关规定而受到处罚或处分的记录。
d) 单元判定：如果上述条款均为肯定，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。

6.1.8.2 人员离岗

测评单元（L2-HRS1-05）

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。

6.1.8.3 安全意识教育和培训

测评单元（L2-HRS1-06）

该测评单元包括以下要求：

a) 测评指标：**应制定安全教育和培训计划。（F2）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否具有安全教育和培训的计划表。
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。

测评单元（L2-HRS1-07）

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。

测评单元（L2-HRS1-08）

该测评单元包括以下要求：

a) 测评指标：**每年应至少对网络安全管理人员进行一次网络安全培训。（F2）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否具有每年对网络安全管理人员进行网络安全培训的培训记录。

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。

6.1.8.4 外部人员访问管理

测评单元（L2-HRS1-09）

该测评单元包括以下要求：

a) 测评指标：应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等。
   2) 应核查外部人员访问重要区域的申请文档是否具有批准人允许访问的批准等。
   3) 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-HRS1-10）

该测评单元包括以下要求：

a) 测评指标：应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程。
   2) 应核查外部人员访问系统的申请文档是否明确外部人员的访问权限，是否具有允许访问的批准等。
   3) 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-HRS1-11）

该测评单元包括以下要求：

a) 测评指标：外部人员离场后应及时清除其所有的访问权限。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限。
   2) 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-HRS1-12）

该测评单元包括以下要求：

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，不得进行非授权的增加、删除、修改、查询数据等操作，不得复制和泄露金融机构的任何信息。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否与获得系统访问授权的外部人员签署了保密协议。

2) 应核查保密协议中是否有禁止进行未授权的增加、删除、修改、查询数据操作，禁止复制和泄露金融机构的任何信息等相关要求。

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

6.1.9 安全建设管理

6.1.9.1 定级和备案

测评单元（L2-CMS1-01）

该测评单元包括以下要求：

a) 测评指标：应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由。

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

测评单元（L2-CMS1-02）

该测评单元包括以下要求：

a) 测评指标：应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见。

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

测评单元（L2-CMS1-03）

该测评单元包括以下要求：

a) 测评指标：应保证定级结果经过相关部门的批准。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见。

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

测评单元（L2-CMS1-04）

该测评单元包括以下要求：

a) 测评指标：应将备案材料报主管部门和相应公安机关备案。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查是否具有公安机关出具的备案证明文档。

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

6.1.9.2 安全方案设计

测评单元（L2-CMS1-05）

该测评单元包括以下要求：

a) 测评指标：应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

b) 测评对象：安全规划设计类文档。

c) 测评实施：应核查安全设计文档是否根据安全保护等级选择安全措施，是否根据安全需求调整安全措施。

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

测评单元（L2-CMS1-06）

该测评单元包括以下要求：

a) 测评指标：应根据保护对象的安全保护等级进行安全方案设计。
b) 测评对象：安全规划设计类文档。
c) 测评实施：应核查安全设计方案是否是根据安全保护等级进行设计规划。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-07）

该测评单元包括以下要求：

a) 测评指标：应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查安全方案的论证评审记录或文档是否有相关部门和有关安全技术专家的批准意见和论证意见。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.9.3 产品采购和使用

测评单元（L2-CMS1-08）

该测评单元包括以下要求：

a) 测评指标：应确保网络安全产品采购和使用符合国家的有关规定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查有关网络安全产品是否符合国家的有关规定，如网络安全产品获得了销售许可等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-09）

该测评单元包括以下要求：

a) 测评指标：应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈建设负责人是否采用了密码产品及其相关服务。
   2) 应核查密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-CMS1-10）

该测评单元包括以下要求：

a) 测评指标：**各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有扫描、检查类网络安全产品购置前本机构科技主管部门的批准、备案记录。
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。

测评单元（L2-CMS1-11）

该测评单元包括以下要求：

a) 测评指标：**扫描、检测类网络安全产品应仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查网络安全产品使用记录，是否仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。
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。

测评单元（L2-CMS1-12）

该测评单元包括以下要求：

a) 测评指标：**应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取应急措施并按规定程序报告。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有定期对各类网络安全产品相关日志和报表信息进行汇总分析的记录或分析报告。
   2) 应核查一旦发现重大问题，是否具有相应的控制措施和报告程序。
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。

测评单元（L2-CMS1-13）

该测评单元包括以下要求：

a) 测评指标：**应定期对各类网络安全产品产生的日志和报表进行备份存档。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有对各类网络安全产品日志和报表进行定期备份存档的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-14）

该测评单元包括以下要求：

a) 测评指标：**应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。（F2）**
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) 应核查网络安全产品维护和报废相关管理制度中是否有及时升级维护规定以及报废审批流程。
   2) 应核查是否具有网络安全产品升级维护记录。
   3) 应核查对于超过使用期限或不能继续使用的网络安全产品是否具有报废、审批记录。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.9.4 自行软件开发

测评单元（L2-CMS1-15）

该测评单元包括以下要求：

a) 测评指标：**应将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试中使用。（F2）**
b) 测评对象：建设负责人。
c) 测评实施包括以下内容：

1) 应访谈建设负责人自主开发软件是否在独立的物理环境中完成编码和调试，与实际运行环境分开。
2) 应核查敏感数据是否脱敏后在开发或测试中使用。

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

测评单元（L2-CMS1-16）

该测评单元包括以下要求：

a) 测评指标：**应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制。（F2）**
b) 测评对象：建设负责人。
c) 测评实施包括以下内容：
1) 应访谈建设负责人开发人员和测试人员是否分离。
2) 应访谈建设负责人开发人员是否没有兼任系统管理员或业务操作人员。
3) 应核查测试数据和测试结果是否受控使用。
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。

测评单元（L2-CMS1-17）

该测评单元包括以下要求：

a) 测评指标：应在软件开发过程中对**代码规范、代码质量、代码安全性进行审查**，在软件安装前对可能存在的恶意代码进行检测。**（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.9.5 外包软件开发

测评单元（L2-CMS1-18）

该测评单元包括以下要求：

a) 测评指标：应在软件交付前检测其中可能存在的恶意代码。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有交付前的恶意代码检测报告。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-19）

该测评单元包括以下要求：

a) 测评指标：应保证开发单位提供软件设计文档和使用指南。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-20）

该测评单元包括以下要求：

a) 测评指标：**应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F2）**
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈建设负责人是否要求外包服务商保留操作痕迹、记录完整的日志。
   2) 应核查相关内容和保存期限是否满足事件分析、安全取证、独立审计和监督检查需要。
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。

测评单元（L2-CMS1-21）

该测评单元包括以下要求：
a) 测评指标：**应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F2）**
b) 测评对象：外包合同商务类文档。
c) 测评实施：应核查外包合同等商务文件是否具有控制外包服务商分包的条款。
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。

测评单元（L2-CMS1-22）

该测评单元包括以下要求：
a) 测评指标：**应定期对外包服务活动和外包服务商的服务能力进行审核和评估。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有对外包活动和外包服务商的服务能力进行定期审核和评估的报告。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.9.6 工程实施

测评单元（L2-CMS1-23）

该测评单元包括以下要求：
a) 测评指标：应指定或授权专门的部门或人员负责工程实施过程的管理。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否指定专门部门或人员对工程实施进行进度和质量控制。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-24）

该测评单元包括以下要求：
a) 测评指标：应制定安全工程实施方案控制工程实施过程。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查安全工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.9.7 测试验收

测评单元（L2-CMS1-25）

该测评单元包括以下要求：
a) 测评指标：应制订测试验收方案，并依据测试验收方案实施测试验收，**在测试验收过程中应详细记录测试验收结果**，形成测试验收报告。**（F2）**
b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：
   1) 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容。
   2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-CMS1-26）

该测评单元包括以下要求：
a) 测评指标：应进行上线前的安全性测试，并出具安全测试报告。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有上线前的安全测试报告。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-27）

该测评单元包括以下要求：
a) 测评指标：**对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方案、数据备份与系统恢复措施、应急处置措施后，经主管领导审批后开展测试工作，以确保生产系统的安全。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 针对在生产系统上进行测试的情况，应核查是否事先进行了风险分析和告知。
   2) 针对在生产系统上进行测试的情况，应核查是否具有详细的系统测试方案、数据备份与系统恢复措施、应急处置措施。
   3) 针对在生产系统上进行测试的情况，应核查是否具有主管领导的审批记录。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.9.8 系统交付

测评单元（L2-CMS1-28）

该测评单元包括以下要求：
a) 测评指标：应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查交付清单是否说明交付的各类设备、软件、文档等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-29）

该测评单元包括以下要求：
a) 测评指标：应对负责运行维护的技术人员进行相应的技能培训。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查交付技术培训记录是否包括培训内容、培训时间和参与人员等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-30）

该测评单元包括以下要求：
a) 测评指标：应提供建设过程文档和运行维护文档。

b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否提供建设过程文档和运行维护文档。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-31）

该测评单元包括以下要求：
a) 测评指标：**外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查金融机构与外部建设单位之间是否签署知识产权保护协议和保密协议，并核查协议中是否具有禁止将系统关键安全技术措施和核心安全功能对外公开的条款。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.9.9 等级测评

测评单元（L2-CMS1-32）

该测评单元包括以下要求：
a) 测评指标：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人本次测评是否为首次，若非首次，是否根据以往测评结果进行相应的安全整改。
   2) 应核查是否具有以往等级测评报告和安全整改方案。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-CMS1-33）

该测评单元包括以下要求：
a) 测评指标：应在发生重大变更或级别发生变化时进行等级测评。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否有过重大变更或级别发生过变化及是否进行相应的等级测评。
   2) 应核查是否具有相应情况下的等级测评报告。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-CMS1-34）

该测评单元包括以下要求：
a) 测评指标：应确保测评机构的选择符合国家有关规定。
b) 测评对象：等级测评报告和相关资质文件。
c) 测评实施：应核查以往等级测评的测评单位是否具有等级测评机构资质。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.9.10 服务供应商管理

测评单元（L2-CMS1-35）

该测评单元包括以下要求：
a) 测评指标：**应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。（F2）**

b) 测评对象：服务供应商。
c) 测评实施：应访谈建设负责人是否评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。
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。

测评单元（L2-CMS1-36）

该测评单元包括以下要求：
a) 测评指标：应确保服务供应商的选择符合国家的有关规定。
b) 测评对象：服务供应商。
c) 测评实施：应访谈建设负责人选择的安全服务商是否符合国家有关规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS1-37）

该测评单元包括以下要求：
a) 测评指标：应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查与服务供应商签订的服务合同或安全责任合同书是否明确了后期的技术支持和服务承诺等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.10 安全运维管理

6.1.10.1 环境管理

测评单元（L2-MMS1-01）

该测评单元包括以下要求：
a) 测评指标：应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。
b) 测评对象：物理安全负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理，对基础设施（如空调、供配电设备、灭火设备等）进行定期维护。
   2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员。
   3) 应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息。
   4) 应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
d) 单元判定：如果 1）～4）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-02）

该测评单元包括以下要求：
a) 测评指标：应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等方面。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房安全管理制度是否覆盖物理访问、物品进出和环境安全等方面内容。
   2) 应核查物理访问、物品进出和环境安全等相关记录是否与制度相符。

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

测评单元（L2-MMS1-03）

该测评单元包括以下要求：

a) 测评指标：**机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F2）**
b) 测评对象：机房。
c) 测评实施：应核查机房布线是否做到跳线整齐，跳线与配线架是否统一编号，标记是否清晰。
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。

测评单元（L2-MMS1-04）

该测评单元包括以下要求：

a) 测评指标：**进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房管理制度是否要求进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。
   2) 应核查是否具有进出机房人员审批记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-05）

该测评单元包括以下要求：

a) 测评指标：**机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查人员管理或培训相关制度是否要求机房管理员经过相关培训后才能上岗。
   2) 应核查是否具有机房管理员培训记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-06）

该测评单元包括以下要求：

a) 测评指标：**应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查机房设施维修保养记录是否记录机房设施定期维护保养的情况。
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。

测评单元（L2-MMS1-07）

该测评单元包括以下要求：

a) 测评指标：**机房出入口和内部应安装 7*24 小时录像监控设施，录像至少保存 3 个月。（F2）**
b) 测评对象：机房和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房出入口和内部是否安装 7*24 小时监控设施。
   2) 应核查监控录像保存时间是否满足至少 3 个月。
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。

测评单元（L2-MMS1-08）

该测评单元包括以下要求：

a) 测评指标：**机房应设置弱电井或桥架，并留有可扩展空间。（F2）**

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房是否设置弱电井或桥架。

2) 应核查弱电井或桥架是否留有扩展空间。

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

测评单元（L2-MMS1-09）

该测评单元包括以下要求：

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

b) 测评对象：安全管理员和办公环境。

c) 测评实施包括以下内容：

1) 应访谈安全管理员是否有相关规定明确接待来访人员区域。

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

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

6.1.10.2 资产管理

测评单元（L2-MMS1-10）

该测评单元包括以下要求：

a) 测评指标：应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容。

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

6.1.10.3 介质管理

测评单元（L2-MMS1-11）

该测评单元包括以下要求：

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

b) 测评对象：资产管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理。

2) 应核查介质管理记录是否记录介质归档和使用等情况。

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

测评单元（L2-MMS1-12）

该测评单元包括以下要求：

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

b) 测评对象：资产管理员和记录表单类文档。

c) 测评实施包括以下内容：
   1) 应访谈资产管理员介质在物理传输过程中的人员选择、打包、交付等情况是否进行控制。
   2) 应核查是否对介质的归档和查询等进行登记记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-13）

该测评单元包括以下要求：
a) 测评指标：**所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F2）**
b) 测评对象：资产管理员。
c) 测评实施：应访谈资产管理员并核查存放数据备份介质的环境是否防磁、防潮、防尘、防高温、防挤压。
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。

测评单元（L2-MMS1-14）

该测评单元包括以下要求：
a) 测评指标：**对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F2）**
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) 应核查纸质文档是否实行借阅登记制度，是否未经相关部门领导批准，任何人不得将文档转借、复制或对外公开。
   2) 应核查电子文档是否采用电子化办公审批平台进行管理。
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。

测评单元（L2-MMS1-15）

该测评单元包括以下要求：
a) 测评指标：**对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录；信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F2）**
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) 应核查载有敏感信息存储介质的销毁制度，是否对介质的销毁严格管理。
   2) 应核查是否具有销毁介质的备案、销毁记录等。
   3) 应核查对于存储介质未在金融机构内部使用的情况，是否对存储介质进行信息的不可恢复性销毁。
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。

测评单元（L2-MMS1-16）

该测评单元包括以下要求：
a) 测评指标：**应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有移动存储介质使用规范。
   2) 应核查是否具有移动存储介质的使用记录等。
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。

测评单元（L2-MMS1-17）

该测评单元包括以下要求：

a) 测评指标：**应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F2）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查是否具有定期对主要备份业务数据进行恢复验证的记录。

2) 应核查是否根据介质使用期限及时转储数据。

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。

6.1.10.4 设备维护管理

测评单元（L2-MMS1-18）

该测评单元包括以下要求：

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

b) 测评对象：设备管理员和管理制度类文档。

c) 测评实施包括以下内容：

1) 应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护。

2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。

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

测评单元（L2-MMS1-19）

该测评单元包括以下要求：

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

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

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

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

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

测评单元（L2-MMS1-20）

该测评单元包括以下要求：

a) 测评指标：**新购置的设备应经过验收，验收合格后方能投入使用。（F2）**

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查设备维护管理制度是否明确新购置的设备应经过验收，验收合格后方能投入使用。

2) 应核查新购置设备的验收报告和使用记录。

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

测评单元（L2-MMS1-21）

该测评单元包括以下要求：

a) 测评指标：**应制定设备管理规范，落实设备使用者的安全保护责任。（F2）**

b) 测评对象：管理制度类文档。

c) 测评实施：应核查设备管理规范是否落实设备使用者的安全保护责任。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-22）

该测评单元包括以下要求：
a) 测评指标：**需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复性销毁处理；信息消除处理仅限于废止设备仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查设备维护管理制度是否要求废止的设备应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等。
   2) 应核查是否具有废止设备的销毁记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-23）

该测评单元包括以下要求：
a) 测评指标：**设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前应请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查设备维护管理制度是否要求设备送外单位维修应彻底清除所存的工作相关信息并拆除与密码有关的硬件。
   2) 应核查是否与设备维修厂商签订保密协议。
   3) 应核查密码设备配套使用的设备送修前是否请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。
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。

测评单元（L2-MMS1-24）

该测评单元包括以下要求：
a) 测评指标：**应制定规范化的故障处理流程，建立详细的故障日志（包括故障发生的时间、范围、现象、处理结果和处理人员等内容）。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查设备故障处理制度是否包含规范化的故障处理流程。
   2) 应核查故障日志是否包括故障发生的时间、范围、现象、处理结果和处理人员等内容。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.10.5 漏洞和风险管理

测评单元（L2-MMS1-25）

该测评单元包括以下要求：
a) 测评指标：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：
   1) 应核查是否有识别安全漏洞和隐患的安全报告或记录（如漏洞扫描报告、渗透测试报告和安全通报等）。
   2) 应核查相关记录是否对发现的漏洞及时进行修补或评估可能的影响后进行修补。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.10.6 网络和系统安全管理

测评单元（L2-MMS1-26）

该测评单元包括以下要求：
a) 测评指标：应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查网络和系统安全管理文档，是否划分了网络和系统管理员等不同角色，并定义各个角色的责任和权限。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-27）

该测评单元包括以下要求：
a) 测评指标：应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理。
   2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-28）

该测评单元包括以下要求：
a) 测评指标：应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略、账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与打补丁、审计日志管理、登录设备和系统的口令更新周期等方面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-29）

该测评单元包括以下要求：
a) 测评指标：应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
b) 测评对象：操作规程类文档。
c) 测评实施：应核查重要设备或系统（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、参数配置等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-30）

该测评单元包括以下要求：

a) 测评指标：应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-31）

该测评单元包括以下要求：

a) 测评指标：**应对网络环境运行状态进行巡检，保留记录，并由操作人员和复核人员确认。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有网络环境运行状态巡检记录。
   2) 应核查巡检记录是否有操作人员和复核人员确认的相关信息。
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。

测评单元（L2-MMS1-32）

该测评单元包括以下要求：

a) 测评指标：**金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F2）**
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统管理员网间互联安全是否实行统一规范、分级管理、各负其责的安全管理模式。
   2) 应核查与外部机构实施网间互联时是否具有审批记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-33）

该测评单元包括以下要求：

a) 测评指标：**应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。（F2）**
b) 测评对象：系统管理员、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) 应访谈系统管理员是否制定远程访问控制规范。
   2) 应核查远程访问控制规范是否明确要求严禁跨境远程连接，严格控制国内远程访问范围。
   3) 确因工作需要进行远程访问的，应核查是否具有审批记录。
   4) 应核查远程访问操作过程中是否保留不可篡改的审计日志。
   5) 应核查是否针对远程访问采取了单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。
d) 单元判定：如果1）～5）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。

测评单元（L2-MMS1-34）

该测评单元包括以下要求：

a) 测评指标：**各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查网络安全管理制度是否明确规定未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。
   2) 应核查多媒体使用批准记录是否与管理制度要求一致。
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。

测评单元（L2-MMS1-35）

该测评单元包括以下要求：
a) 测评指标：**网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不应对外公开，未经科技主管部门授权，任何外部机构与人员不应检测或扫描机构内部网络。（F2）**
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) 应核查网络安全管理制度是否明确规定网络安全管理人员经本部门主管领导批准后，才能对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息未经授权不得对外公开。
   2) 应核查安全检测、扫描等批准记录是否与管理制度要求一致。
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。

测评单元（L2-MMS1-36）

该测评单元包括以下要求：
a) 测评指标：**系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的，应征得业务部门审批，并详细记录维护信息过程。（F2）**
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) 应核查网络安全管理制度是否明确规定系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对系统数据库进行技术维护性操作的，应征得业务部门审批，并详细记录维护过程。
   2) 应核查业务数据维护操作的审批记录是否与管理制度要求一致。
   3) 应核查业务数据维护操作记录是否包括详细的维护信息过程。
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。

测评单元（L2-MMS1-37）

该测评单元包括以下要求：
a) 测评指标：**每年应至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补。（F2）**
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) 应核查网络安全管理规定是否明确要求每年至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补。
   2) 应核查系统漏洞扫描、修补记录是否与管理制度要求一致。
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。

6.1.10.7 恶意代码防范管理

测评单元（L2-MMS1-38）

该测评单元包括以下要求：

a) 测评指标：应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。
b) 测评对象：运维负责人和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识。
   2) 应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系统前进行恶意代码检查。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-39）

该测评单元包括以下要求：

a) 测评指标：应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查恶意代码防范管理制度是否包括防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-40）

该测评单元包括以下要求：

a) 测评指标：应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
b) 测评对象：安全管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否出现过大规模的病毒事件，如何处理。
   2) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-41）

该测评单元包括以下要求：

a) 测评指标：**客户端应统一安装病毒防治软件，设置用户口令和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。（F2）**
b) 测评对象：安全管理员和客户端。
c) 测评实施包括以下内容：
   1) 应访谈安全管理员客户端是否统一安装了病毒防治软件，设置了用户口令和屏幕保护口令等安全防护措施，及时更新病毒特征码，以及安装了必要的补丁程序等。
   2) 应核查客户端病毒防治软件安装、用户口令设置、屏幕保护口令设置、病毒特征码更新以及补丁程序安装情况等是否与访谈结果一致。
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。

6.1.10.8 配置管理

测评单元（L2-MMS1-42）

该测评单元包括以下要求：

a) 测评指标：应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
b) 测评对象：系统管理员。
c) 测评实施：应访谈系统管理员是否对基本配置信息进行记录和保存。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.10.9 密码管理

测评单元（L2-MMS1-43）

该测评单元包括以下要求：
a) 测评指标：应遵循密码相关的国家标准和行业标准。
b) 测评对象：安全管理员。
c) 测评实施：应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-44）

该测评单元包括以下要求：
a) 测评指标：应使用国家密码管理主管部门认证核准的密码技术和产品。
b) 测评对象：安全管理员。
c) 测评实施：应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。
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。

测评单元（L2-MMS1-45）

该测评单元包括以下要求：
a) 测评指标：**应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工。（F2）**
b) 测评对象：管理制度类文档和密钥管理人员。
c) 测评实施包括以下内容：
   1) 应核查密钥管理制度是否明确了密钥的产生、分发和接收、使用、存储、更新、销毁等方面的管理要求。
   2) 应核查密钥管理人员是否为本机构在编的正式员工。
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。

测评单元（L2-MMS1-46）

该测评单元包括以下要求：
a) 测评指标：**系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求。（F2）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查密码管理制度是否要求系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-47）

该测评单元包括以下要求：

a) 测评指标：**应支持各类环境中密码设备使用、管理权限分离。（F2）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查密码管理制度是否要求各类环境中密码设备使用、管理权限分离。
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。

6.1.10.10 变更管理

测评单元（L2-MMS1-48）

该测评单元包括以下要求：
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。
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查变更方案是否包含变更类型、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。

测评单元（L2-MMS1-49）

该测评单元包括以下要求：
a) 测评指标：**变更前应做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查变更方案是否要求变更前做好系统和数据的备份。
   2) 应核查是否具有数据备份记录和跟踪记录文档。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.10.11 备份与恢复管理

测评单元（L2-MMS1-50）

该测评单元包括以下要求：
a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等。
b) 测评对象：系统管理员和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统管理员有哪些需定期备份的业务信息、系统数据及软件系统。
   2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-51）

该测评单元包括以下要求：
a) 测评指标：应规定备份信息的备份方式、备份频度、存储介质、保存期等。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-52）

该测评单元包括以下要求：

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。
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文档是否根据数据的重要程度制定相应备份恢复策略和程序等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-53）

该测评单元包括以下要求：

a) 测评指标：**恢复及使用备份数据时需要提供相关口令密码的，应妥善保管口令密码密封与数据备份介质。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施：恢复及使用备份数据时需要提供相关口令密码的，应核查是否将口令密码密封后与数据备份介质一并妥善保管。
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。

测评单元（L2-MMS1-54）

该测评单元包括以下要求：

a) 测评指标：**应建立灾难恢复计划，定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。（F2）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否制定了灾难恢复计划。
   2) 应核查是否具有灾难恢复培训和灾难恢复演练记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.10.12 安全事件处置

测评单元（L2-MMS1-55）

该测评单元包括以下要求：

a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件。
b) 测评对象：运维负责人和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告。
   2) 应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-56）

该测评单元包括以下要求：

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。
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是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和响应流程等。

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

测评单元（L2-MMS1-57）

该测评单元包括以下要求：

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。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过程、经验教训、补救措施等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.10.13 应急预案管理

测评单元（L2-MMS1-58）

该测评单元包括以下要求：

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。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否制定了重要事件的应急预案（如针对机房、系统、网络等各个方面）。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS1-59）

该测评单元包括以下要求：

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。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否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是否记录演练时间、主要操作内容、演练结果等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-60）

该测评单元包括以下要求：

a) 测评指标：**突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F2）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查突发事件管理相关制度是否明确要求突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。
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。

测评单元（L2-MMS1-61）

该测评单元包括以下要求：

a) 测评指标：**突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F2）**

b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否由突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源。
   2) 应核查是否具有应急处置联络人名单并上报至本行业网络安全监管部门。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS1-62）

该测评单元包括以下要求：
a) 测评指标：**应定期对原有的应急预案重新评估，修订完善。（F2）**
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否具有管理制度规定定期对原有的应急预案重新评估。
   2) 应核查应急预案重新评估记录是否与管理要求一致。
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。

6.1.10.14 外包运维管理

测评单元（L2-MMS1-63）

该测评单元包括以下要求：
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。
b) 测评对象：运维负责人。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否有外包运维服务情况。
   2) 应访谈运维负责人外包运维服务单位是否符合国家有关规定。
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。

测评单元（L2-MMS1-64）

该测评单元包括以下要求：
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。
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是否明确约定外包运维的范围和工作内容。
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。

测评单元（L2-MMS1-65）

该测评单元包括以下要求：
a) 测评指标：**应要求外包运维服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F2）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有外包服务商的操作记录文档。
   2) 应核查操作记录文档的内容和保存期限是否满足事件分析、安全取证、独立审计和监督检查需要。
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。

测评单元（L2-MMS1-66）

该测评单元包括以下要求：

a) 测评指标：**应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F2）**

b) 测评对象：记录表单类文档。

c) 测评实施：应核查是否具有数据中心外包服务应急计划以应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形。

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

6.2 云计算安全测评扩展要求

6.2.1 安全物理环境

6.2.1.1 基础设施位置

测评单元（L2-PES2-01）

该测评单元包括以下要求：

a) 测评指标：应保证云计算基础设施位于中国境内。

b) 测评对象：机房管理员、办公场地、机房和平台建设方案。

c) 测评实施包括以下内容：

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

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

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

6.2.2 安全通信网络

6.2.2.1 网络架构

测评单元（L2-CNS2-01）

该测评单元包括以下要求：

a) 测评指标：应保证云计算平台不承载高于其安全保护等级的业务应用系统。

b) 测评对象：云计算平台和业务应用系统定级备案材料。

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

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

测评单元（L2-CNS2-02）

该测评单元包括以下要求：

a) 测评指标：应实现不同云服务客户虚拟网络之间的隔离。

b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台。

c) 测评实施包括以下内容：

1) 应核查云服务客户之间是否采取网络隔离措施。

2) 应核查云服务客户之间是否设置并启用网络资源隔离策略。

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

测评单元（L2-CNS2-03）

该测评单元包括以下要求：

a) 测评指标：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。
b) 测评对象：防火墙、入侵检测系统等安全设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云计算平台是否具备为云服务客户提供通信传输、边界防护、入侵防范等安全防护机制的能力。
   2) 应核查上述安全防护机制是否满足云服务客户的业务需求。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.2.3 安全区域边界

6.2.3.1 访问控制

测评单元（L2-ABS2-01）

该测评单元包括以下要求：

a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备。
c) 测评实施包括以下内容：
   1) 应核查是否在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
   2) 应核查是否设置了云计算平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略等。
   3) 应核查是否设置了云计算平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等。
   4) 应核查是否设置了不同云服务客户间访问控制规则和访问控制策略等。
   5) 应核查是否设置了云服务客户不同安全保护等级业务系统之间访问控制规则和访问控制策略等。
d) 单元判定：如果1）～5）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-ABS2-02）

该测评单元包括以下要求：

a) 测评指标：应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备。
c) 测评实施包括以下内容：
   1) 应核查是否在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
   2) 应核查不同安全等级网络区域边界的访问控制规则和访问控制策略是否有效。
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。

6.2.3.2 入侵防范

测评单元（L2-ABS2-03）

该测评单元包括以下要求：

a) 测评指标：应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：

1) 应核查是否采取了入侵防范措施对网络入侵行为进行防范，如部署抗 APT 攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件。
2) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件的规则库升级方式，核查规则库是否进行及时更新。
3) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能，以及报警功能和清洗处置功能。
4) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具有对 SQL 注入、跨站脚本等攻击行为的发现和阻断能力。
5) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否能够检测出具有恶意行为、过分占用计算资源和带宽资源等恶意行为的虚拟机。
6) 应核查云管理平台对云服务客户攻击行为的防范措施，核查是否能够对云服务客户的网络攻击行为进行记录，记录应包括攻击类型、攻击时间和攻击流量等内容。
7) 应核查云管理平台或入侵防范设备是否能够对云计算平台内部发起的恶意攻击或恶意外连行为进行限制，核查是否能够对内部行为进行监控。
8) 通过对外攻击发生器伪造对外攻击行为，核查云租户的网络攻击日志，确认是否正确记录相应的攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP 和攻击流量规模等内容。
9) 应核查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，确认其安全加固手段是否能够避免或减少虚拟化共享带来的安全漏洞。

d) 单元判定：如果1）～9）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。

测评单元（L2-ABS2-04）

该测评单元包括以下要求：

a) 测评指标：应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否部署网络攻击行为检测设备或相关组件对虚拟网络节点的网络攻击行为进行防范，并能记录攻击类型、攻击时间、攻击流量等。
   2) 应核查网络攻击行为检测设备或相关组件的规则库是否为最新。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-ABS2-05）

该测评单元包括以下要求：

a) 测评指标：应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。
b) 测评对象：虚拟机、宿主机、抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c) 测评实施：应核查是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量的检测功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.3.3 安全审计

测评单元（L2-ABS2-06）

该测评单元包括以下要求：

a) 测评指标：应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。

b) 测评对象：堡垒机和相关组件。
c) 测评实施：应核查云服务商（含第三方运维服务商）和云服务客户在远程管理时执行的远程特权命令是否有相关审计记录。
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。

测评单元（L2-ABS2-07）

该测评单元包括以下要求：
a) 测评指标：应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。
b) 测评对象：综合审计系统或相关组件。
c) 测评实施：应核查是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4 安全计算环境

6.2.4.1 访问控制

测评单元（L2-CES2-01）

该测评单元包括以下要求：
a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移。
b) 测评对象：虚拟机、虚拟机迁移记录和相关配置。
c) 测评实施包括以下内容：
   1) 应核查虚拟机迁移时访问控制策略是否随之迁移。
   2) 应核查是否具备虚拟机迁移记录及相关配置。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-CES2-02）

该测评单元包括以下要求：
a) 测评指标：应允许云服务客户设置不同虚拟机之间的访问控制策略。
b) 测评对象：虚拟机和安全组或相关组件。
c) 测评实施：应核查云服务客户是否能够设置不同虚拟机之间访问控制策略。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4.2 镜像和快照保护

测评单元（L2-CES2-03）

该测评单元包括以下要求：
a) 测评指标：应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
b) 测评对象：虚拟机镜像文件。
c) 测评实施：应核查是否对生成的虚拟机镜像采取必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。
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。

测评单元（L2-CES2-04）

该测评单元包括以下要求：
a) 测评指标：应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。

b) 测评对象：云管理平台和虚拟机镜像、快照或相关组件。
c) 测评实施：应核查是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4.3 数据完整性和保密性

测评单元（L2-CES2-05）

该测评单元包括以下要求：
a) 测评指标：应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
b) 测评对象：数据库服务器、数据存储设备和管理文档记录。
c) 测评实施包括以下内容：
   1) 应核查云服务客户数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内。
   2) 应核查上述数据出境时是否符合国家相关规定。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-CES2-06）

该测评单元包括以下要求：
a) 测评指标：应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限。
b) 测评对象：云管理平台、数据库、相关授权文档和管理文档。
c) 测评实施包括以下内容：
   1) 应核查云服务客户数据管理权限授权流程、授权方式、授权内容。
   2) 应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查是否有相关授权证明。
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。

测评单元（L2-CES2-07）

该测评单元包括以下要求：
a) 测评指标：应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
b) 测评对象：虚拟机。
c) 测评实施：应核查在虚拟资源迁移过程中，是否采取校验技术或密码技术等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
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。

6.2.4.4 数据备份恢复

测评单元（L2-CES2-08）

该测评单元包括以下要求：
a) 测评指标：云服务客户应在本地保存其业务数据的备份。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否提供备份措施保证云服务客户可以在本地备份其业务数据。
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。

测评单元（L2-CES2-09）

该测评单元包括以下要求：

a) 测评指标：应提供查询云服务客户数据及备份存储位置的能力。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4.5 剩余信息保护

测评单元（L2-CES2-10）

该测评单元包括以下要求：

a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
b) 测评对象：云计算平台。
c) 测评实施包括以下内容：
   1) 应核查虚拟机的内存和存储空间回收时，是否得到完全清除。
   2) 应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。
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。

测评单元（L2-CES2-11）

该测评单元包括以下要求：

a) 测评指标：云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。
b) 测评对象：云存储和云计算平台。
c) 测评实施：应核查当云服务客户删除业务应用数据时，云存储中所有副本是否被删除。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.5 安全建设管理

6.2.5.1 云服务商选择

测评单元（L2-CMS2-01）

该测评单元包括以下要求：

a) 测评指标：应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
b) 测评对象：系统建设负责人和服务合同。
c) 测评实施包括以下内容：
   1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云计算平台及云服务商。
   2) 应核查云服务商提供的相关服务合同是否明确其云计算平台具有与所承载的业务应用系统具有相应或高于的安全保护能力。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-CMS2-02）

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标。
b) 测评对象：服务水平协议或服务合同。

c) 测评实施：应核查服务水平协议或服务合同是否规定了云服务的各项服务内容和具体指标等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS2-03）

该测评单元包括以下要求：
a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
b) 测评对象：服务水平协议或服务合同。
c) 测评实施：应核查服务水平协议或服务合同中是否规定了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS2-04）

该测评单元包括以下要求：
a) 测评指标：应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
b) 测评对象：服务水平协议或服务合同。
c) 测评实施：应核查服务水平协议或服务合同是否明确服务合约到期时，云服务商完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.5.2 供应链管理

测评单元（L2-CMS2-05）

该测评单元包括以下要求：
a) 测评指标：应确保供应商的选择符合国家有关规定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查云服务商的选择是否符合国家的有关规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS2-06）

该测评单元包括以下要求：
a) 测评指标：应将供应链安全事件信息或威胁信息及时传达到云服务客户。
b) 测评对象：供应链安全事件报告或威胁报告。
c) 测评实施：应核查供应链安全事件报告或威胁报告是否及时传达到云服务客户，报告是否明确相关事件信息或威胁信息。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.6 安全运维管理

6.2.6.1 云计算环境管理

测评单元（L2-MMS2-01）

该测评单元包括以下要求：
a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。
b) 测评对象：运维设备、运维地点、运维记录和相关管理文档。

c) 测评实施：应核查运维地点是否位于中国境内，从境外对境内云计算平台实施远程运维操作的行为是否遵循国家相关规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3 移动互联安全测评扩展要求

6.3.1 安全物理环境

6.3.1.1 无线接入点的物理位置

测评单元（L2-PES3-01）

该测评单元包括以下要求：
a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。
b) 测评对象：无线接入网关设备。
c) 测评实施包括以下内容：
   1) 应核查物理位置与无线信号的覆盖范围是否合理。
   2) 应测试验证无线信号是否可以避免电磁干扰。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.2 安全通信网络

6.3.2.1 通信传输

测评单元（L2-CNS3-01）

该测评单元包括以下要求：
a) 测评指标：**应在移动终端与服务器之间建立安全的信息传输通道，并进行双向认证，例如使用有效安全版本的 TLS 或 IPSec 等协议。（F2）**
b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件的协议。
c) 测评实施：应劫持移动端与服务器之间传输协议，核查是否进行双向认证、传输协议类型和版本是否安全。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.3 安全区域边界

6.3.3.1 边界防护

测评单元（L2-ABS3-01）

该测评单元包括以下要求：
a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。
b) 测评对象：无线接入网关设备。
c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.3.2 访问控制

测评单元（L2-ABS3-02）

该测评单元包括以下要求：
a) 测评指标：无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

b) 测评对象：无线接入设备。
c) 测评实施：应核查是否开启接入认证功能，是否使用除 WEP 方式以外的其他方式进行认证，密钥长度不小于 8 位。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.3.3 入侵防范

测评单元（L2-ABS3-03）

该测评单元包括以下要求：
a) 测评指标：应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施：应核查是否能够检测非授权无线接入设备和移动终端的接入行为。
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。

测评单元（L2-ABS3-04）

该测评单元包括以下要求：
a) 测评指标：应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。
b) 测评对象：入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够对网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测。
   2) 应核查规则库版本是否及时更新。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-ABS3-05）

该测评单元包括以下要求：
a) 测评指标：应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
b) 测评对象：无线接入设备或相关组件。
c) 测评实施：应核查是否能够检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
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。

测评单元（L2-ABS3-06）

该测评单元包括以下要求：
a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。
b) 测评对象：无线接入设备和无线接入网关设备。
c) 测评实施：应核查是否关闭了 SSID 广播、WEP 认证等存在风险的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-ABS3-07）

该测评单元包括以下要求：
a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否分别使用了不同的鉴别密钥。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.4 安全计算环境

6.3.4.1 移动终端管控

测评单元（L2-CES3-01）

该测评单元包括以下要求：

a) 测评指标：**应保证移动终端安装、注册并运行终端管理客户端软件。（F2）**
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查移动终端是否安装、注册并运行移动终端客户端软件。
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。

测评单元（L2-CES3-02）

该测评单元包括以下要求：

a) 测评指标：**移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。（F2）**
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施包括以下内容：
   1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略。
   2) 应测试验证是否能够对移动终端进行远程锁定和远程擦除等。
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。

6.3.4.2 移动应用管控

测评单元（L2-CES3-03）

该测评单元包括以下要求：

a) 测评指标：应具有选择应用软件安装、运行的功能。
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查是否具有选择应用软件安装、运行的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CES3-04）

该测评单元包括以下要求：

a) 测评指标：应只允许可靠证书签名的应用软件安装和运行。
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查全部移动应用是否由可靠证书签名。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.4.3 访问控制

测评单元（L2-CES3-05）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。（F2）**
b) 测评对象：移动客户端权限。
c) 测评实施：应核查客户端应用软件向移动终端操作系统申请的权限是否是业务必须获取的权限。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.4.4 入侵防范

测评单元（L2-CES3-06）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。（F2）**
b) 测评对象：移动客户端软件防劫持能力。
c) 测评实施：应核查客户端应用软件在安装、启动、更新时是否对自身的完整性和真实性进行校验以抵御篡改、替换或劫持。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5 安全建设管理

6.3.5.1 移动应用软件采购

测评单元（L2-CMS3-01）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
b) 测评对象：移动终端。
c) 测评实施：应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-CMS3-02）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件由可靠的开发者开发。
b) 测评对象：移动终端。
c) 测评实施：应核查移动应用软件是否由可靠的开发者开发。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5.2 移动应用软件开发

测评单元（L2-CMS3-03）

该测评单元包括以下要求：

a) 测评指标：应对移动业务应用软件开发者进行资格审查。
b) 测评对象：系统建设负责人。
c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查。
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。

测评单元（L2-CMS3-04）

该测评单元包括以下要求：

a) 测评指标：应保证开发移动业务应用软件的签名证书合法性。
b) 测评对象：移动业务应用软件的签名证书。
c) 测评实施：应核查开发移动业务应用软件的签名证书是否具有合法性。
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。

6.4 物联网安全测评扩展要求

6.4.1 安全物理环境

6.4.1.1 感知节点设备物理防护

测评单元（L2-PES4-01）

该测评单元包括以下要求：

a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动等，**使用环境与外壳保护等级（IP 代码）范围一致。（F2）**

b) 测评对象：感知节点设备所处物理环境、设计文档或验收文档 。

c) 测评实施包括以下内容：

1) 应核查感知节点设备所处的物理环境、设计文档或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动、使用环境与外壳保护等级（IP 代码）等能力的说明，是否与实际情况一致。

2) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动、外壳保护（IP 代码）等的防护措施。

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

测评单元（L2-PES4-02）

该测评单元包括以下要求：

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

b) 测评对象:感知节点设备所处物理环境、设计文档或验收文档。

c) 测评实施包括以下内容：

1) 应核查感知节点设备所处物理环境、设计文档或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际保持一致。

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

b) 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。

测评单元（L2-PES4-03）

该测评单元包括以下要求：

a) 测评指标：**感知节点设备的部署应遵循封闭性原则，降低设备被非法拆除、非法篡改的风险。（F2）**

b) 测评对象：感知节点所处物理环境和设计或验收文档。

c) 测评实施包括以下内容：

1) 应核查关键感知节点设备所处环境是否遵循了封闭性原则。

2) 应核查关键感知节点是否存在防止非法拆除的物理防护措施。

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

6.4.1.2 感知网关节点设备物理安全要求

测评单元（L2-PES4-04）

该测评单元包括以下要求：

a) 测评指标：**关键感知网关节点设备应具有持久稳定的电力供应措施。（F2）**

b) 测评对象：关键感知网关节点设备的电力供应设计文档或验收文档。

c) 测评实施包括以下内容：

1) 应核查关键感知网关节点设备电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障关键感知网关节点设备长时间工作的电力供应措施。

2) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。

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。

测评单元（L2-PES4-05）

该测评单元包括以下要求：

a) 测评指标：**应保证关键感知网关节点设备所在物理环境具有良好的信号收发能力（如避免信道遭遇屏蔽）。（F2）**
b) 测评对象：关键感知网关节点设备所处物理环境、设计文档或验收文档。
c) 测评实施包括以下内容：
   1) 应核查关键感知网关节点设备所处物理环境的设计或验收文档，是否具有关键感知网关节点设备所处物理环境防强干扰、防屏蔽等能力的说明。
   2) 应核查关键感知网关节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等保护措施。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-PES4-06）

该测评单元包括以下要求：

a) 测评指标：**关键感知网关节点设备应具有定位装置。（F2）**
b) 测评对象：关键感知网关节点设备的功能和系统设计文档、产品白皮书。
c) 测评实施包括以下内容：
   1) 应核查关键感知网关节点设备是否有 GPS 或类似定位装置设备功能，是否采取了防强干扰、防阻挡屏蔽等措施。
   2) 应核查关键感知网关节点设备的定位功能是否有效和准确。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.2 安全区域边界

6.4.2.1 接入控制

测评单元（L2-ABS4-01）

该测评单元包括以下要求：

a) 测评指标：应保证只有授权的感知节点可以接入。
b) 测评对象：感知节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述。
   2) 应对边界和感知层网络进行渗透测试，测试验证是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。
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。

测评单元（L2-ABS4-02）

该测评单元包括以下要求：

a) 测评指标：**每个感知节点和感知网关节点应具备传感网络中唯一标识，且该标识不应被非授权访问所篡改。（F2）**
b) 测评对象：感知节点和感知网关节点设备的功能和系统设计文档、产品白皮书。
c) 测评实施包括以下内容：
   1) 应核查感知节点和感知网关节点设备的功能和系统设计文档、产品白皮书，是否可创建永久唯一标识符。
   2) 应核查感知节点和感知网关节点设备，创建的传感网络中唯一标识是否不可被非授权访问所篡改。

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。

测评单元（L2-ABS4-03）

该测评单元包括以下要求：

a) 测评指标：**具有指令接收功能的感知节点设备，应保证只有授权过的系统、终端可以对感知节点下发指令。（F2）**

b) 测评对象：感知节点设备和设计文档。

c) 测评实施包括以下内容：

1) 应核查感知节点设备接入机制设计文档是否具有防止非法系统、终端设备下发指令的设计内容。

2) 应对边界和感知层网络进行渗透测试，测试验证是否不存在非法下发指令的可能。

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。

测评单元（L2-ABS4-04）

该测评单元包括以下要求：

a) 测评指标：**由第三方平台提供感知节点、感知网关节点中转接入时，第三方平台的安全保护等级应不低于接入的物联网系统的安全保护等级。（F2）**

b) 测评对象：第三方平台和设计文档、安全保护等级报告。

c) 测评实施包括以下内容：

1) 应核查第三方平台和设计文档、安全保护等级报告是否具有网络接入认证措施实现说明。

2) 应核查第三方平台的安全保护等级是否不低于接入的物联网系统的安全保护等级。

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

6.4.2.2 入侵防范

测评单元（L2-ABS4-05）

该测评单元包括以下要求：

a) 测评指标：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。

b) 测评对象：感知节点设备和设计文档。

c) 测评实施包括以下内容：

1) 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明。

2) 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求。

3) 应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。

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。

测评单元（L2-ABS4-06）

该测评单元包括以下要求：

a) 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

b) 测评对象：网关节点设备和设计文档。

c) 测评实施包括以下内容：

1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明。

2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求。

3) 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。

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。

6.4.3 安全计算环境

6.4.3.1 感知节点设备安全

测评单元（L2-CES4-01）

该测评单元包括以下要求：

a) 测评指标：**应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。（F2）**

b) 测评对象：感知节点设备。

c) 测评实施包括以下内容：

1) 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更。

2) 应通过试图接入和控制传感网访问未授权的资源等方式，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。

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。

测评单元（L2-CES4-02）

该测评单元包括以下要求：

a) 测评指标：**应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力。（F2）**

b) 测评对象：网关节点设备（包括读卡器）。

c) 测评实施包括以下内容：

1) 应核查是否对连接的网关节点设备（包括读卡器）进行身份标识与鉴别，是否配置了符合安全策略的参数。

2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

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。

测评单元（L2-CES4-03）

该测评单元包括以下要求：

a) 测评指标：**应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。（F2）**

b) 测评对象：其他感知节点设备（包括路由节点）。

c) 测评实施包括以下内容：

1) 应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数。

2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

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

6.4.3.2 网关节点设备安全

测评单元（L2-CES4-04）

该测评单元包括以下要求：

a) 测评指标：**应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力。（F2）**

b) 测评对象：网关节点设备。

c) 测评实施包括以下内容：
   1) 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心）进行标识并配置了鉴别功能。
   2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
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。

测评单元（L2-CES4-05）

该测评单元包括以下要求：
a) 测评指标：**应具备过滤非法节点和伪造节点所发送的数据的能力。（F2）**
b) 测评对象：网关节点设备。
c) 测评实施包括以下内容：
   1) 应核查是否具备过滤非法节点和伪造节点发送的数据的功能。
   2) 应测试验证是否能够过滤非法节点和伪造节点发送的数据。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.4 安全运维管理

6.4.4.1 感知节点管理

测评单元（L2-MMS4-01）

该测评单元包括以下要求：
a) 测评指标：应指定人员**或使用自动化巡检手段**，定期**检查**感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。**（F2）**
b) 测评对象：维护记录。
c) 测评实施包括以下内容：
   1) 应访谈系统运维负责人，是否有专门的人员或自动化巡检系统对感知节点设备、网关节点设备进行定期维护。
   2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L2-MMS4-02）

该测评单元包括以下要求：
a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。
b) 测评对象：感知节点和网关节点设备安全管理文档。
c) 测评实施：应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L2-MMS4-03）

该测评单元包括以下要求：
a) 测评指标：**应在经过充分测试评估后，在不影响关键感知节点、感知网关节点安全稳定运行的情况下进行补丁、固件更新等工作。（F2）**
b) 测评对象：补丁、固件更新管理制度和测评评估记录。
c) 测评实施包括以下内容：

1） 应核查是否建立补丁、固件更新的操作规范等管理制度，明确进行补丁、固件更新前应经过充分测试评估。
2） 应核查补丁、固件更新前是否有相应的测试评估记录。

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

测评单元（L2-MMS4-04）

该测评单元包括以下要求：

a） 测评指标：**关键感知节点、感知网关节点应通过安全传输通道进行固件与补丁更新，在检测到异常时应能将结果上报至安全管理中心。（F2）**
b） 测评对象：关键感知节点、感知网关节点设备和系统设计文档。
c） 测评实施：应核查关键感知节点、感知网关节点设备是否通过安全传输通道进行固件与补丁更新并能将异常结果上报至安全管理中心。
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。

测评单元（L2-MMS4-05）

该测评单元包括以下要求：

a） 测评指标：**应对感知节点状态进行监测，发现异常时应定位处理。（F2）**
b） 测评对象：监测记录文档、监测数据分析报告。
c） 测评实施包括以下内容：
1） 应核查是否对感知节点设备状态进行监测，是否形成监测记录文档，是否组织人员对监测记录进行整理并保管。
2） 应核查发现异常时是否对监测记录进行分析、评审，形成监测数据分析报告并定位处理。
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。

7 第三级测评要求

7.1 安全测评通用要求

7.1.1 安全物理环境

7.1.1.1 物理位置选择

测评单元（L3-PES1-01）

该测评单元包括以下要求：

a） 测评指标：机房场地应选择在具有防震、防风和防雨等能力的建筑内。
b） 测评对象：记录表单类文档和机房。
c） 测评实施包括以下内容：
1） 应核查所在建筑物是否具有建筑物抗震设防审批文档。
2） 应核查机房是否不存在雨水渗漏。
3） 应核查机房门窗是否不存在因风导致的尘土严重。
4） 应核查屋顶、墙体、门窗和地面等是否没有破损开裂。
d） 单元判定：如果1）～4）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES1-02）

该测评单元包括以下要求：

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

c) 测评实施：应核查机房是否不位于所在建筑物的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-PES1-03）

该测评单元包括以下要求：
a) 测评指标：**机房应避开火灾危险程度高的区域，周围 100 米内不得有加油站、燃气站等危险建筑。（F3）**
b) 测评对象：机房。
c) 测评实施：应核查机房是否不位于火灾危险程度高的区域，周围 100 米内是否没有加油站、燃气站等危险建筑。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.1.2 物理访问控制

测评单元（L3-PES1-04）

该测评单元包括以下要求：
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。
b) 测评对象：机房电子门禁系统。
c) 测评实施包括以下内容：
   1) 应核查机房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能够控制、鉴别和记录进入的人员。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES1-05）

该测评单元包括以下要求：
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物理隔离装置，在重要区域前设置交付或安装等过渡区域。（F3）**
b) 测评对象：机房。
c) 测评实施包括以下内容：
   1) 应核查机房是否划分区域进行管理，是否在区域和区域之间设置物理隔离装置。
   2) 应核查机房是否在重要区域前设置交付或安装等过渡区域。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.3 防盗窃和防破坏

测评单元（L3-PES1-06）

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。

测评单元（L3-PES1-07）

该测评单元包括以下要求：

a) 测评指标：应将通信线缆铺设在隐蔽安全处。
b) 测评对象：机房通信线缆。
c) 测评实施：应核查机房内通信线缆是否铺设在隐蔽安全处，如桥架中等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-PES1-08）

该测评单元包括以下要求：

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，**非7*24小时人员值守和巡查的机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。（F3）**
b) 测评对象：机房防盗报警系统或视频监控系统。
c) 测评实施包括以下内容：
   1) 应核查机房是否设置机房防盗报警系统或有专人值守的视频监控系统。
   2) 应核查机房防盗报警系统或视频监控系统是否启用。
   3) 非7*24小时人员值守和巡查的机房，应核查机房主要出入口是否安装红外线探测设备等光电防盗设备，并核查光电防盗设备是否可以显示入侵部位以及驱动声光报警装置。
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。

测评单元（L3-PES1-09）

该测评单元包括以下要求：

a) 测评指标：**应建立机房视频监控系统和动环监控系统，并对监控内容进行记录，对机房风冷水电设备、消防设施、门禁系统等重要设施实行连续24小时全面监控，视频监控记录和门禁系统出入记录至少保存3个月。（F3）**
b) 测评对象：机房视频监控系统和动环监控系统。
c) 测评实施包括以下内容：
   1) 应核查机房是否配置视频监控系统和动环监控系统。
   2) 应核查视频监控系统和动环监控系统是否启用。
   3) 应核查视频监控系统和动环监控系统是否对机房风冷水电设备、消防设施、门禁系统等重要设施实行连续24小时全面监控，并核查视频监控记录和门禁系统出入记录是否至少保存3个月。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.4 防雷击

测评单元（L3-PES1-10）

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。

测评单元（L3-PES1-11）

该测评单元包括以下要求：

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。
b) 测评对象：机房防雷设施。

c) 测评实施包括以下内容：
   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，否则不符合本或部分符合本测评单元指标要求。

测评单元（L3-PES1-12）

该测评单元包括以下要求：
a) 测评指标：**机房应通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。（F3）**
b) 测评对象：机房防雷设施和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房防雷设施是否通过有关部门验收。
   2) 应核查是否具有防雷设施的定期维护和检测记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合本或部分符合本测评单元指标要求。

7.1.1.5 防火

测评单元（L3-PES1-13）

该测评单元包括以下要求：
a) 测评指标：机房应设置火灾自动消防系统，能够**通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式进行**自动检测火情、自动报警，并自动灭火。**（F3）**
b) 测评对象：机房防火设施。
c) 测评实施包括以下内容：
   1) 应核查机房内是否设置火灾自动消防系统。
   2) 应核查火灾自动消防系统是否可以通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式进行自动检测火情、自动报警并自动灭火。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES1-14）

该测评单元包括以下要求：
a) 测评指标：机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
b) 测评对象：机房验收类文档。
c) 测评实施：应核查机房验收文档是否明确相关建筑材料的耐火等级。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-PES1-15）

该测评单元包括以下要求：
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。
b) 测评对象：机房管理员和机房。
c) 测评实施包括以下内容：
   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。

测评单元（L3-PES1-16）

该测评单元包括以下要求：

a) 测评指标：**机房应备有一定数量的对电子设备影响小的手持式灭火器，消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发。（F3）**
b) 测评对象：机房和消防报警系统。
c) 测评实施包括以下内容：
   1) 应核查机房是否配备一定数量的对电子设备影响小的手持式灭火器。
   2) 应核查消防报警系统是否具有与空调系统、新风系统、门禁系统联动的功能，且一般工作状态为手动触发。
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。

测评单元（L3-PES1-17）

该测评单元包括以下要求：

a) 测评指标：**机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收，纸张、磁带和胶卷等易燃物品要放置于防火柜内。（F3）**
b) 测评对象：机房验收类文档和机房。
c) 测评实施包括以下内容：
   1) 应核查机房验收类文档，是否明确内部通道设置、装修装饰材料、设备线缆等满足消防验收要求。
   2) 应核查机房内纸张、磁带和胶卷等易燃物品是否放置于防火柜内。
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。

测评单元（L3-PES1-18）

该测评单元包括以下要求：

a) 测评指标：**主机房宜采用管网式洁净气体灭火系统，也可采用高压细水雾灭火系统， 应同时设置两种火灾探测器，且消防报警系统应与空调系统、新风系统、门禁系统、灭火系统联动，凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。（F3）**
b) 测评对象：机房灭火系统。
c) 测评实施包括以下内容：
   1) 应核查机房是否采用管网式洁净气体灭火系统或高压细水雾灭火系统。
   2) 应核查机房是否设置两种火灾探测器，且消防报警系统应与空调系统、新风系统、门禁系统、灭火系统联动。
   3) 应核查设置洁净气体灭火系统的机房是否配置了专用空气呼吸器或氧气呼吸器。
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。

测评单元（L3-PES1-19）

该测评单元包括以下要求：

a) 测评指标：**应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。（F3）**
b) 测评对象：机房管理制度和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房管理制度是否具有每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练的相关要求。
   2) 应核查是否具有消防培训和演练记录。
   3) 应核查是否具有消防设施的定期检查记录。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES1-20）

该测评单元包括以下要求：

a) 测评指标：**机房应设置消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用，在机房通道上应设置显著的消防标志。（F3）**

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房是否设置消防逃生通道，并核查机房内各分区到各消防通道的道路是否通畅。

2) 应核查消防逃生通道上是否设置显著的消防标志。

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

7.1.1.6 防水和防潮

测评单元（L3-PES1-21）

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。

测评单元（L3-PES1-22）

该测评单元包括以下要求：

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。

b) 测评对象：机房。

c) 测评实施包括以下内容：

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。

测评单元（L3-PES1-23）

该测评单元包括以下要求：

a) 测评指标：**为便于地下积水的转移，漏水隐患区域地面周围应设排水沟或地漏等排水设施，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。（F3）**

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房内漏水隐患区域地面周围是否设置排水沟或地漏等排水设施。

2) 当采用吊顶上布置空调风口时，应核查机房风口位置是否没有设置在设备正上方。

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。

测评单元（L3-PES1-24）

该测评单元包括以下要求：

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。

b) 测评对象：机房防水检测设施。

c) 测评实施包括以下内容：

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。

测评单元（L3-PES1-25）

该测评单元包括以下要求：

a) 测评指标：**应对温湿度调节设备安装漏水报警装置，并设置防水堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。（F3）**

b) 测评对象：机房防水检测设施。

c) 测评实施包括以下内容：

1) 应核查机房内是否对温湿度调节设备安装漏水报警装置，并设置防水堤。

2) 应核查冷却塔、泵、水箱等供水设备是否具有防冻、防火措施。

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

7.1.1.7 防静电

测评单元（L3-PES1-26）

该测评单元包括以下要求：

a) 测评指标：应采用防静电地板或地面并采用必要的接地防静电措施。

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房内是否安装了防静电地板或地面。

2) 应核查机房内是否采用了接地防静电措施。

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。

测评单元（L3-PES1-27）

该测评单元包括以下要求：

a) 测评指标：应采取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。

b) 测评对象：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。

测评单元（L3-PES1-28）

该测评单元包括以下要求：

a) 测评指标：**主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F3）**

b) 测评对象：机房。

c) 测评实施：应核查机房内主机房和辅助区内的工作台面是否采用导静电或静电耗散材料。

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

7.1.1.8 温湿度控制

测评单元（L3-PES1-29）

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：机房温湿度调节设施。

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。

测评单元（L3-PES1-30）

该测评单元包括以下要求：

a) 测评指标：**机房应采用专用温湿度调节设备，并应满足机房监控系统的要求。（F3）**

b) 测评对象：机房温湿度调节设施。

c) 测评实施包括以下内容：

1) 应核查机房内是否配备专用温湿度调节设备。

2) 应核查机房内温湿度调节设备是否满足机房监控系统的要求。

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

测评单元（L3-PES1-31）

该测评单元包括以下要求：

a) 测评指标：**温湿度调节设备的工作能力应满足机房负载要求，并应保有一定的余量。（F3）**

b) 测评对象：机房温湿度调节设施。

c) 测评实施包括以下内容：

1) 应核查机房内温湿度调节设备是否满足机房负载要求。

2) 应核查机房内温湿度调节设备是否保有一定的余量。

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

7.1.1.9 电力供应

测评单元（L3-PES1-32）

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。

测评单元（L3-PES1-33）

该测评单元包括以下要求：

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。

b) 测评对象：机房备用供电设施。

c) 测评实施包括以下内容：

1) 应核查机房是否配备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。

测评单元（L3-PES1-34）

该测评单元包括以下要求：

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。

b) 测评对象：机房供电设施。

c) 测评实施：应核查机房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。

测评单元（L3-PES1-35）

该测评单元包括以下要求：

a) 测评指标：**应提供应急供电设施，以备供电系统临时停电时启用，并确保应急供电设施能在UPS供电时间内到位，每年需进行应急供电设施的带负载模拟演练，并定期对备用电力供应设备及应急供电设施进行检修和维护，确保其能正常使用。（F3）**

b) 测评对象：机房应急供电设施和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查机房是否配备应急供电设施如备用发电机。

2) 应访谈应急供电设施是否能在UPS供电时间内到位。

3) 应核查是否具有应急供电设施带负载模拟演练的记录。

4) 应核查是否具有电力供应设备及应急供电设施定期检修和维护的记录。

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。

测评单元（L3-PES1-36）

该测评单元包括以下要求：

a) 测评指标：**UPS供电系统的冗余方式应采用N+1、N+2、2N、2（N+1）等方式，未建立备用发电机应急供电系统的单位，UPS后备时间至少1小时，已建立备用发电机应急供电系统的单位，UPS后备时间应满足至少15分钟以上。（F3）**

b) 测评对象：机房备用供电设施。

c) 测评实施包括以下内容：

1) 应核查机房UPS供电系统的冗余方式是否采用N+1、N+2、2N、2（N+1）等方式。

2) 对于未建立备用发电机应急供电系统的单位，应核查UPS后备时间是否满足至少一小时。

3) 对于已建立备用发电机应急供电系统的单位，应核查UPS后备时间是否满足至少15分钟以上。

d) 单元判定：如果1）和2）均为肯定或1）和3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES1-37）

该测评单元包括以下要求：

a) 测评指标：**机房内要求采用机房专用插座，市电、UPS电源插座分开，满足负荷使用要求。（F3）**

b) 测评对象：机房供电设施。

c) 测评实施包括以下内容：

1) 应核查机房是否采用机房专用插座，市电、UPS电源插座是否分开。

2) 应核查机房专用插座是否满足负荷使用要求。

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

测评单元（L3-PES1-38）

该测评单元包括以下要求：

a) 测评指标：**计算机系统应选用铜芯电缆，避免铜、铝混用，若不能避免时，应采用铜铝过渡头连接。（F3）**

b) 测评对象：机房供电设施。

c) 测评实施包括以下内容：

1) 应核查机房是否采用铜芯电缆，避免铜、铝混用。

2) 如果铜、铝混用，应核查是否采用铜铝过渡头连接。

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，否则不符合本测评单元指标要求。

测评单元（L3-PES1-39）

该测评单元包括以下要求：

a) 测评指标：**机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。（F3）**
b) 测评对象：机房。
c) 测评实施包括以下内容：
   1) 应核查机房是否设置应急照明和安全出口指示灯。
   2) 应核查供配电柜（箱）和分电盘内各种开关、手柄、按钮是否标志清晰。
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。

测评单元（L3-PES1-40）

该测评单元包括以下要求：
a) 测评指标：**机房重要区域、重要设备应提供UPS单独供电。（F3）**
b) 测评对象：机房备用供电设施。
c) 测评实施包括以下内容：
   1) 应核查机房重要区域、重要设备是否配备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) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.10 电磁防护

测评单元（L3-PES1-41）

该测评单元包括以下要求：
a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰。
b) 测评对象：机房线缆。
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。

测评单元（L3-PES1-42）

该测评单元包括以下要求：
a) 测评指标：应对关键设备实施电磁屏蔽。
b) 测评对象：机房关键设备。
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) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.2 安全通信网络

7.1.2.1 网络架构

测评单元（L3-CNS1-01）

该测评单元包括以下要求：
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，**如：业务处理能力能满足业务高峰期需要的50%以上。（F3）**
b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信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是否满足需要，如：业务处理能力能满足业务高峰期需要的50%以上。
   2) 应核查网络设备是否从未出现过因设备性能问题导致的宕机情况。
   3) 应测试验证设备是否满足业务高峰期需求。

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

测评单元（L3-CNS1-02）

该测评单元包括以下要求：

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。
b) 测评对象：综合网管系统等。
c) 测评实施包括以下内容：
   1) 应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量需要。
   2) 应测试验证网络带宽是否满足业务高峰期需求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CNS1-03）

该测评单元包括以下要求：

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。
b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否依据重要性、部门等因素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划分原则一致。
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。

测评单元（L3-CNS1-04）

该测评单元包括以下要求：

a) 测评指标：应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
b) 测评对象：网络拓扑。
c) 测评实施包括以下内容：
   1) 应核查网络拓扑图是否与实际网络运行环境一致。
   2) 应核查重要网络区域是否未部署在网络边界处。
   3) 应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、防火墙和设备访问控制列表（ACL）等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CNS1-05）

该测评单元包括以下要求：

a) 测评指标：应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性，**双线路设计时，宜由不同的电信运营商提供。（F3）**
b) 测评对象：网络管理员和网络拓扑。
c) 测评实施包括以下内容：
   1) 应核查是否有关键网络设备、安全设备和关键计算设备的硬件冗余（主备或双活等）和通信线路冗余。
   2) 应核查通信线路是否由不同电信运营商提供。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.2 通信传输

测评单元（L3-CNS1-06）

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，**并按照国家密码管理部门与行业有关要求使用密码算法。（F3）**

b) 测评对象：提供校验技术或密码技术功能的设备或组件。

c) 测评实施包括以下内容：

1) 应核查是否在数据传输过程中使用密码技术来保证其完整性。

2) 应核查完整性措施所使用的密码算法是否符合国家密码管理部门与行业有关要求。

3) 应测试验证密码技术设备或组件能否保证通信过程中数据的完整性。

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。

测评单元（L3-CNS1-07）

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保密性，**并按照国家密码管理部门与行业有关要求使用密码算法。（F3）**

b) 测评对象：提供校验技术功能的设备或组件。

c) 测评实施包括以下内容：

1) 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施。

2) 应核查保密技术措施使用的密码算法是否符合国家密码管理部门与行业有关要求。

3) 应测试验证在通信过程中是否对数据进行加密。

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

7.1.2.3 可信验证

测评单元（L3-CNS1-08）

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、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。

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、重要配置参数和通信应用程序等进行可信验证。

2) 应核查是否在应用程序的关键执行环节进行动态可信验证。

3) 应测试验证当检测到通信设备的可信性受到破坏后是否进行报警。

4) 应测试验证结果是否以审计记录的形式送至安全管理中心。

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

7.1.3 安全区域边界

7.1.3.1 边界防护

测评单元（L3-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。

测评单元（L3-ABS1-02）

该测评单元包括以下要求：

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检查或限制。
b) 测评对象：终端管理系统或相关设备。
c) 测评实施包括以下内容：
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。
2) 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。
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。

测评单元（L3-ABS1-03）

该测评单元包括以下要求：

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检查或限制。
b) 测评对象：终端管理系统或相关设备。
c) 测评实施：应核查是否采用技术措施防止内部用户存在非法外联行为。
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。

测评单元（L3-ABS1-04）

该测评单元包括以下要求：

a) 测评指标：应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
b) 测评对象：网络拓扑和无线网络设备。
c) 测评实施包括以下内容：
1) 应核查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) 应核查无线网络是否通过受控的边界防护设备接入到内部有线网络。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.2 访问控制

测评单元（L3-ABS1-05）

该测评单元包括以下要求：

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。
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) 应核查在网络边界或区域之间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。

测评单元（L3-ABS1-06）

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。

测评单元（L3-ABS1-07）

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) 测评实施包括以下内容：
   1) 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。
   2) 应测试验证访问控制策略中设定的相关配置参数是否有效。
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。

测评单元（L3-ABS1-08）

该测评单元包括以下要求：

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。（F3）**
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) 应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力，控制粒度是否为端口级。
   2) 应测试验证是否为进出数据流提供明确的允许/拒绝访问的能力。
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。

测评单元（L3-ABS1-09）

该测评单元包括以下要求：

a) 测评指标：应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
b) 测评对象：第二代防火墙等提供应用层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) 应核查是否部署访问控制设备并启用访问控制策略。
   2) 应测试验证设备访问控制策略是否能够对进出网络的数据流实现基于应用协议和应用内容的访问控制。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ABS1-10）

该测评单元包括以下要求：

a) 测评指标：**应对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。（F3）**

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) 应核查是否梳理网络设备自带端口并关闭不必要端口。

2) 应核查是否制定端口开放审批制度。

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

测评单元（L3-ABS1-11）

该测评单元包括以下要求：

a) 测评指标：**应定期检查并锁定或撤销网络设备中不必要的用户账号。（F3）**

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) 应核查是否定期检查网络设备的用户账号。

2) 应核查是否锁定或撤销不必要的用户账号。

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

7.1.3.3 入侵防范

测评单元（L3-ABS1-12）

该测评单元包括以下要求：

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。

b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查相关系统或组件是否能够检测从外部发起的网络攻击行为。

2) 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本。

3) 应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点。

4) 应测试验证相关系统或组件的配置信息或安全策略是否有效。

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。

测评单元（L3-ABS1-13）

该测评单元包括以下要求：

a) 测评指标：应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查相关系统或组件是否能够检测从内部发起的网络攻击行为。

2) 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本。

3) 应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点。

4) 应测试验证相关系统或组件的配置信息或安全策略是否有效。

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。

测评单元（L3-ABS1-14）

该测评单元包括以下要求：

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新型网络攻击行为的分析。
b) 测评对象：抗 APT 攻击系统、网络回溯系统和威胁情报检测系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否部署相关系统或组件对新型网络攻击进行检测和分析。
   2) 应测试验证是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。

测评单元（L3-ABS1-15）

该测评单元包括以下要求：

a) 测评指标：当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查相关系统或组件的记录是否包括攻击源 IP、攻击类型、攻击目标、攻击时间等相关内容。
   2) 应测试验证相关系统或组件的报警策略是否有效。
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。

测评单元（L3-ABS1-16）

该测评单元包括以下要求：

a) 测评指标：**应采取技术手段对高级持续威胁进行监测、发现。（F3）**
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施：应核查相关系统或组件是否采取技术手段对高级持续威胁进行监测、发现。
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。

测评单元（L3-ABS1-17）

该测评单元包括以下要求：

a) 测评指标：**应建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。（F3）**
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否建立安全防护技术手段能诱捕、欺骗攻击者。
   2) 应核查技术手段是否能对攻击者行为进行捕获和分析。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.4 恶意代码防范

测评单元（L3-ABS1-18）

该测评单元包括以下要求：

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。

b) 测评对象：防病毒网关和UTM等提供防恶意代码功能的系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查在关键网络节点处是否部署防恶意代码产品等技术措施。
   2) 应核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ABS1-19）

该测评单元包括以下要求：
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。
b) 测评对象：提供防垃圾邮件功能的系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查在关键网络节点处是否部署防垃圾邮件产品等技术措施。
   2) 应核查防垃圾邮件策略是否更新到最新版本。
   3) 应核查防垃圾邮件产品运行是否正常。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.5 安全审计

测评单元（L3-ABS1-20）

该测评单元包括以下要求：
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。
b) 测评对象：综合安全审计系统等。
c) 测评实施包括以下内容：
   1) 应核查是否部署了综合安全审计系统或类似功能的系统平台。
   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了审计。
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。

测评单元（L3-ABS1-21）

该测评单元包括以下要求：
a) 测评指标：**应记录无线网络接入行为，形成日志进行留存，保存时间不少于6个月。（F3）**
b) 测评对象：综合安全审计系统等。
c) 测评实施包括以下内容：
   1) 应核查是否有记录无线网络接入行为，并形成日志进行留存。
   2) 应核查日志保存时间不少于6个月。
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。

测评单元（L3-ABS1-22）

该测评单元包括以下要求：
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。
b) 测评对象：综合安全审计系统等。
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。

测评单元（L3-ABS1-23）

该测评单元包括以下要求：

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，**审计记录保存时间不少于6个月。（F3）**

b) 测评对象：综合安全审计系统等。

c) 测评实施包括以下内容：

1) 应核查是否采取了技术措施对审计记录进行保护。

2) 应核查是否采取技术措施对审计记录进行定期备份。

3) 应核查审计记录保存时间是否不少于6个月。

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。

测评单元（L3-ABS1-24）

该测评单元包括以下要求：

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。

b) 测评对象：综合安全审计系统等。

c) 测评实施：应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。

测评单元（L3-ABS1-25）

该测评单元包括以下要求：

a) 测评指标：**所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致。（F3）**

b) 测评对象：综合安全审计系统等。

c) 测评实施包括以下内容：

1) 应访谈网络安全管理员是否采用了技术手段进行网络设备时钟同步。

2) 应核查是否所有的审计手段都具备统一的时间戳。

3) 应抽查相关网络设备，核查是否时间一致。

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

7.1.3.6 可信验证

测评单元（L3-ABS1-26）

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、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。

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、重要配置参数和边界防护应用程序等进行可信验证。

2) 应核查是否在应用程序的关键执行环节进行动态可信验证。

3) 应测试验证当检测到边界设备的可信性受到破坏后是否进行报警。

4) 应测试验证结果是否以审计记录的形式送至安全管理中心。

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

7.1.4 安全计算环境

7.1.4.1 身份鉴别

测评单元（L3-CES1-01）

该测评单元包括以下要求：

a) 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，**应实现身份鉴别信息防窃取和防重用。静态口令应在8位以上，由字母、数字、符号等混合组成并每半年更换口令，不允许新设定的口令与前次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定期更换。（F3）**

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) 应核查用户身份鉴别信息是否具有防窃取和防重用措施。
5) 应核查除应用系统用户以外的用户静态口令是否满足8位以上，由字母、数字、符号混合组成并每半年更换一次，新设定的口令不允许与前次旧口令相同。
6) 应核查应用系统用户口令是否满足8位以上，由字母、数字、符号混合组成并定期更换。

d) 单元判定：如果1）～6）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。

测评单元（L3-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、**限制登录间隔**、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。**（F3）**

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、限制登录间隔等。
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。

测评单元（L3-CES1-03）

该测评单元包括以下要求：

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。

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：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。

测评单元（L3-CES1-04）

该测评单元包括以下要求：

a) 测评指标：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

b) 测评对象：终端和服务器等设备中的操作系统（包括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) 应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别：

2) 应核查其中一种鉴别技术是否使用密码技术来实现。

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

7.1.4.2 访问控制

测评单元（L3-CES1-05）

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) 应核查是否为用户分配了账户和权限及相关设置情况。

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。

测评单元（L3-CES1-06）

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，修改默认账户或**预设账户**的默认口令。**（F3）**

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或预设账户的默认口令。

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。

测评单元（L3-CES1-07）

该测评单元包括以下要求：

a) 测评指标：**应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。（F3）**

b) 测评对象：业务应用系统。

c) 测评实施包括以下内容：
   1) 应核查应用系统是否对首次登录的用户提示修改默认账户或预设账户的默认口令。
   2) 应核查是否已修改默认账户或预设账户的默认口令。
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。

测评单元（L3-CES1-08）

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) 应核查并测试多余的、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。

测评单元（L3-CES1-09）

该测评单元包括以下要求：
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。
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) 应核查是否进行角色划分。
   2) 应核查管理用户的权限是否已进行分离。
   3) 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。

测评单元（L3-CES1-10）

该测评单元包括以下要求：
a) 测评指标：**应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。（F3）**
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：应核查是否严格限制默认账户或预设账户的权限，如将默认账户或预设账户的权限设置为空权限或某单一功能专用权限等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CES1-11）

该测评单元包括以下要求：
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。

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) 应核查是否由授权主体（如管理用户）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) 应测试验证用户是否有可越权访问情形。
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。

测评单元（L3-CES1-12）

该测评单元包括以下要求：
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。
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：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。

测评单元（L3-CES1-13）

该测评单元包括以下要求：
a) 测评指标：应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
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) 应核查是否对重要主体和客体设置了安全标记。
   2) 应测试验证是否控制主体对有安全标记信息资源的访问。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.3 安全审计

测评单元（L3-CES1-14）

该测评单元包括以下要求：
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。
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) 应核查是否提供并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。

测评单元（L3-CES1-15）

该测评单元包括以下要求：

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。

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：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。

测评单元（L3-CES1-16）

该测评单元包括以下要求：

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，**审计记录保存时间应不少于 6 个月。（F3）**

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) 应核查是否采取了保护措施对审计记录进行保护。

2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

3) 应核查审计记录保持时间是否不少于 6 个月。

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。

测评单元（L3-CES1-17）

该测评单元包括以下要求：

a) 测评指标：应对审计进程进行保护，防止未经授权的中断。

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：应测试验证通过非审计管理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。

测评单元（L3-CES1-18）

该测评单元包括以下要求：

a) 测评指标：**对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。（F3）**

b) 测评对象：移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统等。

c) 测评实施：对于从互联网客户端登录的应用系统，应测试验证是否能在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。

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。

测评单元（L3-CES1-19）

该测评单元包括以下要求：

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，以确保审计分析的一致性与正确性。（F3）**

b) 测评对象：时钟服务器、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) 应核查是否具有唯一确定的时钟同步服务器。

2) 应核查系统的时间与时钟同步服务器时间是否一致。

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

7.1.4.4 入侵防范

测评单元（L3-CES1-20）

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) 应核查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。

测评单元（L3-CES1-21）

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。

测评单元（L3-CES1-22）

该测评单元包括以下要求：

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。

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：应核查配置文件或参数是否对终端接入范围进行限制。

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

测评单元（L3-CES1-23）

该测评单元包括以下要求：

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。
b) 测评对象：业务应用系统、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的内容是否包括数据有效性检验功能的内容或模块。
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。

测评单元（L3-CES1-24）

该测评单元包括以下要求：

a) 测评指标：应能**通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时**发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。**（F3）**
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、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等。
c) 测评实施包括以下内容：
   1) 应核查是否有使用漏洞扫描工具、人工漏洞排查分析等检查手段开展漏洞检查工作。
   2) 应核查是否不存在高风险漏洞或在充分测试评估后及时修补漏洞。
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。

测评单元（L3-CES1-25）

该测评单元包括以下要求：

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。
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、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等。
c) 测评实施包括以下内容：
   1) 应核查是否采取技术措施对重要节点进行入侵检测。
   2) 应核查是否能对严重入侵事件进行报警，如声音、邮件、短信等方式。
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。

测评单元（L3-CES1-26）

该测评单元包括以下要求：

a) 测评指标：**所有安全计算环境设备应全部专用化，不得进行与业务不相关的操作。（F3）**
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、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等。
c) 测评实施包括以下内容：
   1) 应核查各安全计算环境设备的业务用途是否专用化。
   2) 应核查各安全计算环境设备是否未进行过与业务用途不相关的操作。

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。

测评单元（L3-CES1-27）

该测评单元包括以下要求：

a) 测评指标：**应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3）**
b) 测评对象：移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统等。
c) 测评实施：应通过给系统人为制造一些故障（如系统异常），测试验证系统是否未在故障发生时将技术错误信息直接或间接反馈到前台界面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.4.5 恶意代码防范

测评单元（L3-CES1-28）

该测评单元包括以下要求：

a) 测评指标：应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，将其有效阻断**并定期统一进行升级和更新防恶意代码库。（F3）**
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）、移动终端、移动终端管理系统、移动终端管理客户端和控制设备等。
c) 测评实施包括以下内容：
   1) 应核查是否安装了防恶意代码软件或相应功能的软件，定期升级和更新防恶意代码库。
   2) 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为。
   3) 应核查当识别入侵和病毒行为时是否将其有效阻断。
d) 单元判定：如果 1）和 3）或 2）和 3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CES1-29）

该测评单元包括以下要求：

a) 测评指标：**应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3）**
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：应核查是否建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.4.6 可信验证

测评单元（L3-CES1-30）

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、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。
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、重要配置参数和应用程序等进行可信验证。
   2) 应核查是否在应用程序的关键执行环节进行动态可信验证。
   3) 应测试验证当检测到计算设备的可信性受到破坏后是否进行报警。
   4) 应测试验证结果是否以审计记录的形式送至安全管理中心。

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

7.1.4.7 数据完整性

测评单元（L3-CES1-31）

该测评单元包括以下要求：

a) 测评指标：应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。
c) 测评实施包括以下内容：
   1) 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性。
   2) 应测试验证应用系统在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，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。

测评单元（L3-CES1-32）

该测评单元包括以下要求：

a) 测评指标：应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。
c) 测评实施包括以下内容：
   1) 应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性。
   2) 应核查应用系统是否采用技术措施（如数据安全保护系统等）保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性。
   3) 应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，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) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.8 数据保密性

测评单元（L3-CES1-33）

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
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) 测评实施包括以下内容：
   1) 应核查系统设计文档，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性。
   2) 应通过嗅探等方式抓取传输过程中的数据包，测试验证鉴别数据、重要业务数据和重要个人信息等传输过程中是否进行了加密处理。
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。

测评单元（L3-CES1-34）

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于**系统**鉴别数据、重要业务数据**和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护其存储过程中的保密性。（F3）**

b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

c) 测评实施包括以下内容：

1) 应核查是否采用密码技术保证系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息在存储过程中的保密性。

2) 应核查是否采用技术措施（如数据安全保护系统等）保证系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息在存储过程中的保密性。

3) 应测试验证是否对指定的数据进行加密处理。

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

7.1.4.9 数据备份恢复

测评单元（L3-CES1-35）

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，**采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指标（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放，数据保存期限依照国家相关规定。（F3）**

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) 应核查备份策略设置是否合理、配置是否正确。

2) 应核查是否按照备份策略进行本地备份。

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。

5) 应核查备份介质是否场外存放。

6) 应核查备份数据保存期限是否满足国家相关规定。

d) 单元判定：如果 1）～6）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。

测评单元（L3-CES1-36）

该测评单元包括以下要求：

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。。

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。

测评单元（L3-CES1-37）

该测评单元包括以下要求：

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。
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（包括边界路由器、边界防火墙、核心交换机、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。

测评单元（L3-CES1-38）

该测评单元包括以下要求：
a) 测评指标：**对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F3）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否建立了同城应用级灾难备份中心，且与生产中心直线距离至少达到30km。
   2) 应核查同城应用级灾难备份中心是否可以接管所有核心业务的运行。
   3) 应核查是否建立了异地应用级灾难备份中心，且与生产中心直线距离至少达到100km。
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。

测评单元（L3-CES1-39）

该测评单元包括以下要求：
a) 测评指标：**为满足灾难恢复策略的要求，应对关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。（F3）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否对关键技术应用的可行性进行验证测试。
   2) 应核查是否具有验证测试结果记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CES1-40）

该测评单元包括以下要求：
a) 测评指标：**数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星期为周期的数据冗余。（F3）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   1) 应核查数据备份是否至少保存两个副本，且至少一份副本异地存放。
   2) 应核查完全数据备份是否至少保证一个星期的数据冗余。
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。

测评单元（L3-CES1-41）

该测评单元包括以下要求：
a) 测评指标：**异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资源（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F3）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施：应核查异地灾难备份中心是否配备恢复所需的运行环境，并处于就绪状态或运行状态。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.4.10 剩余信息保护

测评单元（L3-CES1-42）

该测评单元包括以下要求：

a) 测评指标：应保证**操作系统、数据库系统和应用系统用户**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，**无论这些信息是存放在硬盘上还是内存中。（F3）**

b) 测评对象：终端和服务器等设备中的操作系统、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：应核查相关配置信息或系统设计文档，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。

测评单元（L3-CES1-43）

该测评单元包括以下要求：

a) 测评指标：应保证**操作系统、数据库系统和应用系统用户**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，**无论这些信息是存放在硬盘上还是内存中。（F3）**

b) 测评对象：终端和服务器等设备中的操作系统、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：应核查相关配置信息或系统设计文档，敏感数据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) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.4.11 个人信息保护

测评单元（L3-CES1-44）

该测评单元包括以下要求：

a) 测评指标：**金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F3）**

b) 测评对象：隐私政策。

c) 测评实施包括以下内容：

1) 应核查是否具有隐私政策。

2) 应核查隐私政策中是否向个人金融信息主体明示收集、使用信息的目的、方式和范围。

3) 应核查隐私政策是否获得个人信息主体的明示同意。

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。

测评单元（L3-CES1-45）

该测评单元包括以下要求：

a) 测评指标：应仅采集和保存业务必需的用户个人**金融**信息。**（F3）**

b) 测评对象：业务应用系统和数据库管理系统等。

c) 测评实施包括以下内容：

1) 应核查采集和保存的用户个人金融信息是否是业务应用必需的。

2) 应核查是否制定了有关用户个人金融信息保护的管理制度和流程。

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。

测评单元（L3-CES1-46）

该测评单元包括以下要求：

a) 测评指标：**应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限**应禁止未授权访问和非法使用用户个人**金融**信息。**（F3）**

b) 测评对象：业务应用系统和数据库管理系统等。

c) 测评实施包括以下内容：

1) 应核查是否采用技术措施限制对用户个人金融信息的访问和使用。

2) 应核查是否根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理。

3) 应核查是否制定了有关用户个人金融信息保护的管理制度和流程。

4) 应验证未经授权是否不能访问用户个人金融信息。

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。

测评单元（L3-CES1-47）

该测评单元包括以下要求：

a) 测评指标：**金融机构应依据JR/T 0171—2020对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3）**

b) 测评对象：个人金融信息、个人金融信息全生命周期管理相关规范、个人金融信息生命周期过程进行安全检查与评估的相关文档等。

c) 测评实施包括以下内容：

1) 应访谈是否对个人金融信息生命周期过程进行安全检查与评估。

2) 应核查是否具有个人金融信息生命周期过程进行安全检查与评估的报告。

3) 应核查是否对个人金融信息生命周期过程的安全检查与评估中发现的高风险问题进行补充测试。

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。

测评单元（L3-CES1-48）

该测评单元包括以下要求：

a) 测评指标：**金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F3）**

b) 测评对象：计算机屏幕、客户端软件、银行卡受理设备、ATM设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等可能展示个人金融信息的界面。

c) 测评实施包括以下内容：

1) 应访谈并核查个人金融信息以何种方式展示，如计算机屏幕、客户端软件、银行卡受理设备、ATM设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等。

2) 应核查展示个人金融信息的界面是否采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。

d) 单元判定：如果2）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。

测评单元（L3-CES1-49）

该测评单元包括以下要求：

a) 测评指标：**应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3）**

b) 测评对象：隐私政策和个人金融信息。

c) 测评实施包括以下内容：

1) 应访谈并核查是否存在个人金融信息共享、转让的情况。

2) 查看用户隐私政策，是否明确告知个人金融信息主体共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力。
3) 应核查隐私政策是否获得个人信息主体的明示同意。
4) 应核查共享、转让的个人金融信息是否经去标识化处理，且数据接收方无法重新识别个人金融信息主体。

d) 单元判定：如果 1）为否定，则不适用本测评单元指标要求，如果 1）～3）均为肯定或 4）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。

测评单元（L3-CES1-50）

该测评单元包括以下要求：

a) 测评指标：**开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3）**
b) 测评对象：开发环境、测试环境、开发和测评环境中使用的数据。
c) 测评实施包括以下内容：
1) 应核查系统开发环境和测试环境中的数据是否使用虚构的个人金融信息。
2) 如果使用真实的个人金融信息，是否对真实的个人金融信息进行去标识化处理，账号、卡号、协议号、支付指令等测试确需除外。
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，否则不符合本测评单元指标要求。

7.1.5 安全管理中心

7.1.5.1 系统管理

测评单元（L3-SMC1-01）

该测评单元包括以下要求：

a) 测评指标：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。
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施包括以下内容：
1) 应核查是否对系统管理员进行身份鉴别。
2) 应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作。
3) 应核查是否对系统管理的操作进行审计。
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。

测评单元（L3-SMC1-02）

该测评单元包括以下要求：

a) 测评指标：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、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施：应核查是否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、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-SMC1-03）

该测评单元包括以下要求：

a) 测评指标：**应每月对设备的配置文件进行备份，发生变动时应及时备份。（F3）**
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施包括以下内容：

1） 应核查是否每月对设备的配置文件进行备份。
2） 应核查系统发生变动时是否及时备份。

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。

测评单元（L3-SMC1-04）

该测评单元包括以下要求：

a） 测评指标：**应使用自动化技术手段对设备运行状况进行实时监测，运维人员应每天定期查看并记录系统运行状况。（F3）**
b） 测评对象：提供集中系统管理功能的系统和运维人员。
c） 测评实施包括以下内容：
1） 应核查是否使用自动化手段对设备的运行状况进行监测。
2） 应核查运维人员是否每天定期查看并记录系统运行状况。
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。

测评单元（L3-SMC1-05）

该测评单元包括以下要求：

a） 测评指标：**应每季度检验网络设备软件版本信息，并通过有效测试验证后进行相应的升级，同时留存测试验证相关记录。（F3）**
b） 测评对象：提供集中系统管理功能的系统。
c） 测评实施包括以下内容：
1） 应核查是否每季度检验网络设备软件版本信息，并通过有效测试验证后进行相应的升级。
2） 应核查是否有具有网络设备软件版本升级测试验证相关记录。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.5.2 审计管理

测评单元（L3-SMC1-06）

该测评单元包括以下要求：

a） 测评指标：应对审计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审计操作，并对这些操作进行审计。
b） 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c） 测评实施包括以下内容：
1） 应核查是否对审计管理员进行身份鉴别。
2） 应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作。
3） 应核查是否对审计管理员的操作进行审计。
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。

测评单元（L3-SMC1-07）

该测评单元包括以下要求：

a） 测评指标：应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
b） 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c） 测评实施：应核查是否通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-SMC1-08）

该测评单元包括以下要求：

a) 测评指标：**应严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审计用户的权限分离，避免非授权的删除、修改或覆盖。（F3）**

b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问。

2) 应核查管理用户和审计用户的权限是否分离。

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

7.1.5.3 安全管理

测评单元（L3-SMC1-09）

该测评单元包括以下要求：

a) 测评指标：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，并对这些操作进行审计。

b) 测评对象：提供集中安全管理功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否对安全管理员进行身份鉴别。

2) 应核查是否只允许安全管理员通过特定的命令或操作界面进行安全审计操作。

3) 应核查是否对安全管理操作进行审计。

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。

测评单元（L3-SMC1-10）

该测评单元包括以下要求：

a) 测评指标：应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

b) 测评对象：提供集中安全管理功能的系统。

c) 测评实施：应核查是否通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

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

7.1.5.4 集中管控

测评单元（L3-SMC1-11）

该测评单元包括以下要求：

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。

b) 测评对象：网络拓扑。

c) 测评实施包括以下内容：

1) 应核查是否划分出单独的网络区域用于部署安全设备或安全组件。

2) 应核查各个安全设备或安全组件是否集中部署在单独的网络区域内。

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。

测评单元（L3-SMC1-12）

该测评单元包括以下要求：

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。

b) 测评对象：路由器、交换机和防火墙等设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否采用安全方式（如 SSH、HTTPS、IPSec VPN 等）对安全设备或安全组件进行管理。
   2) 应核查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，否则不符合本测评单元指标要求。

测评单元（L3-SMC1-13）

该测评单元包括以下要求：
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。
b) 测评对象：综合网管系统等提供运行状态监测功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、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) 应测试验证运行状态监测系统是否根据网络链路、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。

测评单元（L3-SMC1-14）

该测评单元包括以下要求：
a) 测评指标：应对分散在各个设备上的**安全事件**、审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。**（F3）**
b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c) 测评实施包括以下内容：
   1) 应核查各个设备是否配置并启用了相关策略，将安全事件、审数据发送到独立于设备自身的外部集中安全审计系统中。
   2) 应核查是否部署统一的集中安全审计系统，统一收集和存储各设备日志，并根据需要进行集中审计分析。
   3) 应核查审记录的留存时间是否至少为 6 个月。
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。

测评单元（L3-SMC1-15）

该测评单元包括以下要求：
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。
b) 测评对象：提供集中安全管控功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否能够对安全策略（如防火墙访回控制策略、入侵保护系统防护策略、WAF 安全防护策略等）进行集中管理。
   2) 应核查是否实现对操作系统防恶意代码系统及网络恶意代码防护设备的集中管理，实现对防恶意代码病毒规则库的升级进行集中管理。
   3) 应核查是否实现对各个系统或设备的补丁升级进行集中管理。
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。

测评单元（L3-SMC1-16）

该测评单元包括以下要求：
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、分析**、响应和处置**。**（F3）**
b) 测评对象：提供集中安全管控功能的系统。
c) 测评实施包括以下内容：

1) 应核查是否部署了相关系统平台能够对各类安全事件进行分析、响应和处置，并通过声光等方式实时报警。
2) 应核查监测范围是否能够覆盖网络所有关键路径。

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

7.1.6 安全管理制度

7.1.6.1 安全策略

测试单元（L3-PSS1-01）

该测评单元包括以下要求：

a) 测评指标：应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等，**并编制形成网络安全方针制度文件。（F3）**
b) 测评对象：总体方针策略类文档。
c) 测评实施：应核查网络安全工作的总体方针和安全策略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) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.6.2 管理制度

测评单元（L3-PSS1-02）

该测评单元包括以下要求：

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。
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物理、网络、主机系统、数据、应用、建设和运维等管理内容。
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。

测评单元（L3-PSS1-03）

该测评单元包括以下要求：

a) 测评指标：应对管理人员或操作人员执行的日常管理操作建立操作规程。
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。

测评单元（L3-PSS1-04）

该测评单元包括以下要求：

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安全管理制度体系。
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、记录表单是否全面且具有关联性和一致性。
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。

7.1.6.3 制定和发布

测评单元（L3-PSS1-05）

该测评单元包括以下要求：

a) 测评指标：**金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应制定适用辖内的安全管理制度。（F3）**
b) 测评对象：部门/人员职责文件等。
c) 测评实施包括以下内容：
   1) 应核查适用全机构范围的安全管理制度是否在金融机构总部的总体负责下统一制定。
   2) 应核查各分支机构是否制定了适用辖内的安全管理制度。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PSS1-06）

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安全管理制度的制定。
b) 测评对象：部门/人员职责文件等。
c) 测评实施：应核查是否由专门的部门或人员负责制定安全管理制度。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-PSS1-07）

该测评单元包括以下要求：

a) 测评指标：安全管理制度应通过正式、有效的方式发布，并进行版本控制。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容。
   2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.4 评审和修订

测评单元（L3-PSS1-08）

该测评单元包括以下要求：

a) 测评指标：应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期对安全管理制度体系的合理性和适用性进行审定。
   2) 应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.7 安全管理机构

7.1.7.1 岗位设置

测评单元（L3-ORS1-01）

该测评单元包括以下要求：

a) 测评指标：**网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F3）**
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/网络安全主管是否建立了网络安全管理工作实行统一领导、分级管理模式。
   2) 应核查相关制度文档是否明确了总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。
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。

测评单元（L3-ORS1-02）

该测评单元包括以下要求：
a) 测评指标：**应设立由本机构领导、业务与技术相关部门主要负责人组成的**网络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担任或授权，**负责协调本机构及辖内网络安全管理工作，决策本机构及辖内网络安全重大事宜。（F3）**
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/网络安全主管是否成立了由本机构领导、业务与技术相关部门主要负责人组成的指导和管理网络安全工作的委员会或领导小组。
   2) 应核查相关文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责。
   3) 应核查委员会或领导小组的最高领导是否由单位主管领导担任或由其进行了授权。
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。

测评单元（L3-ORS1-03）

该测评单元包括以下要求：
a) 测评指标：应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。
b) 测评对象：信息/网络安全主管和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否设立网络安全管理工作的职能部门。
   2) 应核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责。
   3) 应核查岗位职责文档是否有岗位划分情况和岗位职责。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ORS1-04）

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

测评单元（L3-ORS1-05）

该测评单元包括以下要求：

a) 测评指标：**应设立专门的网络安全审计岗位，负责网络安全审计制度和流程的实施，制订和执行网络安全审计计划，对网络安全整个生命周期和重大事件等进行审计。（F3）**
b) 测评对象：信息/网络安全主管和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否设立了专门的网络安全审计岗位。
   2) 应核查岗位职责文档是否明确了网络安全岗位的职责，包括负责网络安全审计制度和流程的实施，制订和执行网络安全审计计划，对网络安全整个生命周期和重大事件等进行审计。
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。

测评单元（L3-ORS1-06）

该测评单元包括以下要求：
a) 测评指标：**应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。（F3）**
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/网络安全主管是否实现前后台分离、开发与操作分离、技术与业务分离。
   2) 应核查岗位职责文档是否明确了信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。
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。

测评单元（L3-ORS1-07）

该测评单元包括以下要求：
a) 测评指标：**除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开展本部门的网络安全管理工作。（F3）**
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，网络安全管理部门外的其他部门是否指定至少一名部门网络安全员。
   2) 应核查岗位职责文档是否明确了部门网络安全员需协助网络安全管理部门开展本部门的网络安全管理工作。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.7.2 人员配备

测评单元（L3-ORS1-08）

该测评单元包括以下要求：
a) 测评指标：应配备一定数量的系统管理员、审计管理员和安全管理员等。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否配备了系统管理员、审计管理员和安全管理员。
   2) 应核查人员配备文档是否明确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。

测评单元（L3-ORS1-09）

该测评单元包括以下要求：
a) 测评指标：应配备专职安全管理员，**实行 A、B 岗制度，**不可兼任。**（F3）**

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：应核查人员配备文档是否明确配备了专职安全管理员且设置了A、B岗。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.3 授权和审批

测评单元（L3-ORS1-10）

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。

测评单元（L3-ORS1-11）

该测评单元包括以下要求：
a) 测评指标：应针对**系统投入运行、重要资源（如敏感数据等资源）的访问、**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。**（F3）**
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) 应核查系统投入运行、重要资源（如敏感数据等资源）的访问、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是否明确建立了逐级审批程序。
   2) 应核查审批记录操作记录，审批结果是否与相关制度一致。
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。

测评单元（L3-ORS1-12）

该测评单元包括以下要求：
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。
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) 应访谈信息/网络安全主管是否具有授权和审批的项目、审批部门和审批人等信息的更新记录。
   2) 应核查是否具有定期审查审批事项的记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ORS1-13）

该测评单元包括以下要求：
a) 测评指标：**用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系，权限变更应执行相关审批流程，并有完整的变更记录。（F3）**
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/网络安全主管是否根据最小权限原则对用户授权，重要岗位的员工之间是否形成相互制约的关系。
   2) 应核查是否具有权限变更的相关审批流程和完整的变更记录。

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

7.1.7.4 沟通和合作

测评单元（L3-ORS1-14）

该测评单元包括以下要求：

a) 测评指标：应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否建立了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制。
   2) 应核查会议记录是否明确在各类管理人员、组织内部机构和网络安全管理部门之间开展了合作与沟通。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ORS1-15）

该测评单元包括以下要求：

a) 测评指标：应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否建立了与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制。
   2) 应核查会议记录是否明确了与网络安全职能部门、各类供应商、业界专家及安全组织开展了合作与沟通。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ORS1-16）

该测评单元包括以下要求：

a) 测评指标：应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.5 审核和检查

测评单元（L3-ORS1-17）

该测评单元包括以下要求：

a) 测评指标：应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期进行了常规安全检查。
   2) 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ORS1-18）

该测评单元包括以下要求：

a) 测评指标：应定期进行全面安全检查，检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。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期进行了全面安全检查。
   2) 应核查全面安全检查记录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。

测评单元（L3-ORS1-19）

该测评单元包括以下要求：

a) 测评指标：**应建立对门户网站内容发布的审核、管理和监控机制。（F3）**
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否建立了门户网站内容发布的审核、管理和监控机制。
   2) 应核查是否具有门户网站内容发布的审核记录。
d) 单元判定：如果以上测评实施内容肯定，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。

测评单元（L3-ORS1-20）

该测评单元包括以下要求：

a) 测评指标：应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对安全检查结果进行通报并报上一级机构科技部门备案。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录和报上一级机构科技部门备案的记录。
   2) 对于安全检查后要求限期整改的，应核查是否具有整改落实情况相关记录文档。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ORS1-21）

该测评单元包括以下要求：

a) 测评指标：**应制定违反和拒不执行安全管理措施规定的处罚细则。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否具有违反和拒不执行安全管理措施规定的处罚细则。
d) 单元判定：如果以上测评实施内容肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8 安全管理人员

7.1.8.1 人员录用

测评单元（L3-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。

测评单元（L3-HRS1-02）

该测评单元包括以下要求：
a) 测评指标：应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）。
   2) 应核查是否具有人员录用时对录用人身份、安全背景、专业资格或资质等进行审查的相关文档或记录，是否记录审查内容和审查结果等。
   3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-HRS1-03）

该测评单元包括以下要求：
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。
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查保密协议是否有保密范围、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。

测评单元（L3-HRS1-04）

该测评单元包括以下要求：
a) 测评指标：**应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F3）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否有网络安全管理人员的备案制度。
   2) 应核查相关备案记录，网络安全管理人员的配备变更情况是否报上一级科技部门备案，金融机构总部网络安全管理人员是否在总部科技部门备案。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-HRS1-05）

该测评单元包括以下要求：
a) 测评指标：**凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不应从事网络安全管理工作。（F3）**
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：应核查网络安全管理人员是否无因违反国家法律法规和金融机构有关规定而受到处罚或处分的记录。

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

7.1.8.2 人员离岗

测评单元（L3-HRS1-06）

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。

测评单元（L3-HRS1-07）

该测评单元包括以下要求：

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。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查人员离岗的管理文档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是否有调离人员的签字。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.3 人员考核

测评单元（L3-HRS1-08）

该测评单元包括以下要求：

a) 测评指标：**应定期对各个岗位的人员进行安全技能及安全认知的考核。（F3）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查人员考核的管理文档是否明确要求定期对各个岗位的人员进行安全技能及安全认知的考核。
   2) 应核查是否具有安全技能及安全认知考核记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-HRS1-09）

该测评单元包括以下要求：

a) 测评指标：**应对关键岗位的人员进行全面、严格的安全审查和技能考核。（F3）**
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：应访谈信息/网络安全主管是否对关键岗位的人员进行全面、严格的安全审查和技能考核，并核查是否具有审查和考核记录。
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。

测评单元（L3-HRS1-10）

该测评单元包括以下要求：

a) 测评指标：**应对考核结果进行记录并保存。（F3）**

b) 测评对象：记录表单类文档。
c) 测评实施：应核查考核记录，考核人员是否包括各个岗位的人员，考核内容是否包括安全知识、安全技能、安全认知等，记录日期与考核周期是否一致。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.4 安全意识教育和培训

测评单元（L3-HRS1-11）

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。

测评单元（L3-HRS1-12）

该测评单元包括以下要求：
a) 测评指标：应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查安全教育和培训计划文档是否具有不同岗位的培训计划。
   2) 应核查培训内容是否包含安全基础知识、岗位操作规程等。
   3) 应核查安全教育和培训记录是否有培训人员、培训内容、培训结果等描述。
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。

测评单元（L3-HRS1-13）

该测评单元包括以下要求：
a) 测评指标：**每年应至少对网络安全管理人员进行一次网络安全培训。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有对网络安全管理人员进行年度网络安全培训的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.5 外部人员访问管理

测评单元（L3-HRS1-14）

该测评单元包括以下要求：
a) 测评指标：应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等。
   2) 应核查外部人员访问重要区域的申请文档是否具有批准人允许访问的批准等。
   3) 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。

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

测评单元（L3-HRS1-15）

该测评单元包括以下要求：

a) 测评指标：应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程。
   2) 应核查外部人员访问系统的申请文档是否明确外部人员的访问权限，是否具有允许访问的批准等。
   3) 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-HRS1-16）

该测评单元包括以下要求：

a) 测评指标：**应对允许被外部人员访问的网络资源建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控。（F3）**
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) 应核查对允许被外部人员访问的网络资源，是否建立存取控制机制、认证机制。
   2) 应核查外部人员权限表单是否包括所有外部人员及其权限。
   3) 应核查外部人员访问活动是否受到监控。
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。

测评单元（L3-HRS1-17）

该测评单元包括以下要求：

a) 测评指标：外部人员离场后应及时清除其所有的访问权限。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限。
   2) 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-HRS1-18）

该测评单元包括以下要求：

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，不得进行非授权的**增加、删除、修改、查询数据等**操作，不得复制和泄露**金融机构的任何信息。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否与获得系统访问授权的外部人员签署了保密协议。
   2) 应核查保密协议中是否有禁止进行未授权的增加、删除、修改、查询数据操作，禁止复制和泄露金融机构的任何信息等相关要求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.9 安全建设管理

7.1.9.1 定级和备案

测评单元（L3-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。

测评单元（L3-CMS1-02）

该测评单元包括以下要求：

a) 测评指标：应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-03）

该测评单元包括以下要求：

a) 测评指标：应保证定级结果经过相关部门的批准。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-04）

该测评单元包括以下要求：

a) 测评指标：应将备案材料报主管部门和相应公安机关备案。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有公安机关出具的备案证明文档。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.9.2 安全方案设计

测评单元（L3-CMS1-05）

该测评单元包括以下要求：

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

测评单元（L3-CMS1-06）

该测评单元包括以下要求：

a) 测评指标：应根据保护对象的安全保护等级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，设计内容应包含密码技术相关内容，并形成配套文件。
b) 测评对象：安全规划设计类文档。
c) 测评实施：应核查是否有总体规划和安全设计方案等配套文件，设计方案中应包括密码技术相关内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-07）

该测评单元包括以下要求：
a) 测评指标：应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体安全规划、安全设计方案等相关配套文件的批准意见和论证意见。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.9.3 产品采购和使用

测评单元（L3-CMS1-08）

该测评单元包括以下要求：
a) 测评指标：应确保网络安全产品采购和使用符合国家的有关规定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查有关网络安全产品是否符合国家的有关规定，如网络安全产品获得了销售许可等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-09）

该测评单元包括以下要求：
a) 测评指标：应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈建设负责人是否采用了密码产品及其相关服务。
   2) 应核查密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CMS1-10）

该测评单元包括以下要求：
a) 测评指标：**各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有扫描、检查类网络安全产品购置前本机构科技主管部门的批准、备案记录。
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。

测评单元（L3-CMS1-11）

该测评单元包括以下要求：

a) 测评指标：应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-12）

该测评单元包括以下要求：
a) 测评指标：**扫描、检测类网络安全产品应仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查网络安全产品使用记录，是否仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。
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。

测评单元（L3-CMS1-13）

该测评单元包括以下要求：
a) 测评指标：**应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有定期对各类网络安全产品相关日志和报表信息进行汇总分析的记录或分析报告。
   2) 应核查一旦发现重大问题，是否具有相应的控制措施和报告程序。
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。

测评单元（L3-CMS1-14）

该测评单元包括以下要求：
a) 测评指标：**应定期对各类网络安全产品产生的日志和报表进行备份存档。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有对各类网络安全产品日志和报表进行定期备份存档的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-15）

该测评单元包括以下要求：
a) 测评指标：**应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。（F3）**
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) 应核查网络安全产品维护和报废相关管理制度中是否有及时升级维护规定以及报废审批流程。
   2) 应核查是否具有网络安全产品升级维护记录。
   3) 应核查对于超过使用期限或不能继续使用的网络安全产品是否具有报废、审批记录。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.9.4 自行软件开发

测评单元（L3-CMS1-16）

该测评单元包括以下要求：

a) 测评指标：**应将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试中使用。（F3）**

b) 测评对象：建设负责人。

c) 测评实施包括以下内容：

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

2) 应核查敏感数据是否脱敏后在开发或测试中使用。

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

测评单元（L3-CMS1-17）

该测评单元包括以下要求：

a) 测评指标：**应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制。（F3）**

b) 测评对象：建设负责人。

c) 测评实施包括以下内容：

1) 应访谈建设负责人开发人员和测试人员是否分离，开发人员是否未兼任系统管理员或业务操作人员。

2) 应核查测试数据和测试结果是否受控使用。

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

测评单元（L3-CMS1-18）

该测评单元包括以下要求：

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

b) 测评对象：管理制度类文档。

c) 测评实施：应核查软件开发管理制度是否明确软件设计、开发、测试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。

测评单元（L3-CMS1-19）

该测评单元包括以下要求：

a) 测评指标：应制定代码编写安全规范，要求开发人员参照规范编写代码。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查代码编写安全规范是否明确代码安全编写规则。

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

测评单元（L3-CMS1-20）

该测评单元包括以下要求：

a) 测评指标：应具备软件设计的相关文档和使用指南，并对文档使用进行控制。

b) 测评对象：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，并对文档使用进行控制。

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

测评单元（L3-CMS1-21）

该测评单元包括以下要求：

a) 测评指标：应保证在软件开发过程中对**代码规范、代码质量、代码安全性进行审查**，在软件安装前对可能存在的恶意代码进行检测。**（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-22）

该测评单元包括以下要求：

a) 测评指标：应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查对程序资源库的修改、更新、发布进行授权和审批的文档或记录是否有批准人的签字。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-23）

该测评单元包括以下要求：

a) 测评指标：应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
b) 测评对象：建设负责人。
c) 测评实施：应访谈建设负责人开发人员是否为专职，是否对开发人员活动进行控制等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-24）

该测评单元包括以下要求：

a) 测评指标：**在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查在软件开发过程中是否同步完成相关文档手册的编写工作。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.9.5 外包软件开发

测评单元（L3-CMS1-25）

该测评单元包括以下要求：

a) 测评指标：应在软件交付前检测其中可能存在的恶意代码。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有交付前的恶意代码检测报告。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-26）

该测评单元包括以下要求：

a) 测评指标：应保证开发单位提供软件设计文档和使用指南。
b) 测评对象：记录表单类文档。

c) 测评实施：应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-27）

该测评单元包括以下要求：
a) 测评指标：应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈建设负责人委托开发单位是否提供软件源代码。
   2) 应核查软件测试报告是否审查了软件可能存在的后门和隐蔽信道。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CMS1-28）

该测评单元包括以下要求：
a) 测评指标：**应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F3）**
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈建设负责人是否要求外包服务商保留操作痕迹、记录完整的日志。
   2) 应核查相关内容和保存期限是否满足事件分析、安全取证、独立审计和监督检查需要。
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。

测评单元（L3-CMS1-29）

该测评单元包括以下要求：
a) 测评指标：**应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F3）**
b) 测评对象：外包合同商务类文档。
c) 测评实施：应核查外包合同等商务文件是否具有控制外包服务商分包的条款。
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。

测评单元（L3-CMS1-30）

该测评单元包括以下要求：
a) 测评指标：**应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。（F3）**
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈建设负责人是否要求外包服务商聘请外部机构定期对其进行安全审计，并核查是否具有外包服务商提交的安全审计报告。
   2) 应核查外包服务商是否及时整改安全审计发现的问题。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.9.6 工程实施

测评单元（L3-CMS1-31）

该测评单元包括以下要求：

a) 测评指标：应指定或授权专门的部门或人员负责工程实施过程的管理。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否指定专门部门或人员对工程实施进行进度和质量控制。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-32）

该测评单元包括以下要求：
a) 测评指标：应制定安全工程实施方案控制工程实施过程。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查安全工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-33）

该测评单元包括以下要求：
a) 测评指标：应通过第三方工程监理控制项目的实施过程。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查工程监理报告是否明确了工程进展、时间计划、控制措施等方面内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-34）

该测评单元包括以下要求：
a) 测评指标：**应制定灾难备份系统集成与测试计划并组织实施，通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。（F3）**
b) 测评对象：灾难备份系统和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否制定灾难备份系统集成与测试计划并组织实施。
   2) 应核查灾难备份系统技术和业务测试记录，灾难备份系统的功能与性能是否达到设计指标要求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CMS1-35）

该测评单元包括以下要求：
a) 测评指标：**系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有系统建设、升级、扩充等工程的规划、论证和审核材料并妥善保存。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.9.7 测试验收

测评单元（L3-CMS1-36）

该测评单元包括以下要求：
a) 测评指标：**应根据设计方案或合同要求等**制订测试验收方案，并依据测试验收方案实施测试验收，**在测试验收过程中应详细记录测试验收结果，**形成测试验收报告。**（F3）**

b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容。
   2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CMS1-37）

该测评单元包括以下要求：
a) 测评指标：应**由项目承担单位（部门）或公正的第三方制订安全测试方案，**进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容，**并将测试报告报科技部门审查。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有上线前的安全测试方案和安全测试报告，安全测试报告是否包含密码应用安全性测试相关内容。
   2) 应核查安全测试报告是否报科技部门审查。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CMS1-38）

该测评单元包括以下要求：
a) 测评指标：**新建应用系统投入生产运行前，原则上应进行不少于1个月的模拟运行和不少于3个月的试运行。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查应用系统投入生产运行前是否进行不少于1个月的模拟运行和不少于3个月的试运行。
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。

测评单元（L3-CMS1-39）

该测评单元包括以下要求：
a) 测评指标：**对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方案、数据备份与系统恢复措施、应急处置措施后，经系统用户和主管领导审批同意后，才能开展测试工作，以确保生产系统的安全。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 针对在生产系统上进行测试的情况，应核查是否事先进行了风险分析和告知。
   2) 针对在生产系统上进行测试的情况，应核查是否具有详细的系统测试方案、数据备份与系统恢复措施、应急处置措施。
   3) 针对在生产系统上进行测试的情况，应核查是否具有系统用户和主管领导的审批记录。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.9.8 系统交付

测评单元（L3-CMS1-40）

该测评单元包括以下要求：
a) 测评指标：应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

b) 测评对象：记录表单类文档。
c) 测评实施：应核查交付清单是否说明交付的各类设备、软件、文档等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-41）

该测评单元包括以下要求：
a) 测评指标：应对负责运行维护的技术人员进行相应的技能培训。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查系统交付技术培训记录是否包括培训内容、培训时间和参与人员等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-42）

该测评单元包括以下要求：
a) 测评指标：应提供建设过程文档和运行维护文档。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否提供建设过程文档和运行维护文档。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS1-43）

该测评单元包括以下要求：
a) 测评指标：**外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将采用的关键安全技术措施和核心安全功能设计对外公开。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查金融机构与外部建设单位之间是否签署知识产权保护协议和保密协议，并核查协议中是否具有禁止将系统关键安全技术措施和核心安全功能对外公开的相关条款。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.9.9 等级测评

测评单元（L3-CMS1-44）

该测评单元包括以下要求：
a) 测评指标：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人本次测评是否为首次，若非首次，是否根据以往测评结果进行相应的安全整改。
   2) 应核查是否具有以往等级测评报告和安全整改方案。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-CMS1-45）

该测评单元包括以下要求：
a) 测评指标：应在发生重大变更或级别发生变化时进行等级测评。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否有过重大变更或级别发生过变化及是否进行相应的等级测评。

2） 应核查是否具有相应情况下的等级测评报告。

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

测评单元（L3-CMS1-46）

该测评单元包括以下要求：

a） 测评指标：**应选择公安部认可的全国等级保护测评机构推荐目录中的测评单位进行等级测评，并与测评单位签订安全保密协议。（F3）**

b） 测评对象：等级测评报告和相关资质文件。

c） 测评实施包括以下内容：

1） 应核查以往等级测评的测评单位是否具有等级测评机构资质。

2） 应核查是否具有与测评单位签订的安全保密协议。

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

7.1.9.10 服务供应商管理

测评单元（L3-CMS1-47）

该测评单元包括以下要求：

a） 测评指标：**应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。（F3）**

b） 测评对象：建设负责人。

c） 测评实施：应访谈建设负责人是否评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。

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。

测评单元（L3-CMS1-48）

该测评单元包括以下要求：

a） 测评指标：应确保服务供应商的选择符合国家的有关规定。

b） 测评对象：建设负责人。

c） 测评实施：应访谈建设负责人选择的安全服务商是否符合国家有关规定。

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

测评单元（L3-CMS1-49）

该测评单元包括以下要求：

a） 测评指标：应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

b） 测评对象：记录表单类文档。

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

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

测评单元（L3-CMS1-50）

该测评单元包括以下要求：

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

b） 测评对象：管理制度类文档和记录表单类文档。

c） 测评实施包括以下内容：

1） 应核查是否具有服务供应商定期提交的安全服务报告。

2) 应核查是否定期审核评价服务供应商所提供的服务及服务内容变更情况，是否具有服务审核报告。
3) 应核查是否具有服务供应商评价审核管理制度，明确针对服务供应商的评价指标、考核内容等。

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

7.1.10 安全运维管理

7.1.10.1 环境管理

测评单元（L3-MMS1-01）

该测评单元包括以下要求：

a) 测评指标：应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理，**填写机房值班记录、巡视记录。（F3）**
b) 测评对象：物理安全负责人和记录表单类文档。
c) 测评实施包括以下内容：
1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理，对基础设施（如空调、供配电设备、灭火设备等）进行定期维护。
2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员。
3) 应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息。
4) 应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
5) 应核查是否具有机房值班记录、巡视记录。
d) 单元判定：如果1）～5）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。

测评单元（L3-MMS1-02）

该测评单元包括以下要求：

a) 测评指标：应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
1) 应核查机房安全管理制度是否覆盖物理访问、物品进出和环境安全等方面内容。
2) 应核查物理访问、物品进出和环境安全等相关记录是否与制度相符。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-03）

该测评单元包括以下要求：

a) 测评指标：**机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F3）**
b) 测评对象：机房。
c) 测评实施：应核查机房布线是否做到跳线整齐，跳线与配线架是否统一编号，标记是否清晰。
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。

测评单元（L3-MMS1-04）

该测评单元包括以下要求：

a) 测评指标：**机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F3）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：

1） 应核查人员管理或培训相关制度是否要求机房管理员经过相关培训后才能上岗。
2） 应核查是否具有机房管理员培训记录。

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

测评单元（L3-MMS1-05）

该测评单元包括以下要求：

a） 测评指标：**应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F3）**
b） 测评对象：记录表单类文档。
c） 测评实施：应核查机房设施维修保养记录是否记录机房设施定期维护保养的情况。
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。

测评单元（L3-MMS1-06）

该测评单元包括以下要求：

a） 测评指标：**进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F3）**
b） 测评对象：管理制度类文档和记录表单类文档。
c） 测评实施包括以下内容：
1） 应核查机房管理制度是否要求进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。
2） 应核查是否具有进出机房人员审批记录。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-07）

该测评单元包括以下要求：

a） 测评指标：**应设置弱电井，并留有足够的可扩展空间。（F3）**
b） 测评对象：机房。
c） 测评实施包括以下内容：
1） 应核查机房是否设置弱电井。
2） 应核查弱电井是否留有足够的可扩展空间。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-08）

该测评单元包括以下要求：

a） 测评指标：**机房所在区域应安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于3个月，销毁录像等资料应经单位主管领导批准后实施。（F3）**
b） 测评对象：机房和记录表单类文档。
c） 测评实施包括以下内容：
1） 应核查机房所在区域是否安装24小时视频监控录像装置。
2） 应核查重要机房区域是否实行24小时警卫值班，是否设置一个主出入口和一个或多个备用出入口。
3） 应核查出入口控制、入侵报警和电视监控设备运行资料是否妥善保管，保存期限是否不少于3个月。
4） 应核查销毁录像等资料时是否有单位主管领导审批记录。

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。

测评单元（L3-MMS1-09）

该测评单元包括以下要求：

a) 测评指标：应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
b) 测评对象：安全管理员和办公环境。
c) 测评实施包括以下内容：
   1) 应访谈安全管理员是否有相关规定明确接待来访人员区域。
   2) 应核查办公桌面上等位置是否未随意放置含有敏感信息的纸档文件和移动介质等。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.2 资产管理

测评单元（L3-MMS1-10）

该测评单元包括以下要求：

a) 测评指标：应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-11）

该测评单元包括以下要求：

a) 测评指标：应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。
b) 测评对象：资产管理员、管理制度类文档和设备。
c) 测评实施包括以下内容：
   1) 应访谈资产管理员是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施的选取上是否不同。
   2) 应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求。
   3) 应核查资产清单中的设备是否具有相应标识，标识方法是否符合 2）相关要求。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-12）

该测评单元包括以下要求：

a) 测评指标：应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：
   1) 应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）。
   2) 应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等要求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.3 介质管理

测评单元（L3-MMS1-13）

该测评单元包括以下要求：

a) 测评指标：应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。
b) 测评对象：资产管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理。
   2) 应核查介质管理记录是否记录介质归档和使用等情况。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-14）

该测评单元包括以下要求：

a) 测评指标：应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，**应选择安全可靠的传递、交接方式，做好防信息泄漏控制措施，**并对介质的归档和查询等进行登记记录。**（F3）**
b) 测评对象：资产管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈资产管理员介质在物理传输过程中的人员选择、打包、交付等情况是否进行控制。
   2) 应核查是否对介质的归档和查询等进行登记记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-15）

该测评单元包括以下要求：

a) 测评指标：**所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F3）**
b) 测评对象：资产管理员。
c) 测评实施：应访谈资产管理员并核查存放数据备份介质的环境是否防磁、防潮、防尘、防高温、防挤压。
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。

测评单元（L3-MMS1-16）

该测评单元包括以下要求：

a) 测评指标：**对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F3）**
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) 应核查纸质文档是否实行借阅登记制度，是否未经相关部门领导批准，任何人不得将文档转借、复制或对外公开。
   2) 应核查电子文档是否采用电子化办公审批平台进行管理。
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。

测评单元（L3-MMS1-17）

该测评单元包括以下要求：

a) 测评指标：**对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F3）**
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） 应核查载有敏感信息存储介质的销毁制度，是否对介质的销毁严格管理。
2） 应核查是否具有销毁介质的备案、销毁记录等。
3） 应核查对于存储介质未在金融机构内部使用的情况，是否对存储介质进行信息的不可恢复性销毁。

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。

测评单元（L3-MMS1-18）

该测评单元包括以下要求：

a） 测评指标：**应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F3）**
b） 测评对象：管理制度类文档和记录表单类文档。
c） 测评实施包括以下内容：
1） 应核查是否具有移动存储介质使用规范。
2） 应核查是否具有移动存储介质的使用记录等。
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。

测评单元（L3-MMS1-19）

该测评单元包括以下要求：

a） 测评指标：**应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安全区域。（F3）**
b） 测评对象：记录表单类文档。
c） 测评实施包括以下内容：
1） 应核查重要数据是否多重备份。
2） 应核查是否至少1份备份介质存放于科技部门指定的同城或异地安全区域。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-20）

该测评单元包括以下要求：

a） 测评指标：**应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。（F3）**
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） 应核查技术文档管理制度是否规定了对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理。
2） 应核查技术文档处理记录是否与管理制度要求一致。
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。

测评单元（L3-MMS1-21）

该测评单元包括以下要求：

a） 测评指标：**应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F3）**
b） 测评对象：记录表单类文档。
c） 测评实施包括以下内容：
1） 应核查是否具有定期对主要备份业务数据进行恢复验证的记录。
2） 应核查是否根据介质使用期限及时转储数据。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.4 设备维护管理

测评单元（L3-MMS1-22）

该测评单元包括以下要求：

a) 测评指标：应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。
b) 测评对象：设备管理员和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护。
   2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-23）

该测评单元包括以下要求：

a) 测评指标：应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容。
   2) 应核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-24）

该测评单元包括以下要求：

a) 测评指标：**设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前应请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。（F3）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查设备维护管理制度是否要求设备送外单位维修应彻底清除所存的工作相关信息并拆除与密码有关的硬件。
   2) 应核查是否与设备维修厂商签订保密协议。
   3) 应核查密码设备配套使用的设备送修前是否请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。
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。

测评单元（L3-MMS1-25）

该测评单元包括以下要求：

a) 测评指标：**应制定规范化的故障处理流程，建立详细的故障日志（包括故障发生的时间、范围、现象、处理结果和处理人员等内容）。（F3）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查设备故障处理制度是否包含规范化的故障处理流程。
   2) 应核查故障日志是否包括故障发生的时间、范围、现象、处理结果和处理人员等内容。

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

测评单元（L3-MMS1-26）

该测评单元包括以下要求：

a) 测评指标：**新购置的设备应经过验收，验收合格后方能投入使用。（F3）**

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查设备维护管理制度是否明确新购置的设备应经过验收，验收合格后方能投入使用。

2) 应核查新购置设备的验收报告和使用记录。

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

测评单元（L3-MMS1-27）

该测评单元包括以下要求：

a) 测评指标：**应制定设备管理规范，根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护责任。（F3）**

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查设备管理制度是否落实设备使用者的安全保护责任。

2) 应核查是否根据设备使用年限，及时进行更换升级，并核查是否具有相关记录。

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

测评单元（L3-MMS1-28）

该测评单元包括以下要求：

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

b) 测评对象：设备管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈设备管理员含有重要数据的设备带出工作环境是否有加密措施。

2) 应访谈设备管理员对带离机房的设备是否经过审批。

3) 应核查是否具有设备带离机房或办公地点的审批记录。

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

测评单元（L3-MMS1-29）

该测评单元包括以下要求：

a) 测评指标：**需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复性销毁处理，同时备案；信息消除处理仅限于废止设备仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F3）**

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查设备维护管理制度是否要求废止的设备应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等。

2) 应核查是否具有废止设备销毁记录。

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

7.1.10.5 漏洞和风险管理

测评单元（L3-MMS1-30）

该测评单元包括以下要求：

a) 测评指标：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否有识别安全漏洞和隐患的安全报告或记录（如漏洞扫描报告、渗透测试报告和安全通报等）。
   2) 应核查相关记录是否对发现的漏洞及时进行修补或评估可能的影响后进行修补。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-31）

该测评单元包括以下要求：

a) 测评指标：应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
b) 测评对象：安全管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈安全管理员是否定期开展安全测评。
   2) 应核查是否具有安全测评报告。
   3) 应核查是否具有安全整改应对措施文档。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.6 网络和系统安全管理

测评单元（L3-MMS1-32）

该测评单元包括以下要求：

a) 测评指标：应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查网络和系统安全管理文档，是否划分了网络和系统管理员等不同角色，并定义各个角色的责任和权限。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-33）

该测评单元包括以下要求：

a) 测评指标：应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理。
   2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-34）

该测评单元包括以下要求：

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

b) 测评对象：管理制度类文档。
c) 测评实施：应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略、账户管理（用户 责任、义务、风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与打补丁、审计日志管理、登录设备和系统的口令更新周期等方面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-35）

该测评单元包括以下要求：
a) 测评指标：应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
b) 测评对象：操作规程类文档。
c) 测评实施：应核查重要设备或系统（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、参数配置等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-36）

该测评单元包括以下要求：
a) 测评指标：应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容，**重要运维操作要求至少两人在场，保留记录，并由操作和复核人员进行确认，维护记录和确认记录应至少妥善保存 6 个月。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。
   2) 应核查重要运维操作是否要求至少两人在场，保留记录。
   3) 应核查重要运维操作的记录是否具有操作和复核人员的确认信息。
   4) 应核查维护记录是否至少保存 6 个月。
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。

测评单元（L3-MMS1-37）

该测评单元包括以下要求：
a) 测评指标：**应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，经过审批后才可开通，操作过程中应保留不可篡改的审计日志，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。（F3）**
b) 测评对象：系统管理员、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) 应访谈系统管理员是否制定远程访问控制规范。
   2) 应核查远程访问控制规范是否明确要求严禁跨境远程连接，严格控制国内远程访问范围。
   3) 确因工作需要进行远程访问的，应核查是否具有审批记录。
   4) 应核查远程访问操作过程中是否保留不可篡改的审计日志。
   5) 应核查是否针对远程访问采取了单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。
d) 单元判定：如果 1）～5）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。

测评单元（L3-MMS1-38）

该测评单元包括以下要求：

a) 测评指标：**各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F3）**
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) 应核查网络安全管理制度是否明确规定未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。
   2) 应核查多媒体使用批准记录是否与管理制度要求一致。
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。

测评单元（L3-MMS1-39）

该测评单元包括以下要求：
a) 测评指标：**网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不应对外公开，未经科技主管部门授权，任何外部机构与人员不应检测或扫描机构内部网络。（F3）**
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) 应核查网络安全管理制度是否明确规定网络安全管理人员经本部门主管领导批准后，才能对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息未经授权不得对外公开。
   2) 应核查安全检测、扫描等批准记录是否与管理制度要求一致。
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。

测评单元（L3-MMS1-40）

该测评单元包括以下要求：
a) 测评指标：**金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F3）**
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统管理员网间互联安全是否实行统一规范、分级管理、各负其责的安全管理模式。
   2) 应核查与外部机构实施网间互联时是否具有审批记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-41）

该测评单元包括以下要求：
a) 测评指标：**所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。（F3）**
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施：应访谈系统管理员是否定期对所有网间互联应用系统和外联网络区进行威胁评估和脆弱性评估，并核查是否具有威胁和脆弱性评估报告。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-42）

该测评单元包括以下要求：

a) 测评指标：**系统管理员不应兼任业务操作人员，系统管理员不应对业务数据进行任何增加、删除、修改等操作，系统管理员确需对系统数据库进行业务数据维护操作的，应征得业务部门审批，并详细记录维护内容、人员、时间等信息。（F3）**
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) 应核查系统管理员是否未兼任业务操作人员。
   2) 应核查网络安全管理制度是否明确规定系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对系统数据库进行技术维护性操作的，应征得业务部门审批，并详细记录维护过程。
   3) 应核查业务数据维护操作的审批记录是否与管理制度要求一致。
   4) 应核查业务数据维护操作记录是否包含维护内容、人员、时间等信息。
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。

测评单元（L3-MMS1-43）

该测评单元包括以下要求：
a) 测评指标：**每半年应至少进行一次漏洞扫描，对发现的安全漏洞及时进行修补，扫描结果应及时上报。（F3）**
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) 应核查网络安全管理规定是否明确要求每半年至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果及时上报。
   2) 应核查系统漏洞扫描、修补记录是否与管理制度要求一致。
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。

测评单元（L3-MMS1-44）

该测评单元包括以下要求：
a) 测评指标：应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈网络和系统相关人员是否指定专门部门或人员对日志、监测和报警数据等进行分析统计。
   2) 应核查是否具有对日志、监测和报警数据等进行分析统计的报告。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-45）

该测评单元包括以下要求：
a) 测评指标：应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈网络和系统相关人员调整配置参数结束后是否同步更新配置信息库，并核实配置信息库是否为最新版本。
   2) 应核查是否具有变更运维的审批记录，如系统连接、安装系统组件或调整配置参数等活动。
   3) 应核查是否具有变更运维的操作过程记录。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-46）

该测评单元包括以下要求：

a) 测评指标：应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统管理员使用运维工具结束后是否删除工具中的敏感数据。
   2) 应核查是否具有运维工具接入系统的审批记录。
   3) 应核查运维工具的审计日志记录，审计日志是否不可以更改。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-47）

该测评单元包括以下要求：

a) 测评指标：应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统相关人员日常运维过程中是否存在远程运维，若存在，远程运维结束后是否立即关闭了接口或通道。
   2) 应核查是否具有开通远程运维的审批记录。
   3) 应核查针对远程运维的审计日志是否不可以更改。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-48）

该测评单元包括以下要求：

a) 测评指标：应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
b) 测评对象：安全管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统相关人员网络外联连接（如互联网、合作伙伴企业网、上级部门网络等）是否都得到授权与批准。
   2) 应访谈网络管理员是否定期核查违规联网行为。
   3) 应核查是否具有外联授权的记录文件。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.7 恶意代码防范管理

测评单元（L3-MMS1-49）

该测评单元包括以下要求：

a) 测评指标：应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。
b) 测评对象：运维负责人和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识。
   2) 应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系统前进行恶意代码检查。

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

测评单元（L3-MMS1-50）

该测评单元包括以下要求：

a) 测评指标：应定期验证防范恶意代码攻击的技术措施的有效性。
b) 测评对象：安全管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 若采用可信验证技术，应访谈安全管理员是否未发生过恶意代码攻击事件。
   2) 若采用防恶意代码产品，应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否未出现过大规模的病毒事件。
   3) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。
d) 单元判定：如果 1）或 2）和 3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-51）

该测评单元包括以下要求：

a) 测评指标：**客户端应统一安装病毒防治软件，设置用户口令和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。（F3）**
b) 测评对象：安全管理员和客户端。
c) 测评实施包括以下内容：
   1) 应访谈安全管理员客户端是否统一安装了病毒防治软件，设置了用户口令和屏幕保护口令等安全防护措施，及时更新病毒特征码，以及安装了必要的补丁程序等。
   2) 应核查客户端病毒防治软件安装、用户口令设置、屏幕保护口令设置、病毒特征码更新以及补丁程序安装情况等是否与访谈结果一致。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.8 配置管理

测评单元（L3-MMS1-52）

该测评单元包括以下要求：

a) 测评指标：应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
b) 测评对象：系统管理员。
c) 测评实施：应访谈系统管理员是否对基本配置信息进行记录和保存。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-53）

该测评单元包括以下要求：

a) 测评指标：应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库。
   2) 应核查配置信息的变更流程是否具有相应的申报审批程序。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.9 密码管理

测评单元（L3-MMS1-54）

该测评单元包括以下要求：

a) 测评指标：应遵循密码相关的国家标准和行业标准。
b) 测评对象：安全管理员。
c) 测评实施：应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-55）

该测评单元包括以下要求：

a) 测评指标：应使用国家密码管理主管部门认证核准的密码技术和产品。
b) 测评对象：安全管理员。
c) 测评实施：应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。
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。

测评单元（L3-MMS1-56）

该测评单元包括以下要求：

a) 测评指标：**应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。（F3）**
b) 测评对象：管理制度类文档和密钥管理人员。
c) 测评实施包括以下内容：
   1) 应核查密钥管理制度是否明确了密钥的产生、分发和接收、使用、存储、更新、销毁等方面的管理要求。
   2) 应核查密钥管理人员是否为本机构在编的正式员工。
   3) 应核查密钥管理人员是否逐级进行备案。
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。

测评单元（L3-MMS1-57）

该测评单元包括以下要求：

a) 测评指标：**系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，并每半年更换，口令密码的强度应满足不同安全性要求。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查密码管理制度是否要求系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，并每半年更换，口令密码的强度满足不同安全性要求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-58）

该测评单元包括以下要求：

a) 测评指标：**系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。（F3）**
b) 测评对象：管理制度类文档。

c) 测评实施：应核查密码管理制度是否要求系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。
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。

测评单元（L3-MMS1-59）

该测评单元包括以下要求：
a) 测评指标：**密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责，密钥资料须保存在保险柜内，保险柜钥匙由专人负责，使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。（F3）**
b) 测评对象：安全管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈安全管理员，密钥注入、密钥管理功能调试和密钥档案的保管是否由专人负责。
   2) 应访谈安全管理员，密钥资料是否保存在保险柜内，保险柜钥匙是否由专人负责。
   3) 应访谈安全管理员，使用密钥和销毁密钥是否在监督下进行。
   4) 应核查是否具有密钥使用和销毁记录。
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。

测评单元（L3-MMS1-60）

该测评单元包括以下要求：
a) 测评指标：**确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查密码管理制度是否要求远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。
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。

测评单元（L3-MMS1-61）

该测评单元包括以下要求：
a) 测评指标：**应支持各类环境中密码设备使用、管理权限分离。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查密码管理制度是否要求各类环境中密码设备使用、管理权限分离。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.10.10 变更管理

测评单元（L3-MMS1-62）

该测评单元包括以下要求：
a) 测评指标：**变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：
   1) 应核查变更管理制度是否明确了变更流程、审批流程。
   2) 应核查变更管理制度是否明确变更发起方、实施方的职责。
   3) 应核查变更管理制度是否明确了变更方案的测试、审批流程及实施策略。

4) 应核查变更管理制度是否明确要求对有可能影响客户利益的变更应事先通知客户并得到客户的确认。

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。

测评单元（L3-MMS1-63）

该测评单元包括以下要求：

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。

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查变更方案是否包含变更类型、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。

测评单元（L3-MMS1-64）

该测评单元包括以下要求

a) 测评指标：应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查变更控制的申报、审批程序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) 应核查是否具有变更实施过程的记录文档。

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

测评单元（L3-MMS1-65）

该测评单元包括以下要求：

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。

b) 测评对象：运维负责人和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈确认运维负责人的职责以及变更中止或失败后的恢复程序、工作方法是否文档化，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) 应核查变更恢复程序是否规定变更中止或失败后的操作流程。

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。

测评单元（L3-MMS1-66）

该测评单元包括以下要求：

a) 测评指标：**变更前应做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪。（F3）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查变更方案是否要求变更前做好系统和数据的备份。

2) 应核查是否具有数据备份记录和跟踪记录文档。

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

测评单元（L3-MMS1-67）

该测评单元包括以下要求：

a) 测评指标：**如果需要对生产环境进行重大变更，应按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同意后，再进行变更操作，以确保生产系统的安全。（F3）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查对于生产环境重大变更是否制订了详细的系统变更方案、系统及数据备份恢复措施和应急处置方案。

2) 应核查对于生产环境重大变更是否在测试环境进行稳妥测试并通过。

3) 应核查对于生产环境重大变更是否具有系统用户和主管领导审批记录。

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

测评单元（L3-MMS1-68）

该测评单元包括以下要求：

a) 测评指标：**当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性，应尽量减少紧急变更。（F3）**

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) 应核查变更管理制度是否要求当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更。

2) 应核查变更管理制度是否要求尽量减少紧急变更。

3) 应核查变更记录与变更管理制度要求是否一致。

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

7.1.10.11 备份与恢复管理

测评单元（L3-MMS1-69）

该测评单元包括以下要求：

a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等。

b) 测评对象：系统管理员和管理制度类文档。

c) 测评实施包括以下内容：

1) 应访谈系统管理员有哪些需定期备份的业务信息、系统数据及软件系统。

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

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

测评单元（L3-MMS1-70）

该测评单元包括以下要求：

a) 测评指标：应规定备份信息的备份方式、备份频度、存储介质、保存期等。

b) 测评对象：管理制度类文档。

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

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

测评单元（L3-MMS1-71）

该测评单元包括以下要求：

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。
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文档是否根据数据的重要程度制定相应备份恢复策略和程序等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-72）

该测评单元包括以下要求：

a) 测评指标：**应每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。（F3）**
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) 应核查灾备切换演练制度中是否要求每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据人员、信息资源等变动情况以及演练情况更新和完善应急预案。
   2) 应核查是否具有灾难切换演练记录、应急预案更新和完善记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-73）

该测评单元包括以下要求：

a) 测评指标：**应每季度对备份数据的有效性进行检查，备份数据要实行异地保存。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否每季度对备份数据的有效性进行检查，备份数据是否实行异地保存。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-74）

该测评单元包括以下要求：

a) 测评指标：**恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：恢复及使用备份数据时需要提供相关口令密码的，应核查是否将口令密码密封后与数据备份介质一并妥善保管。
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。

测评单元（L3-MMS1-75）

该测评单元包括以下要求：

a) 测评指标：**灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：

1) 应核查灾难恢复相关管理制度是否要求灾难恢复的需求需定期进行再分析且再分析周期最长为三年。
2) 应核查当生产中心环境、生产系统或业务流程发生重大变更时，是否立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。

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

测评单元（L3-MMS1-76）

该测评单元包括以下要求：

a) 测评指标：**应建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：
   1) 应核查是否建立了灾难恢复计划。
   2) 应核查灾难恢复计划是否包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册。
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。

测评单元（L3-MMS1-77）

该测评单元包括以下要求：

a) 测评指标：**金融机构应根据信息系统的灾难恢复工作情况，确定审计频率，应每年至少组织一次内部灾难恢复工作审计。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否每年至少组织一次内部灾难恢复工作审计。
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。

测评单元（L3-MMS1-78）

该测评单元包括以下要求：

a) 测评指标：**应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。（F3）**
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) 应核查灾难恢复管理制度是否要求定期开展灾难恢复培训和灾难恢复演练。
   2) 应核查是否具有灾难恢复培训和演练记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-79）

该测评单元包括以下要求：

a) 测评指标：**应建立灾难备份系统，主备系统实际切换时间应少于RTO时间，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F3）**
b) 测评对象：灾难备份系统。
c) 测评实施包括以下内容：
   1) 应核查是否建立灾难备份系统。
   2) 应核查灾难备份系统的主备系统实际切换时间是否少于RTO时间。
   3) 应核查灾备系统处理能力是否不低于主用系统处理能力的50%。
   4) 应核查通信线路是否分别接入主备系统。

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

7.1.10.12 安全事件处置

测评单元（L3-MMS1-80）

该测评单元包括以下要求：

a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件。
b) 测评对象：运维负责人和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告。
   2) 应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-81）

该测评单元包括以下要求：

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。
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是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和响应流程等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-82）

该测评单元包括以下要求：

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。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过程、经验教训、补救措施等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-83）

该测评单元包括以下要求:

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。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否有不同安全事件的报告流程。
   2) 应核查针对重大安全事件是否制定不同的安全事件报告和处理流程，是否明确具体报告方式、报告内容、报告人等方面内容。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.13 应急预案管理

测评单元（L3-MMS1-84）

该测评单元包括以下要求：

a) 测评指标：应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容，**业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字确认。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：
   1) 应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面。
   2) 应核查业务处理系统应急预案的编制工作是否由相关业务部门和科技部门共同完成。
   3) 应核查业务处理系统应急预案是否由预案涉及的相关机构进行签字确认。
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。

测评单元（L3-MMS1-85）

该测评单元包括以下要求：
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。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否制定了重要事件的应急预案（如针对机房、系统、网络等各个方面）。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-86）

该测评单元包括以下要求：
a) 测评指标：应**每年**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。**（F3）**
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否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是否记录演练时间、主要操作内容、演练结果等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-87）

该测评单元包括以下要求：
a) 测评指标：**在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。（F3）**
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人在与第三方合作的业务中是否建立并完善了内部责任机制以及与相关机构之间的协调机制。
   2) 应核查是否具有完整的应急预案及应急协调预案。
   3) 应核查是否具有联合演练记录。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-88）

该测评单元包括以下要求：
a) 测评指标：**突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F3）**
b) 测评对象：运维负责人和记录表单类文档。

c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否由突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源。
   2) 应核查是否具有应急处置联络人名单并上报至本行业网络安全监管部门。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS1-89）

该测评单元包括以下要求：
a) 测评指标：**突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F3）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查突发事件管理相关制度是否明确要求突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。
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。

测评单元（L3-MMS1-90）

该测评单元包括以下要求：
a) 测评指标：**实施报告制度和启动应急预案的单位应当实行重大突发事件24小时值班制度。（F3）**
b) 测评对象：运维负责人。
c) 测评实施：应访谈运维负责人是否具有重大突发事件24小时值班制度。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS1-91）

该测评单元包括以下要求：
a) 测评指标：应定期对原有的应急预案重新评估，修订完善。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否具有管理制度规定定期对原有的应急预案重新评估。
   2) 应核查应急预案重新评估记录是否与管理要求一致。
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。

测评单元（L3-MMS1-92）

该测评单元包括以下要求：
a) 测评指标：**应急演练结束后，应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有应急演练情况总结报告。
   2) 应核查应急演练情况总结报告内容是否包括：内容、目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划和演练结论。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.10.14 外包运维管理

测评单元（L3-MMS1-93）

该测评单元包括以下要求：

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。
b) 测评对象：运维负责人。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否有外包运维服务情况。
   2) 应访谈运维负责人外包运维服务单位是否符合国家有关规定。
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。

测评单元（L3-MMS1-94）

该测评单元包括以下要求：

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。
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是否明确约定外包运维的范围和工作内容。
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。

测评单元（L3-MMS1-95）

该测评单元包括以下要求：

a) 测评指标：应保证选择的外包运维服务商在技术和管理方面均应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。
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。
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。

测评单元（L3-MMS1-96）

该测评单元包括以下要求：

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。
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。

测评单元（L3-MMS1-97）

该测评单元包括以下要求：

a) 测评指标：**应要求外包运维服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有外包服务商的操作记录文档。
   2) 应核查操作记录文档的内容和保存期限是否满足事件分析、安全取证、独立审计和监督检查需要。
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。

测评单元（L3-MMS1-98）

该测评单元包括以下要求：

a) 测评指标：**应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F3）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有数据中心外包服务应急计划以应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.2 云计算安全测评扩展要求

7.2.1 安全物理环境

7.2.1.1 基础设施位置

测评单元（L3-PES2-01）

该测评单元包括以下要求：

a) 测评指标：应保证云计算基础设施位于中国境内。
b) 测评对象：机房管理员、办公场地、机房和平台建设方案。
c) 测评实施包括以下内容：
   1) 应访谈机房管理员，云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内。
   2) 应核查云计算平台建设方案，云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.2 安全通信网络

7.2.2.1 网络架构

测评单元（L3-CNS2-01）

该测评单元包括以下要求：

a) 测评指标：应保证云计算平台不承载高于其安全保护等级的业务应用系统。
b) 测评对象：云计算平台和业务应用系统定级备案材料。
c) 测评实施：应核查云计算平台和云计算平台承载的业务应用系统相关定级备案材料，云计算平台安全保护等级是否不低于其承载的业务应用系统安全保护等级。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CNS2-02）

该测评单元包括以下要求：

a) 测评指标：应实现不同云服务客户虚拟网络之间**及同一云服务客户不同虚拟网络之间**的隔离。**（F3）**
b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台。
c) 测评实施包括以下内容：
   1) 应核查云服务客户之间是否采取网络隔离措施。
   2) 应核查同一云服务客户不同虚拟网络之间是否采取网络隔离措施。
   3) 应核查云服务客户之间是否设置并启用网络资源隔离策略。
   4) 应核查同一云服务客户不同虚拟网络之间是否设置并启用网络资源隔离策略。
   5) 应测试验证不同云服务客户之间的网络隔离措施是否有效。
   6) 应测试验证同一云服务客户不同虚拟网络之间的网络隔离措施是否有效。

d) 单元判定：如果1）～6）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。

测评单元（L3-CNS2-03）

该测评单元包括以下要求：

a) 测评指标：**应实现云计算平台的业务网络与管理网络安全隔离。（F3）**

b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台。

c) 测评实施包括以下内容：

1) 应核查业务网络与管理网络之间是否存在隔离措施。

2) 应测试验证业务网络与管理网络之间的隔离措施是否有效。

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。

测评单元（L3-CNS2-04）

该测评单元包括以下要求：

a) 测评指标：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。

b) 测评对象：防火墙、入侵检测系统、入侵保护系统和抗APT攻击系统等安全设备。

c) 测评实施包括以下内容：

1) 应核查云计算平台是否具备为云服务客户提供通信传输、边界防护、入侵防范等安全防护机制的能力。

2) 应核查上述安全防护机制是否满足云服务客户的业务需求。

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

测评单元（L3-CNS2-05）

该测评单元包括以下要求：

a) 测评指标：应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略。

b) 测评对象：云管理平台、网络管理平台、网络设备和安全访问路径。

c) 测评实施包括以下内容：

1) 应核查云计算平台是否支持云服务客户自主定义安全策略，包括定义访问路径、选择安全组件、配置安全策略。

2) 应核查云服务客户是否能够自主设置安全策略，包括定义访问路径、选择安全组件、配置安全策略。

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

测评单元（L3-CNS2-06）

该测评单元包括以下要求：

a) 测评指标：应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

b) 测评对象：相关开放性接口和安全服务及相关文档。

c) 测评实施包括以下内容：

1) 应核查接口设计文档或开放性服务技术文档是否符合开放性及安全性要求。

2) 应核查云服务客户是否可以接入第三方安全产品或在云计算平台选择第三方安全服务。

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

7.2.3 安全区域边界

7.2.3.1 访问控制

测评单元（L3-ABS2-01）

该测评单元包括以下要求：

a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备。
c) 测评实施包括以下内容：
   1) 应核查是否在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
   2) 应核查并测试验证云计算平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效。
   3) 应核查并测试验证云计算平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效。
   4) 应核查并测试验证不同云服务客户间访问控制规则和访问控制策略是否有效。
   5) 应核查并测试验证云服务客户不同安全保护等级业务系统之间访问控制规则和访问控制策略是否有效。
d) 单元判定：如果1）～5）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。

测评单元（L3-ABS2-02）

该测评单元包括以下要求：

a) 测评指标：应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备。
c) 测评实施包括以下内容：
   1) 应核查是否在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
   2) 应核查不同安全等级网络区域边界的访问控制规则和访问控制策略是否有效。
   3) 应测试验证不同安全等级的网络区域间进行非法访问时，是否可以正确拒绝该非法访问。
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。

测评单元（L3-ABS2-03）

该测评单元包括以下要求：

a) 测评指标：**应实现虚拟机之间、虚拟机与资源管理和调度平台之间、虚拟机与外部网络之间的安全访问控制。（F3）**
b) 测评对象：云计算平台。
c) 测评实施：应核查云计算平台是否具备不同层面的访问控制能力，如在虚拟防火墙、虚拟路由器、虚拟交换机上配置访问控制策略，实现虚拟机之间、虚拟机与管理平台之间、虚拟机与外部网络之间访问控制。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-ABS2-04）

该测评单元包括以下要求：

a) 测评指标：**应对云计算平台管理员访问管理网络进行访问控制。（F3）**
b) 测评对象：云计算平台管理员访问控制策略。
c) 测评实施包括以下内容：
   1) 应核查是否支持云计算平台管理员访问网络的身份验证和权限控制。
   2) 应核查云计算平台对网络资源管理员的访问控制措施是否有效。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.3.2 入侵防范

测评单元（L3-ABS2-05）

该测评单元包括以下要求：

a) 测评指标：应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。

b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否采取了入侵防范措施对网络入侵行为进行防范，如部署抗 APT 攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件。

2) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件的规则库升级方式，核查规则库是否进行及时更新。

3) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能，以及报警功能和清洗处置功能。

4) 应验证抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证入侵防范设备或相关组件是否能记录攻击类型、攻击时间、攻击流量）。

5) 应验证抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件对云服务客户网络攻击行为的报警策略是否有效（如模拟产生攻击动作，验证抗 APT 攻击系统或网络入侵保护系统是否能实时报警）。

6) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具有对 SQL 注入、跨站脚本等攻击行为的发现和阻断能力。

7) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否能够检测出具有恶意行为、过分占用计算资源和带宽资源等恶意行为的虚拟机。

8) 应核查云管理平台对云服务客户攻击行为的防范措施，核查是否能够对云服务客户的网络攻击行为进行记录，记录应包括攻击类型、攻击时间和攻击流量等内容。

9) 应核查云管理平台或入侵防范设备是否能够对云计算平台内部发起的恶意攻击或恶意外连行为进行限制，核查是否能够对内部行为进行监控。

10) 通过对外攻击发生器伪造对外攻击行为，核查云服务客户的网络攻击日志，确认是否正确记录相应的攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP 和攻击流量规模等内容。

11) 应核查运行虚拟机监控器（VMM）、容器监控器和云管理平台软件的物理主机，确认其安全加固手段是否能够避免或减少虚拟化共享带来的安全漏洞。

d) 单元判定：如果1）～11）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。

测评单元（L3-ABS2-06）

该测评单元包括以下要求：

a) 测评指标：应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。

b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否部署网络攻击行为检测设备或相关组件对虚拟网络节点的网络攻击行为进行防范，并能记录攻击类型、攻击时间、攻击流量等。

2) 应核查网络攻击行为检测设备或相关组件的规则库是否为最新。

3) 应测试验证网络攻击行为检测设备或相关组件对异常流量和未知威胁的监控策略是否有效。

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。

测评单元（L3-ABS2-07）

该测评单元包括以下要求：

a) 测评指标：应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。

b) 测评对象：虚拟机、宿主机、抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量的检测功能。

2) 应测试验证对异常流量的监测策略是否有效。

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。

测评单元（L3-ABS2-08）

该测评单元包括以下要求：

a) 测评指标：应在检测到网络攻击行为、异常流量情况时进行告警。

b) 测评对象：虚拟机、宿主机、抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查检测到网络攻击行为、异常流量时是否进行告警。

2) 应测试验证其对异常流量的监测策略是否有效。

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。

测评单元（L3-ABS2-09）

该测评单元包括以下要求：

a) 测评指标：**应检测和防护云计算平台内部虚拟机发起的针对云计算平台的攻击，能够定位发起攻击的虚拟机，记录攻击类型、攻击时间、攻击流量等信息。（F3）**

b) 测评对象：安全服务、安全组件、监测信息。

c) 测评实施包括以下内容：

1) 应核查云计算平台是否对内部虚拟机发起的针对云计算平台的攻击进行识别、检测与防护。

2) 应核查云计算平台是否能够定位发起攻击的虚拟机，记录攻击类型、攻击时间、攻击流量。

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。

测评单元（L3-ABS2-10）

该测评单元包括以下要求：

a) 测评指标：**云服务客户通过互联网提供金融服务时，应支持DoS/DDoS攻击防护，通过清洗DoS/DDoS攻击流量，保障网络、服务器及上层应用的可用性。（F3）**

b) 测评对象：入侵保护系统、DoS/DDoS防护模块或相关组件。

c) 测评实施包括以下内容：

1) 应核查系统是否具备对 DoS/DDoS 攻击的防护措施。

2) 应核查历史记录或测试验证对 DoS/DDoS 攻击的防护措施是否有效（如模拟产生攻击动作，验证入侵保护系统和相关组件等）。

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。

测评单元（L3-ABS2-11）

该测评单元包括以下要求：

a) 测评指标：**云服务客户通过互联网提供金融服务时，应支持检测Web应用漏洞，拦截SQL注入、XSS攻击等多种Web应用攻击行为。（F3）**
b) 测评对象：入侵保护系统Web应用防火墙或相关组件。
c) 测评实施包括以下内容：
   1) 应核查相关系统或设备是否具备 Web 应用漏洞检测功能，包括拦截 SQL 注入、XSS 攻击相关功能。
   2) 应测试验证或核查历史记录判断相关系统或设备的检测措施是否有效。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.3.3 安全审计

测评单元（L3-ABS2-12）

该测评单元包括以下要求：

a) 测评指标：应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。
b) 测评对象：堡垒机或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云服务商（含第三方运维服务商）和云服务客户在远程管理时执行的远程特权命令是否有相关审计记录。
   2) 应测试验证云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ABS2-13）

该测评单元包括以下要求：

a) 测评指标：应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。
b) 测评对象：综合审计系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计。
   2) 应测试验证云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.4 安全计算环境

7.2.4.1 身份鉴别

测评单元（L3-CES2-01）

该测评单元包括以下要求：

a) 测评指标：当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。
b) 测评对象：管理终端和云计算平台。
c) 测评实施包括以下内容：
   1) 应核查当进行远程管理时是否建立双向身份验证机制。
   2) 应测试验证上述双向身份验证机制是否有效。
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。

测评单元（L3-CES2-02）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户密码策略管理，密码策略管理应支持密码复杂度策略、密码有效期策略，云服务客户账号的初始密码应支持随机生成，云服务客户首次登录支持强制修改初始密码。（F3）**

b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。

c) 测评实施包括以下内容：

1) 被测对象为云计算平台时，应核查云计算平台是否支持云服务客户密码策略管理功能，包括密码复杂度策略、密码有效期策略。

2) 被测对象为云计算平台时，应核查云计算平台是否支持云服务客户账号的初始密码随机生成，是否支持云服务客户首次登录强制修改初始密码。

3) 被测对象为云服务客户时，应核查云服务客户是否开启密码复杂度策略、密码有效期策略。

4) 被测对象为云服务客户时，应核查云服务客户是否开启账户的初始密码随机生成功能，是否开启首次登录强制修改初始密码策略。

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。

测评单元（L3-CES2-03）

该测评单元包括以下要求：

a) 测评指标：**应支持为云服务客户随机生成虚拟机登录口令或云服务客户自行设置登录口令。（F3）**

b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。

c) 测评实施包括以下内容：

1) 被测对象为云计算平台时，应核查云计算平台是否支持云服务客户随机生成虚拟机登录口令或自行设置登录口令。

2) 被测对象为云服务客户时，应核查云服务客户是否可随机生成虚拟机登录口令或自行设置登录口令。

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。

测评单元（L3-CES2-04）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户以密钥对方式登录虚拟机时，自主选择云计算平台生成密钥对或自行上传密钥对。（F3）**

b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。

c) 测评实施包括以下内容：

1) 应核查云计算平台是否支持云服务客户以密钥对方式登录虚拟机。

2) 应核查云服务客户是否可以自主选择云计算平台生成密钥对或自行上传密钥对。

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。

测评单元（L3-CES2-05）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。（F3）**

b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。

c) 测评实施包括以下内容：

1) 应测试验证云计算平台是否支持云服务客户自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。

2) 应测试验证云服务客户是否可以自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。

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

7.2.4.2 访问控制

测评单元（L3-CES2-06）

该测评单元包括以下要求：

a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移。
b) 测评对象：虚拟机、虚拟机迁移记录和相关配置。
c) 测评实施包括以下内容：
   1) 应核查虚拟机迁移时访问控制策略是否随之迁移。
   2) 应测试验证虚拟机迁移后访问控制措施是否随其迁移。
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。

测评单元（L3-CES2-07）

该测评单元包括以下要求：

a) 测评指标：应允许云服务客户设置不同虚拟机之间的访问控制策略。
b) 测评对象：虚拟机和安全组或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云服务客户是否能够设置不同虚拟机间访问控制策略。
   2) 应测试验证上述访问控制策略是否有效。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.4.3 入侵防范

测评单元（L3-CES2-08）

该测评单元包括以下要求：

a) 测评指标：应能检测虚拟机之间的资源隔离失效，并进行告警。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测到虚拟机之间的资源隔离失效并进行告警，如CPU、内存和磁盘资源之间的隔离失效。
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。

测评单元（L3-CES2-09）

该测评单元包括以下要求：

a) 测评指标：应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。
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。

测评单元（L3-CES2-10）

该测评单元包括以下要求：

a) 测评指标：应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。
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。

测评单元（L3-CES2-11）

该测评单元包括以下要求：

a) 测评指标：**应能够检测虚拟机对宿主机资源的异常访问，并进行告警。（F3）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测虚拟机对宿主机资源的异常访问，并进行告警。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.2.4.4 恶意代码防范

测评单元（L3-CES2-12）

该测评单元包括以下要求：

a) 测评指标：**应支持对后门、木马、蠕虫、webshell等恶意代码的静态检测和行为检测，并对检测出的恶意代码进行控制和隔离。（F3）**
b) 测评对象：云管理平台、云服务客户、防病毒网关和UTM等提供防恶意代码功能的系统或相关组件。
c) 测评实施包括以下内容：
   1) 测评对象是云计算平台时，应核查云计算平台是否部署了防恶意代码产品或采取了其他恶意代码防范措施，应核查防恶意代码产品运行是否正常，是否支持对后门、木马、蠕虫、webshell等恶意代码的静态检测和行为检测，应核查恶意代码库是否已经更新到最新，应检查是否支持对检测出的恶意代码进行控制和隔离。
   2) 测评对象是云服务客户时，应核查云服务客户是否开启了恶意代码防范服务或采取了其他恶意代码防范措施。
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。

测评单元（L3-CES2-13）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户自行安装防恶意代码软件，并支持更新防恶意代码软件版本和恶意代码库。（F3）**
b) 测评对象：云管理平台、云服务客户、防病毒网关和UTM等提供防恶意代码功能的系统或相关组件。
c) 测评实施包括以下内容：
   1) 测评对象是云计算平台时，应核查云计算平台是否支持云服务客户自行安装防恶意代码软件，是否支持更新防恶意代码软件版本和恶意代码库，应核查防恶意代码软件版本和恶意代码库是否为最新。
   2) 测评对象是云服务客户时，应核查云服务客户是否可自行安装防恶意代码软件，是否支持更新防恶意代码软件版本和恶意代码库，应核查防恶意代码软件版本和恶意代码库是否为最新。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.4.5 镜像和快照保护

测评单元（L3-CES2-14）

该测评单元包括以下要求：

a) 测评指标：应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
b) 测评对象：虚拟机镜像文件。
c) 测评实施：应核查是否对生成的虚拟机镜像采取必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。
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。

测评单元（L3-CES2-15）

该测评单元包括以下要求：

a) 测评指标：应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。
b) 测评对象：云管理平台和虚拟机镜像、快照或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。
   2) 应测试验证是否能够对镜像、快照进行完整性验证。
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。

测评单元（L3-CES2-16）

该测评单元包括以下要求：

a) 测评指标：应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。
b) 测评对象：云管理平台和虚拟机镜像、快照或相关组件。
c) 测评实施：应核查是否对虚拟机镜像或快照中的敏感资源采用加密、访问控制等技术手段进行保护，防止可能存在的针对快照的非法访问。
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。

测评单元（L3-CES2-17）

该测评单元包括以下要求：

a) 测评指标：**应保证虚拟机镜像和快照文件备份在不同物理服务器。（F3）**
b) 测评对象：云管理平台和虚拟机镜像、快照或相关组件。
c) 测评实施：应核查云平台虚拟机镜像或快照文件备份是否备份在不同的物理服务器。
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。

测评单元（L3-CES2-18）

该测评单元包括以下要求：

a) 测评指标：**应支持自动虚拟机快照功能，保证系统能根据快照恢复。（F3）**
b) 测评对象：云管理平台、云服务客户、虚拟机镜像、快照或相关组件。
c) 测评实施包括以下内容：
   1) 测评对象是云计算平台时，应核查云计算平台是否支持自动虚拟机快照功能，应检验快照是否可以恢复。
   2) 测评对象是云服务客户时，应检验快照是否可以恢复。
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，否则不符合本测评单元指标要求。

7.2.4.6 数据完整性和保密性

测评单元（L3-CES2-19）

该测评单元包括以下要求：

a) 测评指标：应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
b) 测评对象：数据库服务器、数据存储设备和管理文档记录。
c) 测评实施包括以下内容：
   1) 应核查云服务客户数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内。
   2) 应核查上述数据出境时是否符合国家相关规定。

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

测评单元（L3-CES2-20）

该测评单元包括以下要求：

a) 测评指标：应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限。
b) 测评对象：云管理平台、数据库、相关授权文档和管理文档。
c) 测评实施包括以下内容：
   1) 应核查云服务客户数据管理权限授权流程、授权方式、授权内容。
   2) 应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查是否有相关授权证明。
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。

测评单元（L3-CES2-21）

该测评单元包括以下要求：

a) 测评指标：应使用校验技术或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
b) 测评对象：虚拟机。
c) 测评实施：应核查在虚拟资源迁移过程中，是否采取校验技术或密码技术等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
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。

测评单元（L3-CES2-22）

该测评单元包括以下要求：

a) 测评指标：应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。
b) 测评对象：密钥管理解决方案。
c) 测评实施包括以下内容：
   1) 当云服务客户已部署密钥管理解决方案，应核查密钥管理解决方案是否能保证云服务客户自行实现数据的加解密过程。
   2) 应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能保证云服务客户自行实现数据的加解密过程。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.4.7 数据备份恢复

测评单元（L3-CES2-23）

该测评单元包括以下要求：

a) 测评指标：云服务客户应在本地保存其业务数据的备份。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否提供备份措施保证云服务客户可以在本地备份其业务数据。
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。

测评单元（L3-CES2-24）

该测评单元包括以下要求：

a) 测评指标：应提供查询云服务客户数据及备份存储位置的能力。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
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。

测评单元（L3-CES2-25）

该测评单元包括以下要求：
a) 测评指标：云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致。
b) 测评对象：云管理平台、云存储系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本。
   2) 应核查各副本内容是否保持一致。
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。

测评单元（L3-CES2-26）

该测评单元包括以下要求：
a) 测评指标：应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。
b) 测评对象：相关技术措施和手段。
c) 测评实施包括以下内容：
   1) 应核查是否有相关技术手段保证云服务客户能够将业务系统及数据迁移到其他云计算平台和本地系统。
   2) 应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。
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。

测评单元（L3-CES2-27）

该测评单元包括以下要求：
a) 测评指标：**应周期性测试云计算平台的备份系统和备份数据，支持故障识别和备份重建。（F3）**
b) 测评对象：云管理平台或相关组件、备份系统、备份数据、数据备份恢复相关的管理制度。
c) 测评实施包括以下内容：
   1) 应核查云服务商是否周期性测试云计算平台的备份系统和备份数据，支持故障识别和备份重建。
   2) 应核查云计算平台的备份系统和备份数据是否能够正常进行备份和恢复。
   3) 应核查是否具有数据备份系统和备份数据的测试记录。
   4) 应核查数据备份恢复相关的管理制度是否有相关的备份要求。
d) 单元判定：如果1）～4）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.4.8 剩余信息保护

测评单元（L3-CES2-28）

该测评单元包括以下要求：
a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
b) 测评对象：云计算平台。
c) 测评实施包括以下内容：

1） 应核查虚拟机的内存和存储空间回收时，是否得到完全清除。
2） 应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。

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。

测评单元（L3-CES2-29）

该测评单元包括以下要求：

a） 测评指标：云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除，**不能通过软件工具恢复。（F3）**
b） 测评对象：云存储和云计算平台。
c） 测评实施：应核查当云服务客户删除业务应用数据时，云存储中所有副本是否被删除，且不能通过软件工具恢复。
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。

测评单元（L3-CES2-30）

该测评单元包括以下要求：

a） 测评指标：**对于更换或报废的存储介质，应采取安全删除、强化消磁或者物理损坏磁盘等方式，防止恢复已清除数据。（F3）**
b） 测评对象：存储介质和存储介质相关的管理制度。
c） 测评实施包括以下内容：
1） 应核查存储介质相关的管理制度是否规定对于更换或报废的存储介质，应采取安全删除、强化消磁或者物理损坏磁盘等方式，防止恢复已清除数据。
2） 应核查对于更换或报废的存储介质，是否采取了安全删除、强化消磁或者物理损坏磁盘等方式防止恢复已清除数据。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.5 安全管理中心

7.2.5.1 集中管控

测评单元（L3-SMC2-01）

该测评单元包括以下要求：

a） 测评指标：应能对物理资源和虚拟资源按照策略做统一管理调度与分配。
b） 测评对象：资源调度平台、云管理平台或相关组件。
c） 测评实施包括以下内容：
1） 应核查是否有资源调度平台等提供资源统一管理调度与分配策略。
2） 应核查是否能够按照上述策略对物理资源和虚拟资源做统一管理调度与分配。
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。

测评单元（L3-SMC2-02）

该测评单元包括以下要求：

a） 测评指标：应保证云计算平台管理流量与云服务客户业务流量分离。
b） 测评对象：网络架构和云管理平台。
c） 测评实施包括以下内容：
1） 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离。
2） 应测试验证云计算平台管理流量与业务流量是否分离。

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。

测评单元（L3-SMC2-03）

该测评单元包括以下要求：

a) 测评指标：应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。
b) 测评对象：云管理平台、综合审计系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集。
   2) 应核查云服务商和云服务客户是否能够实现各自的集中审计。
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。

测评单元（L3-SMC2-04）

该测评单元包括以下要求：

a) 测评指标：应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等运行状况的集中监测，**监测内容包括CPU利用率、带宽使用情况、内存利用率、存储使用情况等。（F3）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等运行状况的集中监测。
   2) 应核查监控内容是否包括 CPU 利用率、带宽使用情况、内存利用率、存储使用情况等。
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。

测评单元（L3-SMC2-05）

该测评单元包括以下要求：

a) 测评指标：**应对异常行为集中监控分析并告警。集中监控服务质量，并可导出集中监控报告。应支持远程监控的可视化展示。（F3）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云服务商是否对异常行为进行集中监控分析并告警。
   2) 应核查是否可导出集中监控报告。
   3) 应核查是否支持远程监控的可视化展示。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.6 安全建设管理

7.2.6.1 云服务商选择

测评单元（L3-CMS2-01）

该测评单元包括以下要求：

a) 测评指标：应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
b) 测评对象：系统建设负责人和服务合同。
c) 测评实施包括以下内容：
   1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云计算平台及云服务商。

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

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

测评单元（L3-CMS2-02）

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标。
b) 测评对象：服务水平协议或服务合同。
c) 测评实施：应核查服务水平协议或服务合同是否规定了云服务的各项服务内容和具体指标等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS2-03）

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
b) 测评对象：服务水平协议或服务合同。
c) 测评实施：应核查服务水平协议或服务合同中是否规定了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS2-04）

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
b) 测评对象：服务水平协议或服务合同。
c) 测评实施：应核查服务水平协议或服务合同是否明确服务合约到期时，云服务商完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
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。

测评单元（L3-CMS2-05）

该测评单元包括以下要求：

a) 测评指标：应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。
b) 测评对象：保密协议或服务合同。
c) 测评实施：应核查保密协议或服务合同是否包含对云服务商不得泄露云服务客户数据的规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.2.6.2 供应链管理

测评单元（L3-CMS2-06）

该测评单元包括以下要求：

a) 测评指标：应确保供应商的选择符合国家有关规定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查云服务商的选择是否符合国家的有关规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS2-07）

该测评单元包括以下要求：

a) 测评指标：应将供应链安全事件信息或威胁信息及时传达到云服务客户。
b) 测评对象：供应链安全事件报告或威胁报告。
c) 测评实施：应核查供应链安全事件报告或威胁报告是否及时传达到云服务客户，报告是否明确相关事件信息或威胁信息。
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。

测评单元（L3-CMS2-08）

该测评单元包括以下要求：

a) 测评指标：应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。
b) 测评对象：供应商重要变更记录、安全风险评估报告和风险预案。
c) 测评实施：应核查供应商的重要变更是否及时传达到云服务客户，是否对每次供应商的重要变更都进行风险评估并采取控制措施。
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。

测评单元（L3-CMS2-09）

该测评单元包括以下要求：

a) 测评指标：**应分析外包服务或采购产品对云服务安全性的影响。（F3）**
b) 测评对象：云服务商所采购外包服务、产品。
c) 测评实施包括以下内容：
   1) 应核查云服务商是否分析外包服务或采购产品对云服务安全性的影响。
   2) 应核查是否具有分析外包服务或采购产品对云服务安全性的影响报告。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.7 安全运维管理

7.2.7.1 云计算环境管理

测评单元（L3-MMS2-01）

该测评单元包括以下要求：

a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。
b) 测评对象：运维设备、运维地点、运维记录和相关管理文档。
c) 测评实施：应核查运维地点是否位于中国境内，从境外对境内云计算平台实施远程运维操作的行为是否遵循国家相关规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.2.7.2 网络和系统安全管理

测评单元（L3-MMS2-02）

该测评单元包括以下要求：

a) 测评指标：**云服务商应制定相关策略，持续监控设备、资源、服务以及安全措施的有效性，并将安全措施有效性的监控结果定期提供给云服务客户。（F3）**
b) 测评对象：云服务商、云服务客户、相关安全策略。

c) 测评实施：应核查云服务商是否制定相关安全策略，要求持续监控设备、资源、服务以及安全措施的有效性，并将安全措施有效性的监控结果定期提供给云服务客户。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.2.7.3 应急预案管理

测评单元（L3-MMS2-03）

该测评单元包括以下要求：
a) 测评指标：**云服务提供商应将应急预案提前告知云服务客户。（F3）**
b) 测评对象：云服务商和应急预案。
c) 测评实施：应核查云服务提供商是否将应急预案提前告知云服务客户。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3 移动互联安全测评扩展要求

7.3.1 安全物理环境

7.3.1.1 无线接入点的物理位置

测评单元（L3-PES3-01）

该测评单元包括以下要求：
a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。
b) 测评对象：无线接入设备。
c) 测评实施包括以下内容：
   1) 应核查物理位置与无线信号的覆盖范围是否合理。
   2) 应测试验证无线信号是否可以避免电磁干扰。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES3-02）

该测评单元包括以下要求：
a) 测评指标：**应为营业网点的无线接入设备的安装选择合理位置，避免被非法破坏、替换。（F3）**
b) 测评对象：无线接入设备。
c) 测评实施包括以下内容：
   1) 应核查物理位置与无线信号的覆盖范围是否合理。
   2) 应核查是否采取防破坏、替换措施并定期检查。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2 安全通信网络

7.3.2.1 通信传输

测评单元（L3-CNS3-01）

该测评单元包括以下要求：
a) 测评指标：**应在移动终端与服务器之间建立安全的信息传输通道，例如使用有效安全版本的 TLS 或 IPSec 等协议。（F3）**
b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件的协议。
c) 测评实施：应劫持移动端与服务器之间传输协议，核查传输协议类型和版本是否安全。

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。

测评单元（L3-CNS3-02）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件与服务器应进行双向认证，可通过密钥、证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。（F3）**
b) 测评对象：客户端认证协议。
c) 测评实施包括以下内容：
   1) 应核查客户端应用软件与服务器是否采用双向协议。
   2) 应核查认证方式是否为安全认证方式。
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。

测评单元（L3-CNS3-03）

该测评单元包括以下要求：

a) 测评指标：**通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术。（F3）**
b) 测评对象：客户端发起的资金类报文及保护措施。
c) 测评实施：应核查客户端应用软件发起的资金类交易报文是否具有抗抵赖措施。
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。

测评单元（L3-CNS3-04）

该测评单元包括以下要求：

a) 测评指标：**通过客户端应用软件发起的资金类交易报文或客户敏感信息变更报文，应能够防止重放攻击。（F3）**
b) 测评对象：客户端发起的身份认证或资金类报文及保护措施。
c) 测评实施：应通过获取客户端应用软件发起的资金类交易报文或客户敏感信息变更报文，发起重放攻击等方式，测试验证是否具有抗重放的机制。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3 安全区域边界

7.3.3.1 边界防护

测评单元（L3-ABS3-01）

该测评单元包括以下要求：

a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。
b) 测评对象：无线接入网关设备。
c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3.2 访问控制

测评单元（L3-ABS3-02）

该测评单元包括以下要求：

a) 测评指标：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。
b) 测评对象：无线接入设备。

c) 测评实施：应核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3.3 入侵防范

测评单元（L3-ABS3-03）

该测评单元包括以下要求：
a) 测评指标：应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够检测非授权无线接入设备和移动终端的接入行为。
   2) 应测试验证是否能够检测非授权无线接入设备和移动终端的接入行为。
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。

测评单元（L3-ABS3-04）

该测评单元包括以下要求：
a) 测评指标：应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为。
b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够对网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测。
   2) 应核查规则库版本是否及时更新。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-ABS3-05）

该测评单元包括以下要求：
a) 测评指标：应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态。
b) 测评对象：无线接入设备或相关组件。
c) 测评实施：应核查是否能够检测无线接入设备的SSID广播、WPS等高风险功能的开启状态。
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。

测评单元（L3-ABS3-06）

该测评单元包括以下要求：
a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等。
b) 测评对象：无线接入设备和无线接入网关设备。
c) 测评实施：应核查是否关闭了SSID广播、WEP认证等存在风险的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-ABS3-07）

该测评单元包括以下要求：
a) 测评指标：应禁止多个AP使用同一个认证密钥。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否分别使用了不同的认证密钥。

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。

测评单元（L3-ABS3-08）

该测评单元包括以下要求：

a) 测评指标：应能够阻断非授权无线接入设备或非授权移动终端。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够阻断非授权无线接入设备或非授权移动终端接入。
   2) 应测试验证是否能够阻断非授权无线接入设备或非授权移动终端接入。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.4 安全计算环境

7.3.4.1 移动终端管控

测评单元（L3-CES3-01）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、注册并运行终端管理客户端软件。
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施：应核查移动终端是否安装、注册并运行移动终端客户端软件。
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。

测评单元（L3-CES3-02）

该测评单元包括以下要求：

a) 测评指标：移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施包括以下内容：
   1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略。
   2) 应测试验证是否能够对移动终端进行远程锁定和远程擦除等。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.4.2 移动应用管控

测评单元（L3-CES3-03）

该测评单元包括以下要求：

a) 测评指标：应具有选择应用软件安装、运行的功能。
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查是否具有选择应用软件安装、运行的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CES3-04）

该测评单元包括以下要求：

a) 测评指标：应只允许指定证书签名的应用软件安装和运行。
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查全部移动应用是否由指定证书签名。

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

测评单元（L3-CES3-05）

该测评单元包括以下要求：

a) 测评指标：应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。
b) 测评对象：移动终端管理客户端。
c) 测评实施包括以下内容：
   1) 应核查是否具有软件白名单功能。
   2) 应测试验证白名单功能是否能够控制应用软件安装、运行。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.4.3 访问控制

测评单元（L3-CES3-06）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。（F3）**
b) 测评对象：移动客户端权限。
c) 测评实施：应核查客户端应用软件向移动终端操作系统申请的权限是否是业务必须获取的权限。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CES3-07）

该测评单元包括以下要求：

a) 测评指标：**应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问。（F3）**
b) 测评对象：移动客户端权限。
c) 测评实施：应核查客户端应用软件数据是否仅能被授权用户或授权应用组件访问。
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。

测评单元（L3-CES3-08）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。（F3）**
b) 测评对象：移动客户端权限。
c) 测评实施包括以下内容：
   1) 应核查客户端应用软件访问的文件和数据是否在授权范围。
   2) 应核查客户端应用软件是否未访问非业务必需的文件和数据。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.4.4 安全审计

测评单元（L3-CES3-09）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文。（F3）**
b) 测评对象：运行日志。
c) 测评实施包括以下内容：
   1) 应核查运行日志是否未打印支付敏感信息。

2) 应核查运行日志是否未打印完整的敏感数据原文。

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

7.3.4.5 入侵防范

测评单元（L3-CES3-10）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件应对软件接口进行保护，防止其他应用对客户端应用软件接口进行非授权调用。（F3）**

b) 测评对象：移动客户端软件接口。

c) 测评实施：应核查客户端应用软件是否对软件接口进行保护，是否能防止其他应用对客户端应用软件接口进行非授权调用。

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。

测评单元（L3-CES3-11）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。（F3）**

b) 测评对象：移动客户端软件抗攻击能力。

c) 测评实施：应核查客户端应用软件是否具备基本的抗攻击能力，是否能抵御静态分析、动态调试等操作。

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。

测评单元（L3-CES3-12）

该测评单元包括以下要求：

a) 测评指标：**客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。（F3）**

b) 测评对象：移动客户端软件抗攻击能力。

c) 测评实施：应核查客户端应用软件是否具有代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。

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。

测评单元（L3-CES3-13）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。（F3）**

b) 测评对象：移动客户端软件防劫持能力。

c) 测评实施：应核查客户端应用软件在安装、启动、更新时是否对自身的完整性和真实性进行校验以抵御篡改、替换或劫持。

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

7.3.5 安全建设管理

7.3.5.1 移动应用软件采购

测评单元（L3-CMS3-01）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

b) 测评对象：移动终端。
c) 测评实施：应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-CMS3-02）

该测评单元包括以下要求：
a) 测评指标：应保证移动终端安装、运行的应用软件由指定的开发者开发。
b) 测评对象：移动终端。
c) 测评实施：应核查移动应用软件是否由指定的开发者开发。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.5.2 移动应用软件开发

测评单元（L3-CMS3-03）

该测评单元包括以下要求：
a) 测评指标：应对移动业务应用软件开发者进行资格审查。
b) 测评对象：系统建设负责人。
c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查。
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。

测评单元（L3-CMS3-04）

该测评单元包括以下要求：
a) 测评指标：应保证开发移动业务应用软件的签名证书合法性。
b) 测评对象：移动业务应用软件的签名证书。
c) 测评实施：应核查开发移动业务应用软件的签名证书是否具有合法性。
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。

7.3.6 安全运维管理

7.3.6.1 配置管理

测评单元（L3-MMS3-01）

该测评单元包括以下要求：
a) 测评指标：应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。
b) 测评对象：记录表单类文档、移动终端管理系统或相关组件。
c) 测评实施：应核查是否建立无线接入设备和合法移动终端配置库，并通过配置库识别非法设备。
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。

7.4 物联网安全测评扩展要求

7.4.1 安全物理环境

7.4.1.1 感知节点设备物理防护

测评单元（L3-PES4-01）

该测评单元包括以下要求：

a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动等，**使用环境与外壳保护等级（IP 代码）范围一致。（F3）**
b) 测评对象：感知节点设备所处物理环境、设计文档或验收文档。
c) 测评实施包括以下内容:
   1) 应核查感知节点设备所处的物理环境、设计文档或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动、使用环境与外壳保护等级（IP 代码）等能力的说明，是否与实际情况一致。
   2) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动、外壳保护（IP 代码）等的防护措施。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES4-02）

该测评单元包括以下要求：
a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
b) 测评对象：感知节点设备所处物理环境和设计或验收文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致。
   2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES4-03）

该测评单元包括以下要求：
a) 测评指标：感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等。
b) 测评对象：感知节点设备所处物理环境和设计或验收文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备所处物理环境的设计或验收文档，是否具有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明，是否与实际情况一致。
   2) 应核查感知节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等防护措施。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-PES4-04）

该测评单元包括以下要求：
a) 测评指标：关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）。
b) 测评对象：关键感知节点设备的供电设备和设计或验收文档。
c) 测评实施包括以下内容：
   1) 应核查关键感知节点设备电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障关键感知节点设备长时间工作的电力供应措施。
   2) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。
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。

测评单元（L3-PES4-05）

该测评单元包括以下要求：

a) 测评指标：**感知节点设备的部署应遵循封闭性原则，降低设备被非法拆除、非法篡改的风险。（F3）**

b) 测评对象：感知节点所处物理环境和设计或验收文档。

c) 测评实施包括以下内容：

1) 应核查关键感知节点设备所处环境是否遵循了封闭性原则。

2) 应核查关键感知节点是否存在防止非法拆除的物理防护措施。

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

7.4.1.2 感知网关节点设备物理安全要求

测评单元（L3-PES4-06）

该测评单元包括以下要求：

a) 测评指标：**感知网关节点设备应具有持久稳定的电力供应措施。（F3）**

b) 测评对象：感知网关节点设备的供电设备和设计或验收文档。

c) 测评实施包括以下内容：

1) 应核查感知网关节点设备电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障感知网关节点设备持久稳定工作的电力供应措施。

2) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。

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。

测评单元（L3-PES4-07）

该测评单元包括以下要求：

a) 测评指标：**应保证感知网关节点设备所在物理环境具有良好的信号收发能力（如避免信道遭遇屏蔽）。（F3）**

b) 测评对象：设计或验收文档和感知网关节点设备所处物理环境。

c) 测评实施包括以下内容：

1) 应核查感知网关节点设备所处物理环境的设计或验收文档是否具有感知网关节点设备所处物理环境防强干扰、防屏蔽等能力的说明。

2) 应核查感知网关节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等保护措施。

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

测评单元（L3-PES4-08）

该测评单元包括以下要求：

a) 测评指标：**感知网关节点设备应具有定位装置。（F3）**

b) 测评对象：感知网关节点设备的功能和系统设计文档或产品白皮书。

c) 测评实施包括以下内容：

1) 应核查感知网关节点设备是否有 GPS 或类似定位装置设备功能，是否采取了防强干扰、防阻挡屏蔽等措施。

2) 应核查关键感知网关节点设备的定位功能是否有效和准确。

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

7.4.2 安全区域边界

7.4.2.1 接入控制

测评单元（L3-ABS4-01）

该测评单元包括以下要求：

a) 测评指标：应保证只有授权的感知节点可以接入，**应保证感知节点、感知网关节点及处理应用层任意两者间相互鉴别和授权，非授权的感知节点、感知网关节点、处理应用层不能相互接入。（F3）**
b) 测评对象：感知节点设备、感知网关节点及处理应用层和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点、感知网关节点及处理应用层任意两者间是否可相互进行鉴别和授权。
   2) 应对边界和感知层网络进行渗透测试，测试验证是否不存在绕过相关接入控制措施以及身份鉴别机制的方法。
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。

测评单元（L3-ABS4-02）

该测评单元包括以下要求：
a) 测评指标：**每个感知节点和感知网关节点应具备传感网络中唯一标识，且该标识不应被非授权访问所篡改。（F3）**
b) 测评对象：感知节点和感知网关节点设备的功能和系统设计文档、产品白皮书。
c) 测评实施包括以下内容：
   1) 应核查感知节点和感知网关节点设备的功能和系统设计文档、产品白皮书，是否可创建永久唯一标识符。
   2) 应核查感知节点和感知网关节点设备，创建的传感网络中唯一标识是否不可被非授权访问所篡改。
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。

测评单元（L3-ABS4-03）

该测评单元包括以下要求：
a) 测评指标：**具有指令接收功能的感知节点设备，应保证只有授权过的系统、终端可以对感知节点下发指令。（F3）**
b) 测评对象：感知节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备接入机制设计文档是否具有防止非法系统、终端设备下发指令的设计内容。
   2) 应对边界和感知层网络进行渗透测试，测试验证是否不存在非法下发指令的可能。
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。

测评单元（L3-ABS4-04）

该测评单元包括以下要求：
a) 测评指标：**由第三方平台提供感知节点、感知网关节点中转接入时，第三方平台的安全保护等级应不低于接入的物联网系统的安全保护等级。（F3）**
b) 测评对象：第三方平台和设计文档、安全保护等级报告。
c) 测评实施包括以下内容：
   1) 应核查第三方平台和设计文档、安全保护等级报告是否具有网络接入认证措施实现说明。
   2) 应核查第三方平台的安全保护等级是否不低于接入的物联网系统的安全保护等级。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.2.2 入侵防范

测评单元（L3-ABS4-05）

该测评单元包括以下要求：

a) 测评指标：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。
b) 测评对象：感知节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明。
   2) 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求。
   3) 应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
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。

测评单元（L3-ABS4-06）

该测评单元包括以下要求：
a) 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。
b) 测评对象：网关节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明。
   2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求。
   3) 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
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。

测评单元（L3-ABS4-07）

该测评单元包括以下要求：
a) 测评指标：**当感知网关节点检测到攻击行为时，应上报攻击源 IP、攻击类型、攻击时间等信息。（F3）**
b) 测评对象：网关节点设备和报警信息。
c) 测评实施包括以下内容：
   1) 应测试验证当感知网关节点受到攻击行为是否进行报警。
   2) 应测试验证报警信息是否包含攻击源 IP、攻击类型、攻击时间等。
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。

测评单元（L3-ABS4-08）

该测评单元包括以下要求：
a) 测评指标：**可编程的感知节点、网关节点禁止运行未授权的代码。（F3）**
b) 测评对象：感知节点设备、网关节点设备的功能、系统设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备、网关节点设备是否有用户权限设置功能，并严格限制默认账户的权限。
   2) 应测试验证感知节点设备、网关节点设备是否可设置用户运行代码的权限。
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。

7.4.3 安全计算环境

7.4.3.1 感知节点设备安全

测评单元（L3-CES4-01）

该测评单元包括以下要求：

a) 测评指标：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。
b) 测评对象：感知节点设备。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更。
   2) 应通过试图接入和控制传感网访问未授权的资源等方式，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。
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。

测评单元（L3-CES4-02）

该测评单元包括以下要求：

a) 测评指标：应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F3）**
b) 测评对象：网关节点设备（包括读卡器）。
c) 测评实施包括以下内容：
   1) 应核查是否对连接的网关节点设备（包括读卡器）进行身份标识与鉴别，是否配置了符合安全策略的参数，是否至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。
   2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
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。

测评单元（L3-CES4-03）

该测评单元包括以下要求：

a) 测评指标：应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令等其中一种身份鉴别机制。（F3）**
b) 测评对象：其他感知节点设备（包括路由节点）。
c) 测评实施包括以下内容：
   1) 应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数，是否至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。
   2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
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。

测评单元（L3-CES4-04）

该测评单元包括以下要求：

a) 测评指标：**应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F3）**
b) 测评对象：感知节点设备和系统设计文档。
c) 测评实施：应核查感知节点设备是否具备保存密码、密钥、设备标识等安全相关数据的安全单元。
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。

测评单元（L3-CES4-05）

该测评单元包括以下要求：

a) 测评指标：**针对可编程的感知节点设备，应进行代码安全审计。（F3）**
b) 测评对象：感知节点设备。
c) 测评实施：应核查针对可编程的感知节点设备是否进行了代码安全审计。

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

7.4.3.2 网关节点设备安全

测评单元（L3-CES4-06）

该测评单元包括以下要求：

a) 测评指标：应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F3）**

b) 测评对象：网关节点设备。

c) 测评实施包括以下内容：

1) 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心）进行标识并配置了鉴别功能，是否至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。

2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

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。

测评单元（L3-CES4-07）

该测评单元包括以下要求：

a) 测评指标：应具备过滤非法节点和伪造节点所发送的数据的能力。

b) 测评对象：网关节点设备。

c) 测评实施包括以下内容：

1) 应核查是否具备过滤非法节点和伪造节点发送的数据的功能。

2) 应测试验证是否能够过滤非法节点和伪造节点发送的数据。

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。

测评单元（L3-CES4-08）

该测评单元包括以下要求：

a) 测评指标：授权用户应能够在设备使用过程中对关键密钥进行在线更新。

b) 测评对象：感知节点设备。

c) 测评实施：应核查感知节点设备是否对其关键密钥进行在线更新。

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。

测评单元（L3-CES4-09）

该测评单元包括以下要求：

a) 测评指标：授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

b) 测评对象：感知节点设备。

c) 测评实施：应核查是否支持对其关键配置参数进行在线更新及在线更新方式是否有效。

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。

测评单元（L3-CES4-10）

该测评单元包括以下要求：

a) 测评指标：**对于具有数据处理能力的网关节点设备，授权用户应能够在设备使用过程中对相关处理逻辑进行在线更新。（F3）**

b) 测评对象：网关节点设备。

c) 测评实施：对于具有数据处理能力的网关节点设备，应核查是否支持对相关处理逻辑进行在线更新，并核查在线更新方式是否有效。
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。

测评单元（L3-CES4-11）

该测评单元包括以下要求：
a) 测评指标：**对于具有数据处理能力的网关节点设备，应具备计算逻辑主动校验功能，防止处理逻辑被恶意篡改。（F3）**
b) 测评对象：网关节点设备。
c) 测评实施：对于具有数据处理能力的网关节点设备，应核查是否具有计算逻辑主动校验功能，并核查校验是否有效。
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。

测评单元（L3-CES4-12）

该测评单元包括以下要求：
a) 测评指标：**应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F3）**
b) 测评对象：感知节点设备和系统设计文档。
c) 测评实施：应核查感知节点设备是否具备保存密码、密钥、设备标识等安全相关数据的安全单元。
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。

测评单元（L3-CES4-13）

该测评单元包括以下要求：
a) 测评指标：**应进行代码安全审计。（F3）**
b) 测评对象：感知节点设备和系统设计文档。
c) 测评实施：应核查是否具有代码安全审计记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.4.3.3 抗数据重放

测评单元（L3-CES4-14）

该测评单元包括以下要求：
a) 测评指标：应能够鉴别数据的新鲜性，避免历史数据的重放攻击。
b) 测评对象：感知节点设备。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放。
   2) 应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。
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。

测评单元（L3-CES4-15）

该测评单元包括以下要求：
a) 测评指标：应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。
b) 测评对象：感知节点设备。
c) 测评实施包括以下内容：
   1) 应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施。

2) 应测试验证是否能够避免数据的修改重放攻击。

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

7.4.3.4 数据融合处理

测评单元（L3-CES4-16）

该测评单元包括以下要求：

a) 测评指标：应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。

b) 测评对象：物联网应用系统。

c) 测评实施包括以下内容：

1) 应核查是否提供对来自传感网的数据进行数据融合处理的功能。

2) 应测试验证数据融合处理功能是否能够处理不同种类的数据。

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

7.4.3.5 访问控制

测评单元（L3-CES4-17）

该测评单元包括以下要求：

a) 测评指标：**未经过鉴别和授权的感知节点、感知网关节点、处理应用层不应相互访问。（F3）**

b) 测评对象：感知节点设备、感知网关节点及处理应用层和设计文档。

c) 测评实施包括以下内容：

1) 应核查感知节点、感知网关节点及处理应用层任意两者间是否相互进行鉴别和授权才能访问。

2) 应核查感知节点、感知网关节点及处理应用层任意两者间是否设置了访问控制机制，机制是否覆盖访问资源及相关操作。

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

7.4.4 安全运维管理

7.4.4.1 感知节点管理

测评单元（L3-MMS4-01）

该测评单元包括以下要求：

a) 测评指标：应指定人员**或使用自动化巡检手段**，定期**检查**感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护，**针对可编程的智能设备，应定期扫描处理逻辑、进行固件更新维护操作。（F3）**

b) 测评对象：维护记录、固件更新记录。

c) 测评实施包括以下内容：

1) 应访谈系统运维负责人是否有专门的人员或自动化工具对感知节点设备、网关节点设备进行定期维护，是否对可编程的智能设备定期扫描处理逻辑、进行固件更新。

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

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

测评单元（L3-MMS4-02）

该测评单元包括以下要求：

a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。
b) 测评对象：感知节点和网关节点设备安全管理文档。
c) 测评实施：应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L3-MMS4-03）

该测评单元包括以下要求：
a) 测评指标：应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。
b) 测评对象：感知节点设备、网关节点设备部署环境的管理制度。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备、网关节点设备部署环境管理文档是否包括负责核查和维护的人员调离工作岗位立即交还相关核查工具和核查维护记录等方面内容。
   2) 应核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS4-04）

该测评单元包括以下要求：
a) 测评指标：**应在经过充分测试评估后，在不影响感知节点、感知网关节点安全稳定运行的情况下进行补丁、固件更新等工作。（F3）**
b) 测评对象：补丁、固件更新管理制度和测试评估记录。
c) 测评实施包括以下内容：
   1) 应核查是否建立补丁、固件更新的操作规范等管理制度，明确进行补丁、固件更新前应经过充分测试评估。
   2) 应核查补丁、固件更新前是否有相应的测试评估记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L3-MMS4-05）

该测评单元包括以下要求：
a) 测评指标：**关键感知节点、感知网关节点应通过安全传输通道进行固件与补丁更新，在检测到异常时应能将结果上报至安全管理中心。（F3）**
b) 测评对象：关键感知节点、感知网关节点设备和系统设计文档。
c) 测评实施：应核查关键感知节点、感知网关节点设备是否通过安全传输通道进行固件与补丁更新并能将异常结果上报至安全管理中心。
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。

测评单元（L3-MMS4-06）

该测评单元包括以下要求：
a) 测评指标：**针对监控类的感知节点设备，应设置安全阈值，对如设备长时间静默、电压过低、仓库温湿度与噪音等环境要素超过安全范围等情况，进行在线预警。（F3）**
b) 测评对象：感知节点设备的功能和系统设计文档或产品白皮书。
c) 测评实施：应核查感知节点设备是否有设置安全阈值功能（如设备长时间静默、电压过低、仓库温湿度与噪音等要素），超过安全范围是否可进行在线预警。

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。

测评单元（L3-MMS4-07）

该测评单元包括以下要求：

a) 测评指标：**应对感知节点状态进行监测，发现异常时应定位处理。（F3）**

b) 测评对象：监测记录文档、监测数据分析报告。

c) 测评实施包括以下内容：

1) 应核查是否对感知节点设备状态进行监测，是否形成监测记录文档，是否组织人员对监测记录进行整理并保管。

2) 应核查发现异常时是否对监测记录进行分析、评审，形成监测数据分析报告并定位处理。

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。

8 第四级测评要求

8.1 安全测评通用要求

8.1.1 安全物理环境

8.1.1.1 物理位置选择

测评单元（L4-PES1-01）

该测评单元包括以下要求：

a) 测评指标：机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b) 测评对象：记录表单类文档和机房。

c) 测评实施包括以下内容：

1) 应核查所在建筑物是否具有建筑物抗震设防审批文档。

2) 应核查是否不存在雨水渗漏。

3) 应核查门窗是否不存在因风导致的尘土严重。

4) 应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。

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

测评单元（L4-PES1-02）

该测评单元包括以下要求：

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

b) 测评对象：机房。

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

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

测评单元（L4-PES1-03）

该测评单元包括以下要求：

a) 测评指标：**机房应避开火灾危险程度高的区域，周围100米内不得有加油站、燃气站等危险建筑。（F4）**

b) 测评对象：机房。

c) 测评实施：应核查机房是否不位于火灾危险程度高的区域，周围100米内是否没有加油站、燃气站等危险建筑。

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。

8.1.1.2 物理访问控制

测评单元（L4-PES1-04）

该测评单元包括以下要求：

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。
b) 测评对象：机房电子门禁系统。
c) 测评实施包括以下内容：
   1) 应核查机房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。

测评单元（L4-PES1-05）

该测评单元包括以下要求：

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。
b) 测评对象：机房电子门禁系统。
c) 测评实施包括以下内容：
   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。

测评单元（L4-PES1-06）

该测评单元包括以下要求：

b) 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物理隔离装置，在重要区域前设置交付或安装等过渡区域。（F4）**
c) 测评对象：机房。
d) 测评实施包括以下内容：
   1) 应核查机房是否划分区域进行管理，是否在区域和区域之间设置物理隔离装置。
   2) 应核查机房是否在重要区域前设置交付或安装等过渡区域。
e) 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。

8.1.1.3 防盗窃和防破坏

测评单元（L4-PES1-07）

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**放入机柜中**进行固定**放置并配备安全锁**，并设置明显的不易除去的标识。**（F4）**
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放入机柜中固定放置并配备安全锁。
   2) 应核查机房内设备或主要部件上是否设置了明显标签，且标注不易除去的标识。
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。

测评单元（L4-PES1-08）

该测评单元包括以下要求：

a) 测评指标：应将通信线缆铺设在隐蔽安全处。
b) 测评对象：机房通信线缆。
c) 测评实施：应核查机房内通信线缆是否铺设在隐蔽安全处，如桥架中等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-PES1-09）

该测评单元包括以下要求：
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，**机房主要出入口应安装如红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。（F4）**
b) 测评对象：机房防盗报警系统或视频监控系统。
c) 测评实施包括以下内容：
   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。
   3) 应核查机房主要出入口是否安装如红外线探测设备等光电防盗设备，并核查光电防盗设备是否可以显示入侵部位以及驱动声光报警装置。
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。

测评单元（L4-PES1-10）

该测评单元包括以下要求：
b) 测评指标：**应建立机房视频监控系统和动环监控系统，并对监控内容进行记录，对机房风冷水电设备、消防设施、门禁系统等重要设施实行 24 小时全面监控，视频监控记录和门禁系统出入记录至少保存 3 个月。（F4）**
c) 测评对象：机房视频监控系统和动环监控系统。
d) 测评实施包括以下内容：
   1) 应核查机房是否配置视频监控系统和动环监控系统。
   2) 应核查视频监控系统和动环监控系统是否启用。
   3) 应核查视频监控系统和动环监控系统是否对机房风冷水电设备、消防设施、门禁系统等重要设施是否实行 24 小时全面监控，并核查视频监控记录和门禁系统出入记录是否至少保存 3 个月。
e) 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。

8.1.1.4 防雷击

测评单元（L4-PES1-11）

该测评单元包括以下要求：
a) 测评指标：**机房所在建筑应设置防直击雷装置，根据要求装设建筑避雷针、避雷线、避雷网、避雷带等避雷装置，并定期对防雷设施进行维护和防雷检测。（F4）**
b) 测评对象：机房。
c) 测评实施：应核查机房所在建筑应设置防直击雷装置，装设避雷针、避雷线、避雷网、避雷带等避雷装置，是否定期对防雷设施进行维护和防雷检测。
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。

测评单元（L4-PES1-12）

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。

测评单元（L4-PES1-13）

该测评单元包括以下要求：
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。
b) 测评对象：机房防雷设施。
c) 测评实施包括以下内容：
   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。

测评单元（L4-PES1-14）

该测评单元包括以下要求：
a) 测评指标：**机房应通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。（F4）**
b) 测评对象：机房防雷设施和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房防雷设施是否通过有关部门验收。
   2) 应核查是否具有防雷设施的定期维护和检测记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.5 防火

测评单元（L4-PES1-15）

该测评单元包括以下要求：
a) 测评指标：机房应设置火灾自动消防系统，能够**通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式**自动检测火情、自动报警，并自动灭火。**（F4）**
b) 测评对象：机房防火设施。
c) 测评实施包括以下内容：
   1) 应核查机房内是否设置火灾自动消防系统。
   2) 应核查火灾自动消防系统是否可以通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式自动检测火情、自动报警并自动灭火。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES1-16）

该测评单元包括以下要求：
a) 测评指标：机房及相关的工作房间和辅助房应采用具有**至少2级**耐火等级的建筑材料。**（F4）**
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至少为2级。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-PES1-17）

该测评单元包括以下要求：
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。

b) 测评对象：机房管理员和机房。
c) 测评实施包括以下内容：
   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。

测评单元（L4-PES1-18）

该测评单元包括以下要求：
a) 测评指标：**机房应备有一定数量的对电子设备影响小的手持式灭火器，消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发。（F4）**
b) 测评对象：机房和消防报警系统。
c) 测评实施包括以下内容：
   1) 应核查机房是否备有一定数量的对电子设备影响小的手持式灭火器。
   2) 应核查消防报警系统是否具有与空调系统、新风系统、门禁系统联动的功能，且一般工作状态为手动触发。
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。

测评单元（L4-PES1-19）

该测评单元包括以下要求：
a) 测评指标：**机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收，纸张、磁带和胶卷等易燃物品要放置于金属制的防火柜内。（F4）**
b) 测评对象：机房验收类文档和机房。
c) 测评实施包括以下内容：
   1) 应核查机房验收文档，是否明确内部通道设置、装修装饰材料、设备线缆等满足消防验收要求。
   2) 应核查纸张、磁带和胶卷等易燃物品是否放置于防火柜内。
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。

测评单元（L4-PES1-20）

该测评单元包括以下要求：
a) 测评指标：**主机房宜采用管网式洁净气体灭火系统，也可采用高压细水雾灭火系统，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动，凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。（F4）**
b) 测评对象：机房灭火系统。
c) 测评实施包括以下内容：
   1) 应核查主机房是否采用管网式洁净气体灭火系统，或采用高压细水雾灭火系统，如设置洁净气体灭火系统的主机房，应核查是否配置防烟面具。
   2) 应核查机房是否同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动。
   3) 应核查设置洁净气体灭火系统的机房是否配置了专用空气呼吸器或氧气呼吸器。
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。

测评单元（L4-PES1-21）

该测评单元包括以下要求：
a) 测评指标：**应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。（F4）**

b) 测评对象：机房管理制度和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房管理制度是否具有每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练的相关要求。
   2) 应核查是否具有消防培训和演练记录。
   3) 应核查是否具有消防设施的定期检查记录。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES1-22）

该测评单元包括以下要求：
a) 测评指标：**机房应设置消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用，在机房通道上应设置显著的消防标志。（F4）**
b) 测评对象：机房。
c) 测评实施包括以下内容：
   1) 应核查机房是否设置消防逃生通道，并核查机房内各分区到各消防通道的道路是否通畅。
   2) 应核查消防逃生通道上是否设置显著的消防标志。
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。

8.1.1.6 防水和防潮

测评单元（L4-PES1-23）

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。

测评单元（L4-PES1-24）

该测评单元包括以下要求：
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。
b) 测评对象：机房。
c) 测评实施包括以下内容：
   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。

测评单元（L4-PES1-25）

该测评单元包括以下要求：
a) 测评指标：**为便于地下积水的转移，漏水隐患区域地面周围应设排水沟或地漏等排水设施，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。（F4）**
b) 测评对象：机房。
c) 测评实施包括以下内容：
   1) 应核查机房内漏水隐患区域地面周围是否设置排水沟或地漏等排水设施。
   2) 当采用吊顶上布置空调风口时，应核查机房风口位置是否没有设置在设备正上方。
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。

测评单元（L4-PES1-26）

该测评单元包括以下要求：

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。
b) 测评对象：机房漏水检测设施。
c) 测评实施包括以下内容：
   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。

测评单元（L4-PES1-27）

该测评单元包括以下要求：

a) 测评指标：**应对温湿度调节设备安装漏水报警装置，并设置防水堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。（F4）**
b) 测评对象：机房防水检测设施。
c) 测评实施包括以下内容：
   1) 应核查机房内是否对温湿度调节设备安装漏水报警装置，并设置防水堤。
   2) 应核查冷却塔、泵、水箱等供水设备是否具有防冻、防火措施。
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。

8.1.1.7 防静电

测评单元（L4-PES1-28）

该测评单元包括以下要求：

a) 测评指标：应采用防静电地板或地面并采用必要的接地防静电措施。
b) 测评对象：机房。
c) 测评实施包括以下内容：
   1) 应核查机房内是否安装了防静电地板或地面。
   2) 应核查机房内是否采用了接地防静电措施。
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。

测评单元（L4-PES1-29）

该测评单元包括以下要求：

a) 测评指标：应采取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。
b) 测评对象：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。

测评单元（L4-PES1-30）

该测评单元包括以下要求：

a) 测评指标：**主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F4）**
b) 测评对象：机房工作台。
c) 测评实施：应核查主机房和辅助区内的工作台面是否采用导静电或静电耗散材料。
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。

测评单元（L4-PES1-31）

该测评单元包括以下要求：

a) 测评指标：**进入机房应采取防尘措施，如准备鞋套，减少带入机房的灰尘。（F4）**
b) 测评对象：机房。
c) 测评实施：应核查机房是否采取防尘措施。
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。

8.1.1.8 温湿度控制

测评单元（L4-PES1-32）

该测评单元包括以下要求：

a) 测评指标：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。
b) 测评对象：机房温湿度调节设施。
c) 测评实施包括以下内容：
   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。

测评单元（L4-PES1-33）

该测评单元包括以下要求：

a) 测评指标：**机房应采用专用温湿度调节设备，并应满足机房监控系统的要求。（F4）**
b) 测评对象：机房温湿度调节设施。
c) 测评实施包括以下内容：
   1) 应核查机房内是否配备专用温湿度调节设备。
   2) 应核查机房内温湿度调节设备是否满足机房监控系统的要求。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES1-34）

该测评单元包括以下要求：

a) 测评指标：**温湿度调节设备的工作能力应满足机房负载要求，并应保有一定的余量。（F4）**
b) 测评对象：机房温湿度调节设施。
c) 测评实施包括以下内容：
   1) 应核查机房内温湿度调节设备是否满足机房负载要求。
   2) 应核查机房内温湿度调节设备是否保有一定的余量。
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。

8.1.1.9 电力供应

测评单元（L4-PES1-35）

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。

测评单元（L4-PES1-36）

该测评单元包括以下要求：

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。
b) 测评对象：机房备用供电设施。
c) 测评实施包括以下内容：
   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。

测评单元（L4-PES1-37）

该测评单元包括以下要求：

a) 测评指标：应**按照双路供电的原则**设置冗余或并行的电力电缆线路为计算机系统供电。**（F4）**
b) 测评对象：机房供电设施。
c) 测评实施包括以下内容：
   1) 应访谈机房管理员机房供电是否来自两个不同的变电站。
   2) 应核查机房是否按照双路供电的原则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。

测评单元（L4-PES1-38）

该测评单元包括以下要求：

a) 测评指标：应提供应急供电设施，**以备供电系统临时停电时启用，并确保应急供电设施能在 UPS 供电时间内到位，每年需进行应急供电设施的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用。（F4）**
b) 测评对象：机房应急供电设施和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否配置了应急供电设施。
   2) 应核查应急供电设施是否能在 UPS 供电时间内到位。
   3) 应核查是否具有应急供电设施带负载模拟演练的记录。
   4) 应核查是否具有电力供应设备及应急供电设施定期检修和维护的记录。
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。

测评单元（L4-PES1-39）

该测评单元包括以下要求：

a) 测评指标：**UPS 供电系统的冗余方式应采用 N+1、N+2、2N、2（N+1）等方式，负载功率小于单机 UPS 额定功率的 80%，并通过两路独立市电提供 UPS 输入，未建立备用发电机应急供电系统的单位，UPS 后备时间至少 2 小时，已建立备用发电机应急供电系统的单位，UPS 后备时间应满足至少 15 分钟以上。（F4）**
b) 测评对象：机房备用供电设施。
c) 测评实施包括以下内容：
   1) 应核查机房 UPS 供电系统的冗余方式是否采用 N+1、N+2、2N、2（N+1）等方式，负载功率是否小于单机 UPS 额定功率的 80%。
   2) 应核查是否通过两路独立市电提供 UPS 输入，对于建立备用发电机应急供电系统的单位，应核查 UPS 后备时间是否满足至少 2 小时。
   3) 应核查是否通过两路独立市电提供 UPS 输入，对于已建立备用发电机应急供电系统的单位，应核查 UPS 后备时间是否满足至少 15 分钟以上。
d) 单元判定：如果 1）和 2）均为肯定，或 1）和 3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES1-40）

该测评单元包括以下要求：

a) 测评指标：**计算机系统供电应与其他供电分开，机房内要求采用机房专用插座，市电、UPS 电源插座分开，满足负荷使用要求。（F4）**

b) 测评对象：机房供电设施。

c) 测评实施包括以下内容：

1) 应核查机房计算机系统供电是否与其他供电分开。

2) 应核查机房是否采用机房专用插座，市电、UPS 电源插座是否分开。

3) 应核查机房专用插座是否满足负荷使用要求

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

测评单元（L4-PES1-41）

该测评单元包括以下要求：

a) 测评指标：**计算机系统应选用铜芯电缆，避免铜、铝混用，若不能避免时，应采用铜铝过渡头连接。（F4）**

b) 测评对象：机房供电设施。

c) 测评实施包括以下内容：

1) 应核查机房是否采用铜芯电缆，避免铜、铝混用。

2) 如果铜、铝混用，应核查是否采用铜铝过渡头连接。

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，否则不符合本测评单元指标要求。

测评单元（L4-PES1-42）

该测评单元包括以下要求：

a) 测评指标：**机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。（F4）**

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房是否设置应急照明和安全出口指示灯。

2) 应核查机房供配电柜（箱）和分电盘内各种开关、手柄、按钮是否标志清晰。

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。

测评单元（L4-PES1-43）

该测评单元包括以下要求：

a) 测评指标：**机房重要区域、重要设备应提供 UPS 单独供电，核心区域、重要设备应由不同的 UPS 提供双回路供电。（F4）**

b) 测评对象：机房备用供电设施。

c) 测评实施包括以下内容：

1) 应核查机房重要区域、重要设备是否提供 UPS 单独供电。

2) 应核查机房内核心区域、重要设备是否由不同的 UPS 提供双回路供电。

3) 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。

8.1.1.10 电磁防护

测评单元（L4-PES1-44）

该测评单元包括以下要求：

a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰。

b) 测评对象：机房线缆。
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。

测评单元（L4-PES1-45）

该测评单元包括以下要求：
a) 测评指标：应对关键区域和关键设备**以及磁介质**实施电磁屏蔽。**（F4）**
b) 测评对象：机房关键设备或区域。
c) 测评实施包括以下内容：
   1) 应核查机房内是否针对关键区域实施了电磁屏蔽。
   2) 应核查机房内是否为关键设备配备了电磁屏蔽装置。
   3) 应核查机房内是否为磁介质配备了电磁屏蔽装置。
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。

8.1.2 安全通信网络

8.1.2.1 网络架构

测评单元（L4-CNS1-01）

该测评单元包括以下要求：
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，**如：业务处理能力能满足业务高峰期需要的 50%以上。（F4）**
b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信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是否满足需要。
   2) 应核查网络设备是否从未出现过因设备性能问题导致的宕机情况。
   3) 应测试验证设备是否满足业务高峰期需求。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CNS1-02）

该测评单元包括以下要求：
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。
b) 测评对象：综合网管系统等。
c) 测评实施包括以下内容：
   1) 应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量需要。
   2) 应测试验证网络带宽是否满足业务高峰期需求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CNS1-03）

该测评单元包括以下要求：
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。
b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否依据重要性、部门等因素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划分原则一致。

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。

测评单元（L4-CNS1-04）

该测评单元包括以下要求：

a) 测评指标：应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
b) 测评对象：网络拓扑。
c) 测评实施包括以下内容：
   1) 应核查网络拓扑图是否与实际网络运行环境一致。
   2) 应核查重要网络区域是否未部署在网络边界处。
   3) 应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、防火墙和设备访问控制列表（ACL）等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CNS1-05）

该测评单元包括以下要求：

a) 测评指标：应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性，**双线路设计时，宜由不同的电信运营商提供。（F4）**
b) 测评对象：网络管理员和网络拓扑。
c) 测评实施包括以下内容：
   1) 应核查是否有关键网络设备、安全设备和关键计算设备的硬件冗余（主备或双活等）和通信线路冗余。
   2) 应核查通信线路是否由不同电信运营商提供。
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。

测评单元（L4-CNS1-06）

该测评单元包括以下要求：

a) 测评指标：应按照业务服务的重要程度分配带宽，优先保障重要业务。
b) 测评对象：路由器、交换机和流量控制设备等提供带宽控制功能的设备或相关组件。
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。

测评单元（L4-CNS1-07）

该测评单元包括以下要求：

a) 测评指标：**应使用前置设备实现跨机构联网系统与入网金融机构业务主机系统的隔离，防止外部系统直接对入网金融机构业务主机的访问和操作。（F4）**
b) 测评对象：路由器、交换机和流量控制设备等提供带宽控制功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否使用前置设备实现跨机构联网系统与入网金融机构业务主机系统的隔离。
   2) 应测试验证前置设备是否能够防止外部系统直接对入网金融机构业务主机进行访问和操作。
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。

测评单元（L4-CNS1-08）

该测评单元包括以下要求：

a) 测评指标：**应使用专用网络用于金融机构间的重要信息交换，与公用数据网络隔离。（F4）**
b) 测评对象：路由器、交换机和流量控制设备等提供带宽控制功能的设备或相关组件。
c) 测评实施：应核查是否使用与公用数据网络隔离的专用网络用于金融机构间的重要信息交换。
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。

测评单元（L4-CNS1-09）

该测评单元包括以下要求：
a) 测评指标：**机构应至少通过两条主干链路接入跨机构交易交换网络，并可根据实际情况选择使用专用的通信链路。两条主干链路应具有不同的路由，当一条链路发生异常时，另一条链路应能承载全部的交易数据。（F4）**
b) 测评对象：路由器、交换机和流量控制设备等提供带宽控制功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查机构是否至少通过两条主干链路接入跨机构交易交换网络，是否可根据实际情况选择使用专用的通信链路。
   2) 应核查两条主干链路是否具有不同的路由。
   3) 应核查当一条链路发生异常时，另一条链路是否能承载全部的交易数据。
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。

8.1.2.2 通信传输

测评单元（L4-CNS1-10）

该测评单元包括以下要求：
a) 测评指标：应采用密码技术保证通信过程中数据的完整性，**并按照国家密码管理部门与行业有关要求使用密码算法。（F4）**
b) 测评对象：提供密码技术功能的设备或组件。
c) 测评实施包括以下内容：
   1) 应核查是否在数据传输过程中使用密码技术来保证其完整性。
   2) 应核查完整性措施所使用的密码算法是否符合国家密码管理部门与行业有关要求。
   3) 应测试验证密码技术设备或组件能否保证通信过程中数据的完整性。
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。

测评单元（L4-CNS1-11）

该测评单元包括以下要求：
a) 测评指标：应采用密码技术保证通信过程中数据的保密性，**并按照国家密码管理部门与行业有关要求使用密码算法。（F4）**
b) 测评对象：提供密码技术功能的设备或组件。
c) 测评实施包括以下内容：
   1) 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施。
   2) 应核查保密技术措施使用的密码算法是否符合国家密码管理部门与行业有关要求。
   3) 应测试验证在通信过程中是否对数据进行加密。
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。

测评单元（L4-CNS1-12）

该测评单元包括以下要求：
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。
b) 测评对象：提供密码技术功能的设备或组件。

c) 测评实施：应核查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。

测评单元（L4-CNS1-13）

该测评单元包括以下要求：
a) 测评指标：应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。
b) 测评对象：提供密码技术功能的设备或组件。
c) 测评实施包括以下内容：
   1) 应核查是否基于硬件密码模块产生密钥并进行密码运算。
   2) 应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。
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。

8.1.2.3 可信验证

测评单元（L4-CNS1-14）

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、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。
b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。
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、重要配置参数和通信应用程序等进行可信验证。
   2) 应核查是否在应用程序的所有执行环节进行动态可信验证。
   3) 应测试验证当检测到通信设备的可信性受到破坏后是否进行报警。
   4) 应测试验证结果是否以审计记录的形式送至安全管理中心。
   5) 应核查是否能够进行动态关联感知。
d) 单元判定：如果1）～5）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。

8.1.3 安全区域边界

8.1.3.1 边界防护

测评单元（L4-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）核查或测试验证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。

测评单元（L4-ABS1-02）

该测评单元包括以下要求：

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检查或限制。
b) 测评对象：终端管理系统或相关设备。
c) 测评实施包括以下内容：
   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。
   2) 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。
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。

测评单元（L4-ABS1-03）

该测评单元包括以下要求：

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检查或限制。
b) 测评对象：终端管理系统或相关设备。
c) 测评实施：应核查是否采用技术措施防止内部用户存在非法外联行为。
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。

测评单元（L4-ABS1-04）

该测评单元包括以下要求：

a) 测评指标：应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
b) 测评对象：网络拓扑和无线网络设备。
c) 测评实施包括以下内容：
   1) 应核查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) 应核查无线网络是否通过受控的边界防护设备接入到内部有线网络。
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。

测评单元（L4-ABS1-05）

该测评单元包括以下要求：

a) 测评指标：应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断。
b) 测评对象：终端管理系统或相关设备。
c) 测评实施包括以下内容：
   1) 应核查是否采用技术措施能够对非授权设备接入内部网络的行为进行有效阻断。
   2) 应核查是否采用技术措施能够对内部用户非授权联到外部网络的行为进行有效阻断。
   3) 应测试验证是否能够对非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为进行有效阻断。
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。

测评单元（L4-ABS1-06）

该测评单元包括以下要求：

a) 测评指标：应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。
b) 测评对象：终端管理系统或相关设备。
c) 测评实施包括以下内容：
   1) 应核查是否采用可信验证机制对接入到网络中的设备进行可信验证。
   2) 应测试验证是否能够对连接到内部网络的设备进行可信验证。

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。

8.1.3.2 访问控制

测评单元（L4-ABS1-07）

该测评单元包括以下要求：

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。
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) 应核查在网络边界或区域之间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。

测评单元（L4-ABS1-08）

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。

测评单元（L4-ABS1-09）

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) 测评实施包括以下内容：
   1) 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。
   2) 应测试验证访问控制策略中设定的相关配置参数是否有效。
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。

测评单元（L4-ABS1-10）

该测评单元包括以下要求：

b) 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。（F4）**
c) 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。
d) 测评实施包括以下内容：

1） 应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力，控制粒度是否为端口级。
2） 应测试验证是否为进出数据流提供明确的允许/拒绝访问的能力。

e） 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。

测评单元（L4-ABS1-11）

该测评单元包括以下要求：

a） 测评指标：应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。
b） 测评对象：网闸等提供通信协议转换或通信协议隔离功能的设备或相关组件。
c） 测评实施包括以下内容：
1） 应核查是否采取通信协议转换或通信协议隔离等方式进行数据交换。
2） 应通过发送带通用协议的数据等测试方式，测试验证设备是否能够有效阻断。
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。

测评单元（L4-ABS1-12）

该测评单元包括以下要求：

a） 测评指标：**应对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。（F4）**
b） 测评对象：网闸等提供通信协议转换或通信协议隔离功能的设备或相关组件。
c） 测评实施包括以下内容：
1） 应核查是否梳理网络设备自带端口，并关闭不必要端口。
2） 应核查是否制定端口开放审批制度。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ABS1-13）

该测评单元包括以下要求：

a） 测评指标：**应每季度检查并锁定或撤销网络设备中不必要的用户账号。（F4）**
b） 测评对象：网闸等提供通信协议转换或通信协议隔离功能的设备或相关组件。
c） 测评实施：应核查是否按季度检查并锁定或撤销网络设备中不必要的用户账号。
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。

8.1.3.3 入侵防范

测评单元（L4-ABS1-14）

该测评单元包括以下要求：

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。
b） 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c） 测评实施包括以下内容：
1） 应核查相关系统或组件是否能够检测从外部发起的网络攻击行为。
2） 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本。
3） 应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点。
4） 应测试验证相关系统或组件的配置信息或安全策略是否有效。
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。

测评单元（L4-ABS1-15）

该测评单元包括以下要求：

a) 测评指标：应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查相关系统或组件是否能够检测到从内部发起的网络攻击行为。
   2) 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本。
   3) 应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点。
   4) 应测试验证相关系统或组件的配置信息或安全策略是否有效。
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。

测评单元（L4-ABS1-16）

该测评单元包括以下要求：

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新型网络攻击行为的分析。
b) 测评对象：抗 APT 攻击系统、网络回溯系统和威胁情报检测系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否部署相关系统或组件对新型网络攻击进行检测和分析。
   2) 应测试验证是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。

测评单元（L4-ABS1-17）

该测评单元包括以下要求：

a) 测评指标：当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查相关系统或组件的记录是否包括攻击源 IP、攻击类型、攻击目标、攻击时间等相关内容。
   2) 应测试验证相关系统或组件的报警策略是否有效。
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。

测评单元（L4-ABS1-18）

该测评单元包括以下要求：

a) 测评指标：**应采取技术手段对高级持续威胁进行监测、发现。（F4）**
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施：应核查相关系统或组件是否采取技术手段对高级持续威胁进行监测、发现。
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。

测评单元（L4-ABS1-19）

该测评单元包括以下要求：

a) 测评指标：**入侵检测的管理系统应做到分级管理，对系统的部署做到逐级分布。（F4）**
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查入侵检测的管理系统是否做到分级管理。
   2) 应核查对系统的部署是否做到逐级分布。
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。

测评单元（L4-ABS1-20）

该测评单元包括以下要求：
a) 测评指标：**应采用联动防护机制，及时识别网络攻击行为，并实现快速处置。（F4）**
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施：应核查是否采用联动防护机制及时识别网络攻击行为，并实现快速处置。
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。

8.1.3.4 恶意代码和垃圾邮件防范

测评单元（L4-ABS1-21）

该测评单元包括以下要求：
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。
b) 测评对象：防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查在关键网络节点处是否部署防恶意代码产品等技术措施。
   2) 应核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新。
   3) 应测试验证相关系统或组件的安全策略是否有效。
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。

测评单元（L4-ABS1-22）

该测评单元包括以下要求：
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。
b) 测评对象：防垃圾邮件网关等提供防垃圾邮件功能的系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查在关键网络节点处是否部署了防垃圾邮件产品等技术措施。
   2) 应核查防垃圾邮件产品运行是否正常，防垃圾邮件规则库是否已经更新到最新。
   3) 应测试验证相关系统或组件的安全策略是否有效。
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。

8.1.3.5 安全审计

测评单元（L4-ABS1-23）

该测评单元包括以下要求：
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。

b) 测评对象：综合安全审计系统等。
c) 测评实施包括以下内容：
   1) 应核查是否部署了综合安全审计系统或类似功能的系统平台。
   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了审计。
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。

测评单元（L4-ABS1-24）

该测评单元包括以下要求：
a) 测评指标：**应记录无线网络接入行为，形成日志进行留存，保存时间不少于 6 个月。（F4）**
b) 测评对象：综合安全审计系统等。
c) 测评实施包括以下内容：
   1) 应核查是否有记录无线网络接入行为，并形成日志进行留存。
   2) 应核查日志保存时间不少于 6 个月。
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。

测评单元（L4-ABS1-25）

该测评单元包括以下要求：
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。
b) 测评对象：综合安全审计系统等。
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。

测评单元（L4-ABS1-26）

该测评单元包括以下要求：
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，**审计记录保存时间不少于 6 个月。（F4）**
b) 测评对象：综合安全审计系统等。
c) 测评实施包括以下内容：
   1) 应核查是否采取了技术措施能够对审计记录进行保护。
   2) 应核查是否采取技术措施对审计记录进行定期备份。
   3) 应核查审计记录保存时间是否不少于 6 个月。
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。

测评单元（L4-ABS1-27）

该测评单元包括以下要求：
a) 测评指标：**所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致。（F4）**
b) 测评对象：综合安全审计系统等。
c) 测评实施包括以下内容：
   1) 应访谈网络安全管理员是否采用了技术手段进行网络设备时钟同步。
   2) 应核查是否所有的审计手段都具备统一的时间戳。
   3) 应抽查相关网络设备，核查是否时间一致。
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，否则不符合本测评单元指标要求。

8.1.3.6 可信验证

测评单元（L4-ABS1-28）

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、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。

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、重要配置参数和边界防护应用程序等进行可信验证。

2) 应核查是否在应用程序的所有执行环节进行动态可信验证。

3) 应测试验证当检测到边界设备的可信性受到破坏后是否进行报警。

4) 应测试验证结果是否以审计记录的形式送至安全管理中心。

5) 应核查是否能够进行动态关联感知。

d) 单元判定：如果 1）～5）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。

8.1.4 安全计算环境

8.1.4.1 身份鉴别

测评单元（L4-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，**应实现身份鉴别信息防窃取和防重用。静态口令应在 8 位以上，由字母、数字、符号等混合组成，至少每 90 天更换口令一次，不允许新设定的口令与前三次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定期更换。（F4）**

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或测试验证是否不存在空口令用户。

4) 应核查用户身份鉴别信息是否具有防窃取和防重用措施。

5) 应核查除应用系统用户以外的用户静态口令是否在 8 位以上，由字母、数字、符号等混合组成并至少每 90 天更换一次，不允许新设定的口令与前三次旧口令相同。

6) 应核查应用系统用户静态口令是否满足 8 位以上，由字母、数字、符号混合组成并定期更换。

d) 单元判定：如果 1）～6）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。

测评单元（L4-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、**限制登录间隔、**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。**（F4）**

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、限制登录间隔等。
   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。

测评单元（L4-CES1-03）

该测评单元包括以下要求：

a) 测评指标：**操作系统和数据库系统应设置鉴别警示信息，当出现越权访问或尝试非法访问时，系统会自动提示未授权访问。（F4）**

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) 应核查操作系统和数据库系统是否设置鉴别警示信息。
   2) 应核查当出现越权访问或尝试非法访问时，系统是否自动提示未授权访问。

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。

测评单元（L4-CES1-04）

该测评单元包括以下要求：

a) 测评指标：当进行远程管理时，应**对终端进行身份标识和鉴别，采用密码技术**防止鉴别信息在网络传输过程中被窃听。**（F4）**

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：
   1) 应核查是否对终端进行身份标识和鉴别。
   2) 应核查是否采用密码技术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。

测评单元（L4-CES1-05）

该测评单元包括以下要求：

a) 测评指标：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

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) 应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别。

2） 应核查其中一种鉴别技术是否使用密码技术来实现。

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。

8.1.4.2 访问控制

测评单元（L4-CES1-06）

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） 应核查是否为用户分配了账户和权限及相关设置情况。

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。

测评单元（L4-CES1-07）

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**和预设账户**的默认口令。**（F4）**

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和预设账户的默认口令。

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。

测评单元（L4-CES1-08）

该测评单元包括以下要求：

a） 测评指标：**应用系统应强制首次登录的用户修改默认账户或预设账户的默认口令。（F4）**

b） 测评对象：业务应用系统。

c） 测评实施包括以下内容：

1） 应核查应用系统是否对首次登录的用户强制修改默认账户或预设账户的默认口令。

2） 应核查是否已修改默认账户或预设账户的默认口令。

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。

测评单元（L4-CES1-09）

该测评单元包括以下要求：

a） 测评指标：**宜通过技术手段定期检测是否存在多余的、过期的账户。（F4）**

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：应核查是否通过技术手段定期检测多余的、过期的账户。

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。

测评单元（L4-CES1-10）

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) 应测试验证多余的、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。

测评单元（L4-CES1-11）

该测评单元包括以下要求：

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。

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) 应核查是否进行角色划分。

2) 应核查管理用户的权限是否已进行分离。

3) 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。

测评单元（L4-CES1-12）

该测评单元包括以下要求：

a) 测评指标：**应严格限制默认账户或预设账户的权限，如默认账户或预设账户的权限应为空权限或某单一功能专用权限等。（F4）**

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：应核查是否严格限制默认账户或预设账户的权限，如将默认账户或预设账户的权限设置为空权限或某单一功能专用权限等。

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

测评单元（L4-CES1-13）

该测评单元包括以下要求：

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。

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、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） 应核查是否由授权主体（如管理用户）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） 应测试验证用户是否有可越权访问情形。

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。

测评单元（L4-CES1-14）

该测评单元包括以下要求：

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。
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、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。

测评单元（L4-CES1-15）

该测评单元包括以下要求：

a） 测评指标：应对主体、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。
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、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） 应核查是否对主体、客体设置了安全标记。
2） 应测试验证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。

8.1.4.3 安全审计

测评单元（L4-CES1-16）

该测评单元包括以下要求：

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。
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。

测评单元（L4-CES1-17）

该测评单元包括以下要求：

a） 测评指标：审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等。

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：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。

测评单元（L4-CES1-18）

该测评单元包括以下要求：
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，**审计记录保存时间应不少于 6 个月。（F4）**
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) 应核查是否采取了保护措施对审计记录进行保护。
   2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。
   3) 应核查审计记录保存时间是否不少于 6 个月。
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。

测评单元（L4-CES1-19）

该测评单元包括以下要求：
a) 测评指标：应对审计进程**或程序**进行保护，防止未经授权的中断。**（F4）**
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：应测试验证通过非审计管理员的其他账户来中断审计进程或程序，验证审计进程或程序是否受到保护。
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。

测评单元（L4-CES1-20）

该测评单元包括以下要求：
a) 测评指标：**对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息，以便能够及时发现可能的问题。（F4）**
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：对于从互联网客户端登录的应用系统，应测试验证是否能在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。
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。

测评单元（L4-CES1-21）

该测评单元包括以下要求：

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，以确保审计分析的一致性与正确性。（F4）**

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：应测试验证审计记录产生时的时间是否由系统范围内唯一确定的时钟产生。

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。

8.1.4.4 入侵防范

测评单元（L4-CES1-22）

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） 应核查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。

测评单元（L4-CES1-23）

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 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。

测评单元（L4-CES1-24）

该测评单元包括以下要求：

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。

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：应核查配置文件或参数等是否对终端接入范围进行限制。

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

测评单元（L4-CES1-25）

该测评单元包括以下要求：

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。
b) 测评对象：业务应用系统、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) 应测试验证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。

测评单元（L4-CES1-26）

该测评单元包括以下要求：
a) 测评指标：应能**通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时**发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。**（F4）**
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等。
c) 测评实施包括以下内容：
   1) 应核查是否使用漏洞扫描工具、人工漏洞排查分析等检查手段开展漏洞检查工作。
   2) 应核查是否不存在高风险漏洞或在充分测试评估后及时修补漏洞。
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。

测评单元（L4-CES1-27）

该测评单元包括以下要求：
a) 测评指标：应能够检测到对**所有**节点进行入侵的行为，并在发生严重入侵事件时提供报警。**（F4）**
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) 应核查是否采取技术措施对所有节点进行入侵检测。
   2) 应核查是否能对严重入侵事件进行报警，如声音、邮件、短信等方式。。
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。

测评单元（L4-CES1-28）

该测评单元包括以下要求：
a) 测评指标：**所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F4）**
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) 应核查各安全计算环境设备的业务用途是否专用化。
   2) 应核查各安全计算环境设备是否未进行过与业务用途不相关的操作。
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。

测评单元（L4-CES1-29）

该测评单元包括以下要求：

a) 测评指标：**应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接或间接反馈到前台界面。（F4）**
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：应通过给系统人为制造一些故障（如系统异常），测试验证系统是否未在故障发生时将技术错误信息直接或间接反馈到前台界面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.5 恶意代码防范

测评单元（L4-CES1-30）

该测评单元包括以下要求：
a) 测评指标：应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
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）、移动终端、移动终端管理系统、移动终端管理客户端和控制设备等。
c) 测评实施包括以下内容：
   1) 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为。
   2) 应核查当识别入侵和病毒行为时，是否将其有效阻断。。
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。

测评单元（L4-CES1-31）

该测评单元包括以下要求：
a) 测评指标：**应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F4）**
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）、移动终端、移动终端管理系统、移动终端管理客户端和控制设备等。
c) 测评实施：应核查是否建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。
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。

8.1.4.6 可信验证

测评单元（L4-CES1-32）

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、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。
b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。
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、重要配置参数和应用程序等进行可信验证。
   2) 应核查是否在应用程序的所有执行环节进行动态可信验证。
   3) 应测试验证当检测到计算设备的可信性受到破坏后是否进行报警。
   4) 应测试验证结果是否以审计记录的形式送至安全管理中心。
   5) 应核查是否能够进行动态关联感知。
d) 单元判定：如果 1）～5）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。

8.1.4.7 数据完整性

测评单元（L4-CES1-33）

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

c) 测评实施包括以下内容：

1) 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性。

2) 应测试验证应用系统在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，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。

测评单元（L4-CES1-34）

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

c) 测评实施包括以下内容：

1) 应核查设计文档，是否采用了密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性。

2) 应核查应用系统是否采用技术措施（如数据安全保护系统等）保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性。

3) 应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，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。

测评单元（L4-CES1-35）

该测评单元包括以下要求：

a) 测评指标：在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。**证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户。（F4）**

b) 测评对象：业务应用系统和数据库管理系统等。

c) 测评实施包括以下内容：

1) 应核查设计文档，是否采用了密码技术保证数据发送和数据接收操作的不可抵赖性。

2) 应核查是否采取技术措施保证数据发送和数据接收操作的不可抵赖性。

3) 应测试验证是否能够检测到数据在传输过程中不能被篡改。

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

8.1.4.8 数据保密性

测评单元（L4-CES1-36）

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
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) 测评实施包括以下内容：
   1) 应核查系统设计文档，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性。
   2) 应通过嗅探等方式抓取传输过程中的数据包，测试验证鉴别数据、重要业务数据和重要个人信息等传输过程中是否进行了加密处理。
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。

测评单元（L4-CES1-37）

该测评单元包括以下要求：

a) 测评指标：应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据**和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护其存储过程中的保密性。（F4）**
b) 测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。
c) 测评实施包括以下内容：
   1) 应核查是否采用密码技术保证系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息在存储过程中的保密性。
   2) 应核查是否采用技术措施（如数据安全保护系统等）保证系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息在存储过程中的保密性。
   3) 应测试验证是否对指定的数据进行加密处理。
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。

8.1.4.9 数据备份恢复

测评单元（L4-CES1-38）

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，**采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指标（如RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放，数据保存期限依照国家相关规定。（F4）**
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) 应核查备份策略设置是否合理、配置是否正确。
   2) 应核查是否按照备份策略进行本地备份。
   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。
   5) 应核查备份介质是否场外存放。
   6) 应核查备份数据保存期限是否满足国家相关规定。
d) 单元判定：如果1）～6）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。

测评单元（L4-CES1-39）

该测评单元包括以下要求：

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。
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。

测评单元（L4-CES1-40）

该测评单元包括以下要求：

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。
b) 测评对象：重要数据处理系统。
c) 测评实施包括以下内容：应核查重要数据处理系统（包括边界路由器、边界防火墙、核心交换机、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。

测评单元（L4-CES1-41）

该测评单元包括以下要求：

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。
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   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。

测评单元（L4-CES1-42）

该测评单元包括以下要求：

a) 测评指标：**对于同城应用级灾难备份中心，应与生产中心直线距离至少达到 30km，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到 100km。（F4）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否建立了同城应用级灾难备份中心，且与生产中心直线距离至少达到 30km。
   2) 应核查同城应用级灾难备份中心是否可以接管所有核心业务的运行。
   3) 应核查是否建立了异地应用级灾难备份中心，且与生产中心直线距离至少达到 100km。
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。

测评单元（L4-CES1-43）

该测评单元包括以下要求：

a) 测评指标：**为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。（F4）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否对技术方案中关键技术应用的可行性进行验证测试。
   2) 应核查是否记录和保存验证测试的结果。

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。

测评单元（L4-CES1-44）

该测评单元包括以下要求：

a) 测评指标：**数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个月为周期的数据冗余。（F4）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   1) 应核查数据备份是否至少保存两个副本，且至少一份副本异地存放。
   2) 应核查完全数据备份是否至少保证以一个月为周期的数据冗余。
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。

测评单元（L4-CES1-45）

该测评单元包括以下要求：

a) 测评指标：**异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资源（相关软硬件以及数据等资源）已完全满足但设备 CPU 还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU 也在运行状态。（F4）**
b) 测评对象：灾难备份中心及相关组件。
c) 测评实施包括以下内容：
   1) 应核查异地灾难备份中心是否配备恢复所需的运行环境，并处于就绪状态或运行状态。
   2) 应核查备份中心的所需资源（相关软硬件以及数据等资源）是否已完全满足，设备 CPU 还没有运行或者已经处于运行状态中。
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。

8.1.4.10 剩余信息保护

测评单元（L4-CES1-46）

该测评单元包括以下要求：

a) 测评指标：应保证**操作系统、数据库系统和应用系统用户**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，**无论这些信息是存放在硬盘上还是内存中。（F4）**
b) 测评对象：终端和服务器等设备中的操作系统、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：应核查相关配置信息或系统设计文档，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。

测评单元（L4-CES1-47）

该测评单元包括以下要求：

a) 测评指标：应保证**操作系统、数据库系统和应用系统用户**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，**无论这些信息是存放在硬盘上还是内存中。（F4）**
b) 测评对象：终端和服务器等设备中的操作系统、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：应核查相关配置信息或系统设计文档，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。

8.1.4.11 个人信息保护

测评单元（L4-CES1-48）

该测评单元包括以下要求：

a) 测评指标：**金融机构在收集、使用个人金融信息时，应当遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F4）**

b) 测评对象：隐私政策。

c) 测评实施包括以下内容：

1) 应核查是否具有隐私政策。

2) 应核查隐私政策中是否向个人金融信息主体明示收集、使用信息的目的、方式和范围。

3) 应核查隐私政策是否获得个人信息主体的明示同意。

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。

测评单元（L4-CES1-49）

该测评单元包括以下要求：

a) 测评指标：应仅采集和保存业务必需的用户个人**金融**信息。**（F4）**

b) 测评对象：业务应用系统和数据库管理系统等。

c) 测评实施包括以下内容：

1) 应核查采集和保存的用户个人金融信息是否是业务应用必需的。

2) 应核查是否制定了有关用户个人金融信息保护的管理制度和流程。

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。

测评单元（L4-CES1-50）

该测评单元包括以下要求：

a) 测评指标：**应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限，**应禁止未授权访问和非法使用用户个人**金融**信息。**（F4）**

b) 测评对象：业务应用系统和数据库管理系统等。

c) 测评实施包括以下内容：

1) 应核查是否采用技术措施限制对用户个人金融信息的访问和使用。

2) 应核查是否根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理。

3) 应核查是否制定了有关用户个人金融信息保护的管理制度和流程。

4) 应验证未经授权是否不能访问用户个人金融信息。

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。

测评单元（L4-CES1-51）

该测评单元包括以下要求：

a) 测评指标：**金融机构应依据 JR/T 0171-2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F4）**

b) 测评对象：个人金融信息、个人金融信息全生命周期管理相关规范、个人金融信息生命周期过程进行安全检查与评估的相关文档等。

c) 测评实施包括以下内容：

1) 应访谈是否对个人金融信息生命周期过程进行安全检查与评估。

2) 应核查是否具有个人金融信息生命周期过程进行安全检查与评估的报告。

3) 应核查是否对个人金融信息生命周期过程的安全检查与评估中发现的高风险问题进行补充测试。

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。

测评单元（L4-CES1-52）

该测评单元包括以下要求：

a) 测评指标：**金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F4）**

b) 测评对象：计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等可能展示个人金融信息的界面。

c) 测评实施包括以下内容：

1) 应访谈并核查个人金融信息以何种方式展示，如计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等。

2) 应核查展示个人金融信息的界面是否采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。

d) 单元判定：如果 2）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。

测评单元（L4-CES1-53）

该测评单元包括以下要求：

a) 测评指标：**应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F4）**

b) 测评对象：隐私政策和个人金融信息。

c) 测评实施包括以下内容：

1) 应访谈并核查是否存在个人金融信息共享、转让的情况。

2) 查看用户隐私政策，是否明确告知个人金融信息主体共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力。

3) 应核查隐私政策是否获得个人信息主体的明示同意。

4) 应核查共享、转让的个人金融信息是否经去标识化处理，且数据接收方无法重新识别个人金融信息主体。

d) 单元判定：如果 1）为否定，则不适用本测评单元指标要求，如果 1）～3）均为肯定或 4）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。

测评单元（L4-CES1-54）

该测评单元包括以下要求：

a) 测评指标：**开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F4）**

b) 测评对象：开发环境、测试环境、开发和测评环境中使用的数据。

c) 测评实施包括以下内容：

1) 应核查系统开发环境和测试环境中的数据是否使用虚构的个人金融信息。

2) 如果使用真实的个人金融信息，是否对真实的个人金融信息进行去标识化处理，账号、卡号、协议号、支付指令等测试确需除外。

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，否则不符合本测评单元指标要求。

8.1.5 安全管理中心

8.1.5.1 系统管理

测评单元（L4-SMC1-01）

该测评单元包括以下要求：

a) 测评指标：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。
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否对系统管理员进行身份鉴别。
   2) 应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作。
   3) 应核查是否对系统管理操作进行审计。
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。

测评单元（L4-SMC1-02）

该测评单元包括以下要求：

a) 测评指标：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、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施：应核查是否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、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-SMC1-03）

该测评单元包括以下要求：

a) 测评指标：**应每月对设备的配置文件进行备份，发生变动时应及时备份。（F4）**
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否每月对设备的配置文件进行备份。
   2) 应核查系统发生变动时是否及时备份。
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。

测评单元（L4-SMC1-04）

该测评单元包括以下要求：

a) 测评指标：**应使用自动化监控平台对设备运行状况进行实时监测，运维人员应每天定期查看并记录系统运行状况。（F4）**
b) 测评对象：提供集中系统管理功能的系统和运维人员。
c) 测评实施包括以下内容：
   1) 应核查是否使用自动化监控平台对设备运行状况进行实时监测。
   2) 应核查运维人员是否每天定期查看并记录系统运行状况。
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。

测评单元（L4-SMC1-05）

该测评单元包括以下要求：

a) 测评指标：**应每月检验网络设备软件版本信息，并通过有效测试验证进行相应的升级，同时留存测试验证相关记录。（F4）**
b) 测评对象：提供集中系统管理功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否每月检验网络设备软件版本信息，并通过有效测试验证进行相应的升级。
   2) 应核查是否具有网络设备软件版本升级测试验证相关记录。

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

8.1.5.2 审计管理

测评单元（L4-SMC1-06）

该测评单元包括以下要求：

a) 测评指标：应对审计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审计操作，并对这些操作进行审计。
b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否对审计管理员进行身份鉴别。
   2) 应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作。
   3) 应核查是否对安全审计操作进行审计。
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。

测评单元（L4-SMC1-07）

该测评单元包括以下要求：

a) 测评指标：应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c) 测评实施：应核查是否通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-SMC1-08）

该测评单元包括以下要求：

a) 测评指标：**应严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审计用户的权限分离，避免非授权的删除、修改或覆盖。（F4）**
b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问。
   2) 应核查管理用户和审计用户的权限是否分离。
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。

8.1.5.3 安全管理

测评单元（L4-SMC1-09）

该测评单元包括以下要求：

a) 测评指标：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，并对这些操作进行审计。
b) 测评对象：提供集中安全管理功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否对安全管理员进行身份鉴别。
   2) 应核查是否只允许安全管理员通过特定的命令或操作界面进行安全审计操作。
   3) 应核查是否对安全管理操作进行审计。

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。

测评单元（L4-SMC1-10）

该测评单元包括以下要求：

a) 测评指标：应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
b) 测评对象：提供集中安全管理功能的系统。
c) 测评实施：应核查是否通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.5.4 集中管控

测评单元（L4-SMC1-11）

该测评单元包括以下要求：

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。
b) 测评对象：网络拓扑。
c) 测评实施包括以下内容：
   1) 应核查是否划分出单独的网络区域用于部署安全设备或安全组件。
   2) 应核查各个安全设备或安全组件是否集中部署在单独的网络区域内。
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。

测评单元（L4-SMC1-12）

该测评单元包括以下要求：

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。
b) 测评对象：路由器、交换机和防火墙等设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否采用安全方式（如 SSH、HTTPS、IPSec VPN 等）对安全设备或安全组件进行管理。
   2) 应核查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，否则不符合本测评单元指标要求。

测评单元（L4-SMC1-13）

该测评单元包括以下要求：

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。
b) 测评对象：综合网管系统等提供运行状态监测功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、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) 应测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阈值（或默认阈值）实时报警。
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。

测评单元（L4-SMC1-14）

该测评单元包括以下要求：

a) 测评指标：应对分散在各个设备上的**安全事件**、审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。**（F4）**

b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统。
c) 测评实施包括以下内容：
   1) 应核查各个设备是否配置并启用了相关策略，将安全事件、审计数据发送到独立于设备自身的外部集中安全审计系统中。
   2) 应核查是否部署统一的集中安全审计系统，统一收集和存储各设备日志，并根据需要进行集中审计分析。
   3) 应核查审计记录的留存时间是否至少为6个月。
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。

测评单元（L4-SMC1-15）

该测评单元包括以下要求：
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。
b) 测评对象：提供集中安全管控功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否能够对安全策略（如防火墙访问控制策略、入侵保护系统防护策略、WAF安全防护策略等）进行集中管理。
   2) 应核查是否实现对操作系统防恶意代码系统及网络恶意代码防护设备的集中管理，实现对防恶意代码病毒规则库的升级进行集中管理。
   3) 应核查是否实现对各个系统或设备的补丁升级进行集中管理。
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。

测评单元（L4-SMC1-16）

该测评单元包括以下要求：
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、分析**、响应和处置。（F4）**
b) 测评对象：提供集中安全管控功能的系统。
c) 测评实施包括以下内容：
   1) 应核查是否部署了相关系统平台能够对各类安全事件进行分析、响应和处置，并通过声光等方式实时报警。
   2) 应核查监测范围是否能够覆盖网络所有关键路径。
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。

测评单元（L4-SMC1-17）

该测评单元包括以下要求：
a) 测评指标：应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。
b) 测评对象：综合安全审计系统等。
c) 测评实施：应核查是否在系统范围内统一使用了唯一确定的时钟源。
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。

测评单元（L4-SMC1-18）

该测评单元包括以下要求：
a) 测评指标：**应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。（F4）**
b) 测评对象：综合安全审计系统等。
c) 测评实施：应核查是否具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

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。

8.1.6 安全管理制度

8.1.6.1 安全策略

测评单元（L4-PSS1-01）

该测评单元包括以下要求：

a) 测评指标：应制定**全机构范围**网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等，**并编制形成网络安全方针制度文件**。**（F4）**
b) 测评对象：总体方针策略类文档。
c) 测评实施：应核查网络安全工作的总体方针和安全策略文件是否明确全机构安全工作的总体目标、范围、原则和各类安全策略。
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。

8.1.6.2 管理制度

测评单元（L4-PSS1-02）

该测评单元包括以下要求：

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。
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物理、网络、主机系统、数据、应用、建设和运维等管理内容。
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。

测评单元（L4-PSS1-03）

该测评单元包括以下要求：

a) 测评指标：应对管理人员或操作人员执行的日常管理操作建立操作规程。
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。

测评单元（L4-PSS1-04）

该测评单元包括以下要求：

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安全管理制度体系。
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、记录表单是否全面且具有关联性和一致性。
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。

8.1.6.3 制定和发布

测评单元（L4-PSS1-05）

该测评单元包括以下要求：

a) 测评指标：**金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应制定适用辖内的安全管理制度。（F4）**

b) 测评对象：部门/人员职责文件等。
c) 测评实施包括以下内容：
   1) 应核查适用全机构范围的安全管理制度是否在金融机构总部的总体负责下统一制定。
   2) 应核查各分支机构是否制定了适用辖内的安全管理制度。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PSS1-06）

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安全管理制度的制定。
b) 测评对象：部门/人员职责文件等。
c) 测评实施：应核查是否由专门的部门或人员负责制定安全管理制度。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-PSS1-07）

该测评单元包括以下要求：
a) 测评指标：安全管理制度应通过正式、有效的方式发布，并进行版本控制。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容。
   2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.4 评审和修订

测评单元（L4-PSS1-08）

该测评单元包括以下要求：
a) 测评指标：应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期对安全管理制度的合理性和适用性进行审定。
   2) 应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7 安全管理机构

8.1.7.1 岗位设置

测评单元（L4-ORS1-01）

该测评单元包括以下要求：
a) 测评指标：**网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F4）**
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/网络安全主管是否建立了网络安全管理工作实行统一领导、分级管理模式。
2） 应核查相关制度文档是否明确了总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。

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。

测评单元（L4-ORS1-02）

该测评单元包括以下要求：

a） 测评指标：应**设立由本机构领导、业务与技术相关部门主要负责人组成的**网络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担任或授权，**负责协调本机构及辖内网络安全管理工作，决策本机构及辖内网络安全重大事宜。（F4）**
b） 测评对象：信息/网络安全主管、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） 应访谈信息/网络安全主管是否成立了由本机构领导、业务与技术相关部门主要负责人组成的指导和管理网络安全工作的委员会或领导小组。
2） 应核查相关文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责。
3） 应核查委员会或领导小组的最高领导是否由单位主管领导担任或由其进行了授权。
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。

测评单元（L4-ORS1-03）

该测评单元包括以下要求：

a） 测评指标：应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。
b） 测评对象：信息/网络安全主管和管理制度类文档。
c） 测评实施包括以下内容：
1） 应访谈信息/网络安全主管是否设立网络安全管理工作的职能部门。
2） 应核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责。
3） 应核查岗位职责文档是否有岗位划分情况和岗位职责。
d） 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ORS1-04）

该测评单元包括以下要求：

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

测评单元（L4-ORS1-05）

该测评单元包括以下要求：

a） 测评指标：**应设立专门的网络安全审计岗位，负责网络安全审计制度和流程的实施，制订和执行网络安全审计计划，对网络安全整个生命周期和重大事件等进行审计。（F4）**
b） 测评对象：信息/网络安全主管和管理制度类文档。
c） 测评实施包括以下内容：
1） 应访谈信息/网络安全主管是否设立了专门的网络安全审计岗位。

2) 应核查岗位职责文档是否明确了网络安全岗位的职责，包括负责网络安全审计制度和流程的实施，制订和执行网络安全审计计划，对网络安全整个生命周期和重大事件等进行审计。

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。

测评单元（L4-ORS1-06）

该测评单元包括以下要求：

a) 测评指标：**应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。（F4）**

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/网络安全主管是否实现前后台分离、开发与操作分离、技术与业务分离。

2) 应核查岗位职责文档是否明确了信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。

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。

测评单元（L4-ORS1-07）

该测评单元包括以下要求：

a) 测评指标：**除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开展本部门的网络安全管理工作。（F4）**

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，网络安全管理部门外的其他部门是否指定至少一名部门网络安全员。

2) 应核查岗位职责文档是否明确了部门网络安全员需协助网络安全管理部门开展本部门的网络安全管理工作。

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。

8.1.7.2 人员配备

测评单元（L4-ORS1-08）

该测评单元包括以下要求：

a) 测评指标：应配备一定数量的系统管理员、审计管理员和安全管理员等。

b) 测评对象：信息/网络安全主管和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈信息/网络安全主管是否配备了系统管理员、审计管理员和安全管理员。

2) 应核查人员配备文档是否明确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。

测评单元（L4-ORS1-09）

该测评单元包括以下要求：

a) 测评指标：应配备专职安全管理员，不可兼任。

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是否明确配备了专职安全管理员。

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。

测评单元（L4-ORS1-10）

该测评单元包括以下要求：

a) 测评指标：关键事务岗位应配备多人共同管理。
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/网络安全主管是否对关键岗位配备了多人。
   2) 应核查人员配备文档是否针对关键岗位配备多人。
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。

测评单元（L4-ORS1-11）

该测评单元包括以下要求：

a) 测评指标：**应定期对网络安全重要岗位人员进行轮换。（F4）**
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期对网络安全重要岗位人员进行轮换。
   2) 应核查人员配备文档是否具有网络安全重要岗位人员轮换记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7.3 授权和审批

测评单元（L4-ORS1-12）

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。

测评单元（L4-ORS1-13）

该测评单元包括以下要求：

a) 测评指标：应针对**系统投入运行、重要资源（如敏感数据等资源）的访问、**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。**（F4）**
b) 测评对象：操作规程类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查系统投入运行、重要资源（如敏感数据等资源）的访问、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是否明确建立了逐级审批程序。
   2) 应核查审批记录、操作记录是否与相关制度一致。
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。

测评单元（L4-ORS1-14）

该测评单元包括以下要求：

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。
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/网络安全主管是否对各类审批事项进行更新。
2） 应核查是否具有定期审查审批事项的记录。

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

测评单元（L4-ORS1-15）

该测评单元包括以下要求：

a） 测评指标：**用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系，权限变更应执行相关审批流程，并有完整的变更记录。（F4）**
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/网络安全主管是否根据最小权限原则对用户授权，重要岗位的员工之间是否形成相互制约的关系。
2） 应核查是否具有权限变更的相关审批流程和完整的变更记录。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ORS1-16）

该测评单元包括以下要求：

a） 测评指标：**应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。（F4）**
b） 测评对象：信息/网络安全主管和记录表单类文档。
c） 测评实施包括以下内容：
1） 应访谈信息/网络安全主管是否建立系统用户及权限清单并核查相关文档。
2） 应核查是否具有定期对员工权限进行检查核对的记录。
3） 对于在核查核对中发现越权用户、过期用户的，应核查是否及时调整越权用户权限或清理过期用户权限。
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。

8.1.7.4 沟通和合作

测评单元（L4-ORS1-17）

该测评单元包括以下要求：

a） 测评指标：应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。
b） 测评对象：信息/网络安全主管和记录表单类文档。
c） 测评实施包括以下内容：
1） 应访谈信息/网络安全主管是否建立了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制。
2） 应核查会议记录是否明确在各类管理人员、组织内部机构和网络安全管理部门之间开展了合作与沟通。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ORS1-18）

该测评单元包括以下要求：

a） 测评指标：应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
b） 测评对象：信息/网络安全主管和记录表单类文档。
c） 测评实施包括以下内容：

1) 应访谈信息/网络安全主管是否建立了与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制。
2) 应核查会议记录是否明确了与网络安全职能部门、各类供应商、业界专家及安全组织开展了合作与沟通。

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

测评单元（L4-ORS1-19）

该测评单元包括以下要求：

a) 测评指标：应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息。
d) 单元判定：如果以上测评实施内容为肯定，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。

8.1.7.5 审核和检查

测评单元（L4-ORS1-20）

该测评单元包括以下要求：

a) 测评指标：应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期进行了常规安全检查。
   2) 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ORS1-21）

该测评单元包括以下要求：

a) 测评指标：应定期进行全面安全检查，检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。
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否定期进行了全面安全检查。
   2) 应核查全面安全检查记录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。

测评单元（L4-ORS1-22）

该测评单元包括以下要求：

a) 测评指标：**应建立对门户网站内容发布的审核、管理和监控机制。（F4）**
b) 测评对象：信息/网络安全主管和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管是否建立了门户网站内容发布的审核、管理和监控机制。
   2) 应核查是否具有门户网站内容发布的审核记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ORS1-23）

该测评单元包括以下要求：

a) 测评指标：应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对安全检查结果进行通报并报上一级机构科技部门备案。（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录和报上一级机构科技部门备案的记录。

2) 对于安全检查后要求限期整改的，应核查是否具有整改落实情况相关记录文档。

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

测评单元（L4-ORS1-24）

该测评单元包括以下要求：

a) 测评指标：**应制定违反和拒不执行安全管理措施规定的处罚细则。（F4）**

b) 测评对象：管理制度类文档。

c) 测评实施：应核查是否具有违反和拒不执行安全管理措施规定的处罚细则。

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

8.1.8 安全管理人员

8.1.8.1 人员录用

测评单元（L4-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。

测评单元（L4-HRS1-02）

该测评单元包括以下要求：

a) 测评指标：应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）。

2) 应核查是否具有人员录用时对录用人身份、安全背景、专业资格或资质等进行审查的相关文档或记录等，是否记录审查内容和审查结果等。

3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。

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

测评单元（L4-HRS1-03）

该测评单元包括以下要求：

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。

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：
   1) 应核查保密协议是否有保密范围、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。

测评单元（L4-HRS1-04）

该测评单元包括以下要求：
a) 测评指标：应从内部人员中选拔从事关键岗位的人员。
b) 测评对象：人事负责人。
c) 测评实施：应访谈人事负责人从事关键岗位的人员是否是从内部人员选拔担任。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-HRS1-05）

该测评单元包括以下要求：
a) 测评指标：**应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施应包括以下内容：
   1) 应核查是否有网络安全管理人员的备案制度。
   2) 应核查相关备案记录，网络安全管理人员的配备变更情况是否报上一级科技部门备案，金融机构总部网络安全管理人员是否在总部科技部门备案。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-HRS1-06）

该测评单元包括以下要求：
a) 测评指标：**凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不应从事网络安全管理工作。（F4）**
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：应核查网络安全管理人员是否无因违反国家法律法规和金融机构有关规定而受到处罚或处分的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.2 人员离岗

测评单元（L4-HRS1-07）

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。

测评单元（L4-HRS1-08）

该测评单元包括以下要求：

a) 测评指标：应办理严格的调离手续，**关键岗位人员离岗须**承诺调离后的保密义务后方可离开，**并保证离岗人员负责的信息技术系统的口令立即更换。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查人员离岗的管理文档是否规定了人员调离手续和离岗要求等。
   2) 应核查关键岗位人员离岗是否具有按照离岗程序办理调离手续和承诺的保密义务的记录。
   3) 应核查保密承诺文档是否有调离人员的签字。
   4) 应核查离岗人员负责的信息技术系统的口令是否立即更换。
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。

8.1.8.3 人员考核

测评单元（L4-HRS1-09）

该测评单元包括以下要求：
a) 测评指标：**应定期对各个岗位的人员进行安全技能及安全认知的考核。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查人员考核的管理文档是否明确要求定期对各个岗位的人员进行安全技能及安全认知的考核。
   2) 应核查是否具有安全技能及安全认知考核记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-HRS1-10）

该测评单元包括以下要求：
a) 测评指标：**应对关键岗位的人员进行全面、严格的安全审查和技能考核。（F4）**
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：应访谈信息/网络安全主管是否对关键岗位的人员进行全面、严格的安全审查和技能考核，并核查是否具有审查和考核记录。
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。

测评单元（L4-HRS1-11）

该测评单元包括以下要求：
a) 测评指标：**应建立保密制度，并定期或不定期的对保密制度执行情况进行检查或考核。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有保密制度。
   2) 应核查是否具有定期或不定期对保密制度执行情况进行检查或考核的记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-HRS1-12）

该测评单元包括以下要求：
a) 测评指标：**应对考核结果进行记录并保存。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查考核记录，考核人员是否包括各个岗位的人员，考核内容是否包括安全知识、安全技能、安全认知等，记录日期与考核周期是否一致。

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。

8.1.8.4 安全意识教育和培训

测评单元（L4-HRS1-13）

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。

测评单元（L4-HRS1-14）

该测评单元包括以下要求：

a) 测评指标：应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查安全教育和培训计划文档是否具有不同岗位的培训计划。
   2) 应核查培训内容是否包含安全基础知识、岗位操作规程等。
   3) 应核查安全教育和培训记录是否有培训人员、培训内容、培训结果等描述。
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。

测评单元（L4-HRS1-15）

该测评单元包括以下要求：

a) 测评指标：**每年应至少对网络安全管理人员进行一次网络安全培训。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有对网络安全管理人员进行年度网络安全培训的记录。
d) 单元判定：如果以上测评实施为肯定，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。

测评单元（L4-HRS1-16）

该测评单元包括以下要求：

a) 测评指标：应定期对不同岗位的人员进行技术技能考核。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有针对各岗位人员的技能考核记录。
d) 单元判定：如果以上测评实施为肯定，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。

测评单元（L4-HRS1-17）

该测评单元包括以下要求：

a) 测评指标：**应对安全教育和培训的情况和结果进行记录并归档保存。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有针安全教育和培训的情况和结果的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.5 外部人员访问管理

测评单元（L4-HRS1-18）

该测评单元包括以下要求：

a) 测评指标：应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等。
   2) 应核查外部人员访问重要区域的申请文档是否具有批准人允许访问的批准等。
   3) 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-HRS1-19）

该测评单元包括以下要求：

a) 测评指标：应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程。
   2) 应核查外部人员访问系统的申请文档是否明确外部人员的访问权限，是否具有允许访问的批准等。
   3) 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-HRS1-20）

该测评单元包括以下要求：

a) 测评指标：**应对允许被外部人员访问的金融机构计算机系统和网络资源，建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控。（F4）**
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) 应核查对允许被外部人员访问的金融机构计算机系统和网络资源，是否建立存取控制机制、认证机制。
   2) 应核查外部人员权限表单是否包括所有外部人员及其权限。
   3) 应核查外部人员访问活动是否受到监控。
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。

测评单元（L4-HRS1-21）

该测评单元包括以下要求：

a) 测评指标：外部人员离场后应及时清除其所有的访问权限。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限。
   2) 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。

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

测评单元（L4-HRS1-22）

该测评单元包括以下要求：

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，不得进行非授权的**增加、删除、修改、查询数据等**操作，不得复制和泄露**金融机构的任何信息。（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查是否与获得系统访问授权的外部人员签署了保密协议。

2) 应核查保密协议中是否有禁止进行未授权的增加、删除、修改、查询数据操作，禁止复制和泄露金融机构的任何信息等相关要求。

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

测评单元（L4-HRS1-23）

该测评单元包括以下要求：

a) 测评指标：对关键区域或关键系统不允许外部人员访问。

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。

8.1.9 安全建设管理

8.1.9.1 定级和备案

测评单元（L4-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。

测评单元（L4-CMS1-02）

该测评单元包括以下要求：

a) 测评指标：应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见。

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

测评单元（L4-CMS1-03）

该测评单元包括以下要求：

a) 测评指标：应保证定级结果经过相关部门的批准。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见。

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

测评单元（L4-CMS1-04）

该测评单元包括以下要求：

a) 测评指标：应将备案材料报主管部门和相应公安机关备案。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有公安机关出具的备案证明文档。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.9.2 安全方案设计

测评单元（L4-CMS1-05）

该测评单元包括以下要求：

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

测评单元（L4-CMS1-06）

该测评单元包括以下要求：

a) 测评指标：应根据保护对象的安全保护等级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，设计内容应包含密码技术相关内容，并形成配套文件。
b) 测评对象：安全规划设计类文档。
c) 测评实施：应核查是否有总体规划和安全设计方案等配套文件，设计方案中应包括密码技术相关内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-07）

该测评单元包括以下要求：

a) 测评指标：应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体安全规划、安全设计方案等相关配套文件的批准意见和论证意见。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-08）

该测评单元包括以下要求：

a) 测评指标：**使用上一级机构信息系统资源或对其他机构信息系统资源与配置造成影响的区域性建设项目，项目建设方案应分别通过上一级机构业务与科技部门的审核、批准。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查使用上一级机构信息系统资源或对其他机构信息系统资源与配置造成影响的区域性建设项目的项目建设方案是否通过上一级机构业务与科技部门的审核、批准。
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。

8.1.9.3 产品采购和使用

测评单元（L4-CMS1-09）

该测评单元包括以下要求：

a) 测评指标：应确保网络安全产品采购和使用符合国家的有关规定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查有关网络安全产品是否符合国家的有关规定，如网络安全产品获得了销售许可等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-10）

该测评单元包括以下要求：

a) 测评指标：应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈建设负责人是否采用了密码产品及其相关服务。
   2) 应核查密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CMS1-11）

该测评单元包括以下要求：

a) 测评指标：**各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有扫描、检查类网络安全产品购置前本机构科技主管部门的批准、备案记录。
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。

测评单元（L4-CMS1-12）

该测评单元包括以下要求：

a) 测评指标：应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-13）

该测评单元包括以下要求：

a) 测评指标：应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有重要产品专项测试记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-14）

该测评单元包括以下要求：

a) 测评指标：**扫描、检测类网络安全产品应仅限于本机构网络安全管理人员使用。（F4）**
b) 测评对象：记录表单类文档。

c) 测评实施：应核查网络安全产品使用记录，是否仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。
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。

测评单元（L4-CMS1-15）

该测评单元包括以下要求：
a) 测评指标：**应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取整改措施并按规定程序报告。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有定期对各类网络安全产品相关日志和报表信息进行汇总分析的记录或分析报告。
   2) 应核查一旦发现重大问题，是否具有相应的控制措施和报告程序。
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。

测评单元（L4-CMS1-16）

该测评单元包括以下要求：
a) 测评指标：**应定期对各类网络安全产品产生的日志和报表进行备份存档，至少保存 6 个月。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有对各类网络安全产品日志和报表进行定期备份存档的记录。
   2) 应核查备份存档记录是否至少保存 6 个月。
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。

测评单元（L4-CMS1-17）

该测评单元包括以下要求：
a) 测评指标：**应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。（F4）**
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) 应核查网络安全产品维护和报废相关管理制度中是否有及时升级维护规定以及报废审批流程。
   2) 应核查是否具有网络安全产品升级维护记录。
   3) 应核查对于超过使用期限或不能继续使用的网络安全产品是否具有报废、审批记录。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CMS1-18）

该测评单元包括以下要求：
a) 测评指标：**应在本地配置网络安全产品。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否在本地配置网络安全产品。
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。

8.1.9.4 自行软件开发

测评单元（L4-CMS1-19）

该测评单元包括以下要求：

a) 测评指标：应将开发环境与实际运行环境物理分开，**应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员**，测试数据和测试结果受到控制。**（F4）**

b) 测评对象：建设负责人。

c) 测评实施包括以下内容：

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

2) 应核查测试数据和测试结果是否受控使用。

3) 应访谈开发人员和测试人员是否分离，开发人员是否不能兼任系统管理员或业务操作人员。

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。

测评单元（L4-CMS1-20）

该测评单元包括以下要求：

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

b) 测评对象：管理制度类文档。

c) 测评实施：应核查软件开发管理制度是否明确软件设计、开发、测试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。

测评单元（L4-CMS1-21）

该测评单元包括以下要求：

a) 测评指标：应制定代码编写安全规范，要求开发人员参照规范编写代码。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查代码编写安全规范是否明确代码安全编写规则。

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

测评单元（L4-CMS1-22）

该测评单元包括以下要求：

a) 测评指标：应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

b) 测评对象：建设负责人。

c) 测评实施：应访谈建设负责人开发人员是否为专职，是否对开发人员活动进行控制等。

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

测评单元（L4-CMS1-23）

该测评单元包括以下要求：

a) 测评指标：应具备软件设计的相关文档和使用指南，并对文档使用进行控制。

b) 测评对象：管理制度类文档。

c) 测评实施：应核查是否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。

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。

测评单元（L4-CMS1-24）

该测评单元包括以下要求：

a) 测评指标：应在软件开发过程中对**代码规范、代码质量、代码安全性进行审查，**在软件安装前对可能存在的恶意代码进行检测。**（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-25）

该测评单元包括以下要求：
a) 测评指标：应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查对程序资源库的修改、更新、发布进行授权和审批的文档或记录是否有批准人的签字。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-26）

该测评单元包括以下要求：
a) 测评指标：**在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查在软件开发过程中是否同步完成相关文档手册的编写工作。
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。

8.1.9.5 外包软件开发

测评单元（L4-CMS1-27）

该测评单元包括以下要求：
a) 测评指标：应在软件交付前检测其中可能存在的恶意代码。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有交付前的恶意代码检测报告。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-28）

该测评单元包括以下要求：
a) 测评指标：应保证开发单位提供软件设计文档和使用指南。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-29）

该测评单元包括以下要求：
a) 测评指标：应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
b) 测评对象：建设负责人和记录表单类文档。
c) 测评实施包括以下内容：

1） 应访谈建设负责人委托开发单位是否提供软件源代码。
2） 应核查软件测试报告是否审查了软件可能存在的后门和隐蔽信道。

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

测评单元（L4-CMS1-30）

该测评单元包括以下要求：

a） 测评指标：**应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F4）**
b） 测评对象：建设负责人和记录表单类文档。
c） 测评实施包括以下内容：
1） 应访谈建设负责人是否要求外包服务商保留操作痕迹、记录完整的日志。
2） 应核查相关内容和保存期限是否满足事件分析、安全取证、独立审计和监督检查需要。
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。

测评单元（L4-CMS1-31）

该测评单元包括以下要求：

a） 测评指标：**应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F4）**
b） 测评对象：外包合同商务类文档。
c） 测评实施：应核查外包合同等商务文件是否具有控制外包服务商分包的条款。
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。

测评单元（L4-CMS1-32）

该测评单元包括以下要求：

a） 测评指标：**应要求外包服务商每年至少开展一次网络安全风险评估并提交评估报告，应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。（F4）**
b） 测评对象：建设负责人和记录表单类文档。
c） 测评实施包括以下内容：
1） 应访谈建设负责人是否要求外包服务商每年至少开展一次网络安全风险评估，并核查是否具有外包服务商提交的风险评估报告。
2） 应访谈建设负责人是否要求外包服务商聘请外部机构定期对其进行安全审计，并核查是否具有外包服务商提交的安全审计报告。
3） 应核查外包服务商是否及时整改风险评估和安全审计发现的问题。
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。

8.1.9.6 工程实施

测评单元（L4-CMS1-33）

该测评单元包括以下要求：

a） 测评指标：应指定或授权专门的部门或人员负责工程实施过程的管理。
b） 测评对象：记录表单类文档。
c） 测评实施：应核查是否指定专门部门或人员对工程实施进行进度和质量控制。
d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-34）

该测评单元包括以下要求：

a) 测评指标：应制定安全工程实施方案控制工程实施过程。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查安全工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-35）

该测评单元包括以下要求：
a) 测评指标：**针对涉及到新旧数据系统切换的工程实施，应选择对客户影响较小的时间段进行。系统切换时间超过一个工作日，需至少提前5个工作日发布提示公告，并提供应急服务途径。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查新旧数据系统切换的工程实施，是否选择对客户影响较小的时间段进行。
   2) 应核查系统切换时间超过一个工作日时，是否至少提前5个工作日发布提示公告，并提供应急服务途径。
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，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-36）

该测评单元包括以下要求：
a) 测评指标：应通过第三方工程监理控制项目的实施过程。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查工程监理报告是否明确了工程进展、时间计划、控制措施等方面内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-37）

该测评单元包括以下要求：
a) 测评指标：**应制定灾难备份系统集成与测试计划并组织实施，通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。（F4）**
b) 测评对象：灾难备份系统和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否制定灾难备份系统集成与测试计划并组织实施。
   2) 应核查灾难备份系统技术和业务测试记录，灾难备份系统的功能与性能是否达到设计指标要求。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CMS1-38）

该测评单元包括以下要求：
a) 测评指标：**系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有系统建设、升级、扩充等工程的规划、论证和审核材料并妥善保存。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.9.7 测试验收

测评单元（L4-CMS1-39）

该测评单元包括以下要求：

a) 测评指标：**应根据设计方案或合同要求等**制订测试验收方案，并依据测试验收方案实施测试验收，**应详细记录测试验收结果，**形成测试验收报告。**（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

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

2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。

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

测评单元（L4-CMS1-40）

该测评单元包括以下要求：

a) 测评指标：应**由项目承担单位（部门）或公正的第三方制定安全测试方案，**进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容，**并将测试报告报科技部门审查。（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查是否具有上线前的安全测试方案和安全测试报告，安全测试报告是否包含密码应用安全性测试相关内容。

2) 应核查安全测试报告是否报科技部门审查。

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

测评单元（L4-CMS1-41）

该测评单元包括以下要求：

a) 测评指标：**新建应用系统投入生产运行前，原则上应进行不少于 1 个月的模拟运行和不少于 3 个月的试运行。（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施：应核查新建应用系统投入生产运行前是否进行不少于 1 个月的模拟运行和不少于 3 个月的试运行。

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。

测评单元（L4-CMS1-42）

该测评单元包括以下要求：

a) 测评指标：**对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方案、数据备份与系统恢复措施、应急处置措施后，经系统用户和主管领导审批同意后，才能开展测试工作，以确保生产系统的安全。（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 针对在生产系统上进行测试的情况，应核查是否事先进行了风险分析和告知。

2) 针对在生产系统上进行测试的情况，应核查是否具有详细的系统测试方案、数据备份与系统恢复措施、应急处置措施。

3) 针对在生产系统上进行测试的情况，应核查是否具有系统用户和主管领导的审批记录。

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

8.1.9.8 系统交付

测评单元（L4-CMS1-43）

该测评单元包括以下要求：

a) 测评指标：应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查交付清单是否说明系统交付的各类设备、软件、文档等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-44）

该测评单元包括以下要求：

a) 测评指标：应对负责运行维护的技术人员进行相应的技能培训。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查系统交付技术培训记录是否包括培训内容、培训时间和参与人员等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-45）

该测评单元包括以下要求：

a) 测评指标：**建设单位应在完成建设任务后将建设过程文档和运维文档全部移交科技部门。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查交付文档是否包括建设过程文档和运行维护文档等，建设过程文档和运维文档是否全部移交科技部门。
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。

测评单元（L4-CMS1-46）

该测评单元包括以下要求：

a) 测评指标：**外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将采用的关键安全技术措施和核心安全功能设计对外公开。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查金融机构与外部建设单位之间是否签署知识产权保护协议和保密协议，并核查协议中是否具有禁止将系统关键安全技术措施和核心安全功能对外公开的相关条款。
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。

8.1.9.9 等级测评

测评单元（L4-CMS1-47）

该测评单元包括以下要求：

a) 测评指标：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人本次测评是否为首次，若非首次，是否根据以往测评结果进行相应的安全整改。
   2) 应核查是否具有以往等级测评报告和安全整改方案。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CMS1-48）

该测评单元包括以下要求：

a) 测评指标：应在发生重大变更或级别发生变化时进行等级测评。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否有过重大变更或级别发生过变化及是否进行相应的等级测评。
   2) 应核查是否具有相应情况下的等级测评报告。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CMS1-49）

该测评单元包括以下要求：

a) 测评指标：**应选择公安部认可的全国等级保护测评机构推荐目录中的测评单位进行等级测评，并与测评单位签订安全保密协议。（F4）**
b) 测评对象：等级测评报告和相关资质文件。
c) 测评实施包括以下内容：
   1) 应核查以往等级测评的测评单位是否具有等级测评机构资质。
   2) 应核查是否具有与测评单位签订的安全保密协议。
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。

8.1.9.10 服务供应商管理

测评单元（L4-CMS1-50）

该测评单元包括以下要求：

a) 测评指标：**应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。（F4）**
b) 测评对象：建设负责人。
c) 测评实施：应访谈建设负责人是否评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。
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。

测评单元（L4-CMS1-51）

该测评单元包括以下要求：

a) 测评指标：应确保服务供应商的选择符合国家的有关规定。
b) 测评对象：建设负责人。
c) 测评实施：应访谈建设负责人选择的安全服务商是否符合国家有关规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-52）

该测评单元包括以下要求：

a) 测评指标：应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查与服务供应商签订的服务合同或安全责任书是否明确了后期的技术支持和服务承诺等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS1-53）

该测评单元包括以下要求：

a) 测评指标：应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有服务供应商定期提交的安全服务报告。
   2) 应核查是否定期审核评价服务供应商所提供的服务及服务内容变更情况，是否具有服务审核报告。
   3) 应核查是否具有服务供应商评价审核管理制度，明确针对服务供应商的评价指标、考核内容等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.10 安全运维管理

8.1.10.1 环境管理

测评单元（L4-MMS1-01）

该测评单元包括以下要求：

a) 测评指标：**机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F4）**
b) 测评对象：机房。
c) 测评实施：应核查机房布线是否做到跳线整齐，跳线与配线架是否统一编号，标记是否清晰。
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。

测评单元（L4-MMS1-02）

该测评单元包括以下要求：

a) 测评指标：应指定专门的部门或人员负责机房安全，对机房出入进行管理，**每天巡查机房运行状况，**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，**填写机房值班记录、巡视记录。（F4）**
b) 测评对象：物理安全负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理，对基础设施（如空调、供配电设备、灭火设备等）进行定期维护。
   2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员。
   3) 应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息。
   4) 应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
   5) 应核查是否具有机房值班记录、巡视记录。
d) 单元判定：如果 1）～5）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。

测评单元（L4-MMS1-03）

该测评单元包括以下要求：

a) 测评指标：应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查机房安全管理制度是否覆盖物理访问、物品进出和环境安全等方面内容。
   2) 应核查物理访问、物品进出和环境安全等相关记录是否与制度相符。

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

测评单元（L4-MMS1-04）

该测评单元包括以下要求：

a) 测评指标：**进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F4）**

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查机房管理制度是否要求进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。

2) 应核查是否具有进出机房人员审批记录。

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

测评单元（L4-MMS1-05）

该测评单元包括以下要求：

a) 测评指标：**机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F4）**

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查人员管理或培训相关制度是否要求机房管理员经过相关培训后才能上岗。

2) 应核查是否具有机房管理员培训记录。

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

测评单元（L4-MMS1-06）

该测评单元包括以下要求：

a) 测评指标：**应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施：应核查机房设施维修保养记录是否记录机房设施定期维护保养的情况。

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。

测评单元（L4-MMS1-07）

该测评单元包括以下要求：

a) 测评指标：**机房所在区域应安装 24 小时视频监控录像装置，重要机房区域实行 24 小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于 3 个月，销毁录像等资料应经单位主管领导批准后实施。（F4）**

b) 测评对象：机房和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查机房所在区域是否安装 24 小时视频监控录像装置。

2) 应核查重要机房区域是否实行 24 小时警卫值班，是否设置一个主出入口和一个或多个备用出入口。

3) 应核查出入口控制、入侵报警和电视监控设备运行资料是否妥善保管，保存期限是否不少于 3 个月。

4) 应核查销毁录像等资料时是否有单位主管领导审批记录。

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。

测评单元（L4-MMS1-08）

该测评单元包括以下要求：

a) 测评指标：**应设置弱电井，并留有足够的可扩展空间。（F4）**

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应核查机房是否设置弱电井。

2) 应核查弱电井是否留有足够的可扩展空间。

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

测评单元（L4-MMS1-09）

该测评单元包括以下要求：

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

b) 测评对象：管理制度类文档和办公环境。

c) 测评实施包括以下内容：

1) 应核查机房安全管理制度是否明确来访人员的接待区域。

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

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

测评单元（L4-MMS1-10）

该测评单元包括以下要求：

a) 测评指标：应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等。

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查出入人员授权审批记录是否明确对人员进行不同的授权。

2) 应核查重要区域是否安装监控系统，实时监控进入人员活动。

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

8.1.10.2 资产管理

测评单元（L4-MMS1-11）

该测评单元包括以下要求：

a) 测评指标：应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

b) 测评对象：记录表单类文档。

c) 测评实施：应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容。

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

测评单元（L4-MMS1-12）

该测评单元包括以下要求：

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

b) 测评对象：资产管理员、管理制度类文档和设备。

c) 测评实施包括以下内容：

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

2) 应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求。

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

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

测评单元（L4-MMS1-13）

该测评单元包括以下要求：

a) 测评指标：应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：
   1) 应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）。
   2) 应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等要求。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.10.3 介质管理

测评单元（L4-MMS1-14）

该测评单元包括以下要求：

a) 测评指标：应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点。
b) 测评对象：资产管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理。
   2) 应核查介质管理记录是否记录介质归档、使用和定期盘点等情况。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-15）

该测评单元包括以下要求：

a) 测评指标：**所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F4）**
b) 测评对象：资产管理员。
c) 测评实施：应访谈资产管理员并核查存放数据备份介质的环境是否防磁、防潮、防尘、防高温、防挤压。
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。

测评单元（L4-MMS1-16）

该测评单元包括以下要求：

a) 测评指标：应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，**应选择安全可靠的传递、交接方式，做好防信息泄漏控制措施**，并对介质的归档和查询等进行登记记录。**（F4）**
b) 测评对象：资产管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈资产管理员介质在物理传输过程中的人员选择、打包、交付等情况是否进行控制。
   2) 应核查是否对介质的归档和查询等进行登记记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-17）

该测评单元包括以下要求：

a) 测评指标：**对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F4）**
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) 应核查纸质文档是否实行借阅登记制度，是否未经相关部门领导批准，任何人不得将文档转借、复制或对外公开。
   2) 应核查电子文档是否采用电子化办公审批平台进行管理。
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。

测评单元（L4-MMS1-18）

该测评单元包括以下要求：
a) 测评指标：**对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F4）**
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) 应核查载有敏感信息存储介质的销毁制度，是否对介质的销毁严格管理。
   2) 应核查是否具有销毁介质的备案、销毁记录等。
   3) 应核查对于存储介质未在金融机构内部使用的情况，是否对存储介质进行信息的不可恢复性销毁。
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。

测评单元（L4-MMS1-19）

该测评单元包括以下要求：
a) 测评指标：**应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有移动存储介质使用规范。
   2) 应核查是否具有移动存储介质的使用记录等。
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。

测评单元（L4-MMS1-20）

该测评单元包括以下要求：
a) 测评指标：**应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安全区域。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查重要数据是否多重备份。
   2) 应核查是否至少1份备份介质存放于科技部门指定的同城或异地安全区域。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-21）

该测评单元包括以下要求：
a) 测评指标：**应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。（F4）**

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) 应核查技术文档管理制度是否规定了对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理。
   2) 应核查技术文档处理记录是否与管理制度要求一致。
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。

测评单元（L4-MMS1-22）

该测评单元包括以下要求：
a) 测评指标：**应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有定期对主要备份业务数据进行恢复验证的记录。
   2) 应核查是否根据介质使用期限及时转储数据。
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。

8.1.10.4 设备维护管理

测评单元（L4-MMS1-23）

该测评单元包括以下要求：
a) 测评指标：应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。
b) 测评对象：设备管理员和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护。
   2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-24）

该测评单元包括以下要求：
a) 测评指标：应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容。
   2) 应核查是否具有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-25）

该测评单元包括以下要求：
a) 测评指标：**设备确需送外单位维修时，应彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前应请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：

1) 应核查设备维护管理制度是否要求设备送外单位维修应彻底清除所存的工作相关信息并拆除与密码有关的硬件。
2) 应核查是否与设备维修厂商签订保密协议。
3) 应核查密码设备配套使用的设备送修前是否请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息。

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。

测评单元（L4-MMS1-26）

该测评单元包括以下要求：

a) 测评指标：**应制定规范化的故障处理流程，建立详细的故障日志（包括故障发生的时间、范围、现象、处理结果和处理人员等内容）。（F4）**
b) 测评对象：设备管理员和管理制度类文档。
c) 测评实施包括以下内容：
1) 应核查设备故障处理制度是否包含规范化的故障处理流程。
2) 应核查故障日志是否包括故障发生的时间、范围、现象、处理结果和处理人员等内容。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-27）

该测评单元包括以下要求：

a) 测评指标：**新购置的设备应经过验收，验收合格后方能投入使用。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
1) 应核查设备维护管理制度是否明确新购置的设备应经过验收，验收合格后方能投入使用。
2) 应核查新购置设备的验收报告和使用记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-28）

该测评单元包括以下要求：

a) 测评指标：**应制定设备管理规范，根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护责任。（F4）**
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施包括以下内容：
1) 应核查设备管理制度是否落实设备使用者的安全保护责任。
2) 应核查是否根据设备使用年限，及时进行更换升级，并核查是否具有相关记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-29）

该测评单元包括以下要求：

a) 测评指标：信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。
b) 测评对象：设备管理员和记录表单类文档。
c) 测评实施包括以下内容：
1) 应访谈设备管理员含有重要数据的设备带出工作环境是否有加密措施。
2) 应访谈设备管理员对带离机房的设备是否经过审批。
3) 应核查是否具有设备带离机房或办公地点的审批记录。

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

测评单元（L4-MMS1-30）

该测评单元包括以下要求：

a) 测评指标：**需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复性销毁处理，同时备案；信息消除处理仅限于废止设备仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F4）**

b) 测评对象：管理制度类文档和记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查设备维护管理制度是否要求废止的设备应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等。

2) 应核查是否具有废止设备销毁记录。

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

8.1.10.5 漏洞和风险管理

测评单元（L4-MMS1-31）

该测评单元包括以下要求：

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

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

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

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

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

测评单元（L4-MMS1-32）

该测评单元包括以下要求：

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

b) 测评对象：安全管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈安全管理员是否定期开展安全测评。

2) 应核查是否具有安全测评报告。

3) 应核查是否具有安全整改应对措施文档。

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

8.1.10.6 网络和系统安全管理

测评单元（L4-MMS1-33）

该测评单元包括以下要求：

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

b) 测评对象：记录表单类文档。

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

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

测评单元（L4-MMS1-34）

该测评单元包括以下要求：

a) 测评指标：应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理。
   2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-35）

该测评单元包括以下要求：

a) 测评指标：应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略、账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与打补丁、审计日志管理、登录设备和系统的口令更新周期等方面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-36）

该测评单元包括以下要求：

a) 测评指标：应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
b) 测评对象：操作规程类文档。
c) 测评实施：应核查重要设备或系统（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、参数配置等内容。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-37）

该测评单元包括以下要求：

a) 测评指标：应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容，**重要运维操作要求至少两人在场，保留记录，并由操作和复核人员进行确认，维护记录和确认记录应至少妥善保存 6 个月。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。
   应核查重要运维操作是否要求至少两人在场，保留记录。
   应核查重要运维操作的记录是否具有操作和复核人员的确认信息。
   应核查维护记录是否至少保存 6 个月。
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。

测评单元（L4-MMS1-38）

该测评单元包括以下要求：

测评指标：应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。
测评对象：系统管理员和记录表单类文档。

测评实施包括以下内容：

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

应核查是否具有对日志、监测和报警数据等进行分析统计的报告。

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。

测评单元（L4-MMS1-39）

该测评单元包括以下要求：

测评指标：**金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F4）**

测评对象：系统管理员和记录表单类文档。

测评实施包括以下内容：

1） 应访谈系统管理员网间互联安全是否实行统一规范、分级管理、各负其责的安全管理模式。

2） 应核查与外部机构实施网间互联时是否具有审批记录。

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。

测评单元（L4-MMS1-40）

该测评单元包括以下要求：

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

b） 测评对象：系统管理员和记录表单类文档。

c） 测评实施包括以下内容：

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

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

3） 应核查是否具有针对变更运维的操作过程记录。

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

测评单元（L4-MMS1-41）

该测评单元包括以下要求：

a） 测评指标：应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

b） 测评对象：系统管理员和记录表单类文档。

c） 测评实施包括以下内容：

1） 应访谈系统相关人员使用运维工具结束后是否删除工具中的敏感数据。

2） 应核查是否具有运维工具接入系统的审批记录。

3） 应核查运维工具的审计日志记录，审计日志是否不可以更改。

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

测评单元（L4-MMS1-42）

该测评单元包括以下要求：

a） 测评指标：**应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，经过审批后才可开通，操作过程中应保留不可篡改的审计日志，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。（F4）**

b） 测评对象：系统管理员、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) 应访谈系统管理员是否制定远程访问控制规范。
2) 应核查远程访问控制规范是否明确要求严禁跨境远程连接，严格控制国内远程访问范围。
3) 确因工作需要进行远程访问的，应核查是否具有审批记录。
4) 应核查远程访问操作过程中是否保留不可篡改的审计日志。
5) 应核查是否针对远程访问采取了单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。

d) 单元判定：如果1）～5）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。

测评单元（L4-MMS1-43）

该测评单元包括以下要求：

a) 测评指标：**各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F4）**
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) 应核查网络安全管理制度是否明确规定未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。
2) 应核查多媒体使用批准记录是否与管理制度要求一致。
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。

测评单元（L4-MMS1-44）

该测评单元包括以下要求：

a) 测评指标：**网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不应对外公开，未经科技主管部门授权，任何外部机构与人员不应检测或扫描机构内部网络。（F4）**
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) 应核查网络安全管理制度是否明确规定网络安全管理人员经本部门主管领导批准后，才能对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息未经授权不得对外公开。
2) 应核查安全检测、扫描等批准记录是否与管理制度要求一致。
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。

测评单元（L4-MMS1-45）

该测评单元包括以下要求：

a) 测评指标：**所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。（F4）**
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施：应访谈系统管理员是否定期对所有网间互联应用系统和外联网络区进行威胁评估和脆弱性评估，并核查是否具有威胁和脆弱性评估报告。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-46）

该测评单元包括以下要求：

a) 测评指标：**网络系统应采取定时巡检、定期检修和阶段性评估的措施，业务高峰时段和业务高峰日要加强巡检频度和力度，确保硬件可靠、运转正常。（F4）**

b) 测评对象：网络管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈网络管理员，网络系统是否采取定时巡检、定期检修和阶段性评估的措施。
   2) 应核查业务高峰时段和业务高峰日是否加强巡检频度和力度。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-47）

该测评单元包括以下要求：
a) 测评指标：**系统管理员不应兼任业务操作人员，系统管理员不应对业务数据进行任何增加、删除、修改等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门审批，并详细记录维护内容、人员、时间等信息。（F4）**
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) 应核查系统管理员是否未兼任业务操作人员。
   2) 应核查网络安全管理制度是否明确规定系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对系统数据库进行技术维护性操作的，应征得业务部门审批，并详细记录维护过程。
   3) 应核查业务数据维护操作的审批记录是否与管理制度要求一致。
   4) 应核查业务数据维护操作记录是否包含维护内容、人员、时间等信息。
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。

测评单元（L4-MMS1-48）

该测评单元包括以下要求：
a) 测评指标：**每季度应至少进行一次漏洞扫描，对发现的网络安全漏洞及时进行修补，扫描结果应及时上报。（F4）**
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) 应核查网络安全管理规定是否明确要求每季度进行至少一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果及时上报。
   2) 应核查系统漏洞扫描、修补记录是否与管理制度要求一致。
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。

测评单元（L4-MMS1-49）

该测评单元包括以下要求：
a) 测评指标：应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统相关人员日常运维过程中是否存在远程运维，若存在，远程运维结束后是否立即关闭了接口或通道。
   2) 应核查是否具有开通远程运维的审批记录。
   3) 应核查针对远程运维的审计日志是否不可以更改。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-50）

该测评单元包括以下要求：

a) 测评指标：应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
b) 测评对象：安全管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈系统相关人员网络外联连接（如互联网、合作伙伴企业网、上级部门网络等）是否都得到授权与批准。
   2) 应访谈安全管理员是否定期核查违规联网行为。
   3) 应核查是否具有外联授权的记录文件。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-51）

该测评单元包括以下要求：
a) 测评指标：**网络和系统管理员应对网络和系统变更进行详细的记录。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查网络和系统管理员是否对网络和系统变更进行详细的记录。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.10.7 恶意代码防范管理

测评单元（L4-MMS1-52）

该测评单元包括以下要求：
a) 测评指标：应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。
b) 测评对象：运维负责人和管理制度类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识。
   2) 应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系统前进行恶意代码检查。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-53）

该测评单元包括以下要求：
a) 测评指标：**客户端应统一安装病毒防治软件，设置用户口令和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。（F4）**
b) 测评对象：安全管理员和客户端。
c) 测评实施包括以下内容：
   1) 应访谈安全管理员客户端是否统一安装了病毒防治软件，设置了用户口令和屏幕保护口令等安全防护措施，及时更新病毒特征码，以及安装了必要的补丁程序等。
   2) 应核查客户端病毒防治软件安装、用户口令设置、屏幕保护口令设置、病毒特征码更新以及补丁程序安装情况等是否与访谈结果一致。
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。

测评单元（L4-MMS1-54）

该测评单元包括以下要求：
a) 测评指标：应定期验证防范恶意代码攻击的技术措施的有效性。
b) 测评对象：安全管理员和记录表单类文档。

c) 测评实施包括以下内容：
   1) 若采用可信验证技术，应访谈安全管理员是否未发生过恶意代码攻击事件。
   2) 若采用防恶意代码产品，应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否未出现过大规模的病毒事件。
   3) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。
d) 单元判定：如果 1）或 2）和 3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.10.8 配置管理

测评单元（L4-MMS1-55）

该测评单元包括以下要求：
a) 测评指标：应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
b) 测评对象：系统管理员。
c) 测评实施：应访谈系统管理员是否对基本配置信息进行记录和保存。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-56）

该测评单元包括以下要求：
a) 测评指标：应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
b) 测评对象：系统管理员和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库。
   2) 应核查配置信息的变更流程是否具有相应的申报审批程序。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.10.9 密码管理

测评单元（L4-MMS1-57）

该测评单元包括以下要求：
a) 测评指标：应遵循密码相关的国家标准和行业标准。
b) 测评对象：安全管理员。
c) 测评实施：应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-58）

该测评单元包括以下要求：
a) 测评指标：**选用的密码产品和加密算法应符合国家相关密码管理政策规定，应优先使用国产密码算法。（F4）**
b) 测评对象：安全管理员。
c) 测评实施：应访谈安全管理员选用的密码产品和加密算法是否符合国家相关密码管理政策规定，是否优先使用国产密码算法。
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。

测评单元（L4-MMS1-59）

该测评单元包括以下要求：

a) 测评指标：应使用国家密码管理主管部门认证核准的密码技术和产品。
b) 测评对象：安全管理员。
c) 测评实施：应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。
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。

测评单元（L4-MMS1-60）

该测评单元包括以下要求：

a) 测评指标：应采用硬件密码模块实现密码运算和密钥管理。
b) 测评对象：安全管理员。
c) 测评实施：应核查相关产品是否采用密码技术实现硬件密码运算和密钥管理。
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。

测评单元（L4-MMS1-61）

该测评单元包括以下要求：

a) 测评指标：**应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。（F4）**
b) 测评对象：管理制度类文档和密钥管理人员。
c) 测评实施包括以下内容：
   1) 应核查密钥管理制度是否明确了密钥的产生、分发和接收、使用、存储、更新、销毁等方面的管理要求。
   2) 应核查密钥管理人员是否为本机构在编的正式员工。
   3) 应核查密钥管理人员是否逐级进行备案。
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。

测评单元（L4-MMS1-62）

该测评单元包括以下要求：

a) 测评指标：**系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，至少每3个月更换一次，口令密码的强度应满足不同安全性要求。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查密码管理制度是否要求系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，至少每3个月更换一次，口令密码的强度满足不同安全性要求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-63）

该测评单元包括以下要求：

a) 测评指标：**系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查密码管理制度是否要求系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。

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。

测评单元（L4-MMS1-64）

该测评单元包括以下要求：

a) 测评指标：**密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责，密钥资料须保存在保险柜内，保险柜钥匙由专人负责，使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。（F4）**

b) 测评对象：安全管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈安全管理员，密钥注入、密钥管理功能调试和密钥档案的保管是否由专人负责。

2) 应访谈安全管理员，密钥资料是否保存在保险柜内，保险柜钥匙是否由专人负责。

3) 应访谈安全管理员，使用密钥和销毁密钥是否在监督下进行。

4) 应核查是否具有密钥使用和销毁记录。

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。

测评单元（L4-MMS1-65）

该测评单元包括以下要求：

a) 测评指标：**确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F4）**

b) 测评对象：管理制度类文档。

c) 测评实施：应核查密码管理制度是否要求远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。

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。

测评单元（L4-MMS1-66）

该测评单元包括以下要求：

a) 测评指标：**应支持各类环境中密码设备使用、管理权限分离。（F4）**

b) 测评对象：管理制度类文档。

c) 测评实施：应核查密码管理制度是否要求各类环境中密码设备使用、管理权限分离。

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。

8.1.10.10 变更管理

测评单元（L4-MMS1-67）

该测评单元包括以下要求：

a) 测评指标：**变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认。（F4）**

b) 测评对象：管理制度类文档。

c) 测评实施包括以下内容：

1) 应核查变更管理制度是否明确了变更流程、审批流程。

2) 应核查变更管理制度是否明确变更发起方、实施方的职责。

3) 应核查变更管理制度是否明确了变更方案的测试、审批流程及实施策略。

4) 应核查变更管理制度是否明确要求对有可能影响客户利益的变更应事先通知客户并得到客户的确认。

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。

测评单元（L4-MMS1-68）

该测评单元包括以下要求：

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。
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查变更方案是否包含变更类型、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。

测评单元（L4-MMS1-69）

该测评单元包括以下要求：

a) 测评指标：应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查变更控制的申报、审批程序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) 应核查是否具有变更实施过程的记录文档。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-70）

该测评单元包括以下要求：

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。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人变更中止或失败后的恢复程序、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) 应核查变更恢复程序是否规定变更中止或失败后的恢复流程。
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。

测评单元（L4-MMS1-71）

该测评单元包括以下要求：

a) 测评指标：**变更前应做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查变更方案是否要求变更前做好系统和数据的备份。
   2) 应核查是否具有数据备份记录和跟踪记录文档。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-72）

该测评单元包括以下要求：

a) 测评指标：**如果需要对生产环境进行重大变更，应按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同意后，再进行变更操作，以确保生产系统的安全。（F4）**

b) 测评对象：记录表单类文档。

c) 测评实施包括以下内容：

1) 应核查对于生产环境重大变更是否制订了详细的系统变更方案、系统及数据备份恢复措施和应急处置方案。

2) 应核查对于生产环境重大变更是否在测试环境进行稳妥测试并通过。

3) 应核查对于生产环境重大变更是否具有系统用户和主管领导审批记录。

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

测评单元（L4-MMS1-73）

该测评单元包括以下要求：

a) 测评指标：**当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性，应尽量减少紧急变更。（F4）**

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) 应核查变更管理制度是否要求当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更。

2) 应核查变更管理制度是否要求尽量减少紧急变更。

3) 应核查变更记录与变更管理制度要求是否一致。

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。

8.1.10.11 备份与恢复管理

测评单元（L4-MMS1-74）

该测评单元包括以下要求：

a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等。

b) 测评对象：系统管理员和记录表单类文档。

c) 测评实施包括以下内容：

1) 应访谈系统管理员有哪些需定期备份的业务信息、系统数据及软件系统。

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

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

测评单元（L4-MMS1-75）

该测评单元包括以下要求：

a) 测评指标：应**制定数据备份与恢复相关安全管理制度，**对备份信息的备份方式、备份频度、存储介质、保存期等**进行规范。（F4）**

b) 测评对象：管理制度类文档。

c) 测评实施：

1) 应核查是否建立数据备份与恢复相关安全管理制度。

2) 应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容。

d) 单元判定：如果 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。

测评单元（L4-MMS1-76）

该测评单元包括以下要求：

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。
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文档是否根据数据的重要程度制定相应备份恢复策略和程序等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-77）

该测评单元包括以下要求：

a) 测评指标：**应每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。（F4）**
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) 应核查灾备切换演练制度中是否要求每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据人员、信息资源等变动情况以及演练情况更新和完善应急预案。
   2) 应核查是否具有灾难切换演练记录、应急预案更新和完善记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-78）

该测评单元包括以下要求：

a) 测评指标：**应每季度对备份数据的有效性进行检查，备份数据要实行异地保存。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否每季度对备份数据的有效性进行检查，备份数据是否实行异地保存。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-79）

该测评单元包括以下要求：

a) 测评指标：**灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：
   1) 应核查灾难恢复相关管理制度是否要求灾难恢复的需求需定期进行再分析且再分析周期最长为三年。
   2) 应核查当生产中心环境、生产系统或业务流程发生重大变更时，是否立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-80）

该测评单元包括以下要求：

a) 测评指标：**恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：恢复及使用备份数据时需要提供相关口令密码的，应核查是否将口令密码密封后与数据备份介质一并妥善保管。
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。

测评单元（L4-MMS1-81）

该测评单元包括以下要求：
a) 测评指标：**应定期开展灾难恢复培训，在条件许可的情况下，由相关部门统一部署，至少每年进行一次灾难恢复演练，包括异地备份站点切换演练和本地系统灾难恢复演练；异地备份站点切换：在异地建立热备份站点，当主站点因发生灾难导致系统不可恢复时异地备份站点能承担起主站点的功能，本地系统灾难恢复：当本地系统发生异常中断时能够在短时间恢复和保障业务数据的可运行性。（F4）**
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) 应核查灾难恢复管理制度是否要求定期开展灾难恢复培训和灾难恢复演练。
   2) 应核查是否具有灾难恢复培训和演练记录，灾难恢复演练记录是否包括异地备份站点切换演练和本地系统灾难恢复演练。
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。

测评单元（L4-MMS1-82）

该测评单元包括以下要求：
a) 测评指标：**金融机构应根据信息系统的灾难恢复工作情况，确定审计频率，应每年至少组织一次内部灾难恢复工作审计。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否每年至少组织一次内部灾难恢复工作审计。
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。

测评单元（L4-MMS1-83）

该测评单元包括以下要求：
a) 测评指标：**应安排专人负责灾难恢复预案的日常维护管理。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否安排专人负责灾难恢复预案的日常维护管理。
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。

测评单元（L4-MMS1-84）

该测评单元包括以下要求：
a) 测评指标：**应建立灾难备份系统，主备系统实际切换时间应满足实时切换，灾备系统处理能力应不低于主用系统处理能力的 50%，通信线路应分别接入主备系统。有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F4）**
b) 测评对象：灾难备份系统。
c) 测评实施包括以下内容：
   1) 应核查是否建立灾难备份系统。
   2) 应核查灾难备份系统的主备系统实际切换时间是否满足实时切换。
   3) 应核查灾备系统处理能力是否不低于主用系统处理能力的 50%。

4） 应核查通信线路是否分别接入主备系统。

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。

8.1.10.12 安全事件处置

测评单元（L4-MMS1-85）

该测评单元包括以下要求：

a） 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件。

b） 测评对象：运维负责人和记录表单类文档。

c） 测评实施包括以下内容：

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

2） 应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。

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

测评单元（L4-MMS1-86）

该测评单元包括以下要求：

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。

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是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和响应流程等。

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

测评单元（L4-MMS1-87）

该测评单元包括以下要求：

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。

b） 测评对象：记录表单类文档。

c） 测评实施：应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过程、经验教训、补救措施等内容。

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

测评单元（L4-MMS1-88）

该测评单元包括以下要求：

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。

b） 测评对象：运维负责人和记录表单类文档。

c） 测评实施包括以下内容：

1） 应访谈运维负责人是否具备不同安全事件的报告流程。

2） 应核查针对重大安全事件是否制定不同安全事件报告和处理流程，是否明确具体报告方式、报告内容、报告人等方面内容。

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

测评单元（L4-MMS1-89）

该测评单元包括以下要求：

a） 测评指标：应建立联合防护和应急机制，负责处置跨单位安全事件。

b) 测评对象：安全管理员、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) 应访谈安全管理员是否建立跨单位处置安全事件流程。
   2) 应核查跨单位安全事件报告和处置管理制度，核查是否含有联合防护和应急的相关内容。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.10.13 应急预案管理

测评单元（L4-MMS1-90）

该测评单元包括以下要求：
a) 测评指标：应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容，**业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字确认。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施包括以下内容：
   1) 应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面。
   2) 应核查业务处理系统应急预案的编制工作是否由相关业务部门和科技部门共同完成。
   3) 应核查业务处理系统应急预案是否由预案涉及的相关机构进行签字确认。
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。

测评单元（L4-MMS1-91）

该测评单元包括以下要求：
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。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查是否具有重要事件的应急预案（如针对机房、系统、网络等各个方面）。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-92）

该测评单元包括以下要求：
a) 测评指标：应**每年**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。**（F4）**
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否每年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是否记录演练时间、主要操作内容、演练结果等。
d) 单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-93）

该测评单元包括以下要求：
a) 测评指标：应定期对原有的应急预案重新评估，修订完善。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人，是否具有管理制度规定定期对原有的应急预案重新评估。
   2) 应核查应急预案重新评估记录是否与管理要求一致。

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。

测评单元（L4-MMS1-94）

该测评单元包括以下要求：

a) 测评指标：应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练。
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否针对重大安全事件建立跨单位的应急预案并进行过演练。
   2) 应核查是否具有针对重大安全事件跨单位的应急预案。
   3) 应核查跨单位应急预案演练记录是否记录演练时间、主要操作内容、演练结果等。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-95）

该测评单元包括以下要求：

a) 测评指标：**在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。（F4）**
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人在与第三方合作的业务中是否建立并完善了内部责任机制以及与相关机构之间的协调机制。
   2) 应核查是否具有完整的应急预案及应急协调预案。
   3) 应核查是否具有联合演练记录。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-96）

该测评单元包括以下要求：

a) 测评指标：**突发事件应急处置领导小组应统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F4）**
b) 测评对象：运维负责人和记录表单类文档。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否由突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源。
   2) 应核查是否具有应急处置联络人名单并上报至本行业网络安全监管部门。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS1-97）

该测评单元包括以下要求：

a) 测评指标：**突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F4）**
b) 测评对象：管理制度类文档。
c) 测评实施：应核查突发事件管理相关制度是否明确要求突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。

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。

测评单元（L4-MMS1-98）

该测评单元包括以下要求：

a) 测评指标：**实施报告制度和启动应急预案的单位应当实行重大突发事件 24 小时值班制度。（F4）**
b) 测评对象：运维负责人。
c) 测评实施：应访谈运维负责人是否具有重大突发事件 24 小时值班制度。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS1-99）

该测评单元包括以下要求：

a) 测评指标：**应急演练结束后，应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有应急演练情况总结报告。
   2) 应核查应急演练情况总结报告内容是否包括：内容、目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划和演练结论。
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。

8.1.10.14 外包运维管理

测评单元（L4-MMS1-100）

该测评单元包括以下要求：

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。
b) 测评对象：运维负责人。
c) 测评实施包括以下内容：
   1) 应访谈运维负责人是否有外包运维服务情况。
   2) 应访谈运维负责人外包运维服务单位是否符合国家有关规定。
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。

测评单元（L4-MMS1-101）

该测评单元包括以下要求：

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。
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是否明确约定外包运维的范围和工作内容。
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。

测评单元（L4-MMS1-102）

该测评单元包括以下要求：

a) 测评指标：应保证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。
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。

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。

测评单元（L4-MMS1-103）

该测评单元包括以下要求：

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。
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。

测评单元（L4-MMS1-104）

该测评单元包括以下要求：

a) 测评指标：**应要求外包运维服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施包括以下内容：
   1) 应核查是否具有外包服务商的操作记录文档。
   2) 应核查操作记录文档的内容和保存期限是否满足事件分析、安全取证、独立审计和监督检查需要。
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。

测评单元（L4-MMS1-105）

该测评单元包括以下要求：

a) 测评指标：**应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F4）**
b) 测评对象：记录表单类文档。
c) 测评实施：应核查是否具有数据中心外包服务应急计划以应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形。
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。

8.2 云计算安全测评扩展要求

8.2.1 安全物理环境

8.2.1.1 基础设施位置

测评单元（L4-PES2-01）

该测评单元包括以下要求：

a) 测评指标：应保证云计算基础设施位于中国境内。
b) 测评对象：机房管理员、办公场地、机房和平台建设方案。
c) 测评实施包括以下内容：
   1) 应访谈机房管理员，云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内。
   2) 应核查云计算平台建设方案，云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内。

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

测评单元（L4-PES2-02）

该测评单元包括以下要求：

a) 测评指标：**对于团体云部署模式，应保证用于服务金融行业的云计算数据中心的物理服务器与其他行业物理隔离。（F4）**

b) 测评对象：机房管理员、办公场地、机房和平台建设方案。

c) 测评实施包括以下内容：

1) 应访谈机房管理员，云计算服务器、存储设备、网络设备、云管理平台、信息系统等用于服务金融行业的云计算数据中心运行环境是否未存放其他行业物理设备。

2) 应查看机房区域间是否具有有效的物理隔离措施，如实体墙区分、金属网隔离、防火玻璃等。

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。

测评单元（L4-PES2-03）

该测评单元包括以下要求：

a) 测评指标：**应保证云计算平台的运维和运营系统部署在中国境内。（F4）**

b) 测评对象：办公场地、运维地点、运维记录和平台建设方案。

c) 测评实施包括以下内容：

1) 应核查云计算平台运维的系统地点是否位于中国境内，应核查云计算平台运营的系统地点是否位于中国境内。

2) 应核查云计算平台运维和运营的维护地点是否位于中国境内，是否不存在从境外对境内云计算平台实施远程运维和运营的设备、地点和相关内容。

3) 应核查云计算平台远程运维和运营记录中是否不存在境外对境内云计算平台实施运维和运营的操作。

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。

8.2.2 安全通信网络

8.2.2.1 网络架构

测评单元（L4-CNS2-01）

该测评单元包括以下要求：

a) 测评指标：应保证云计算平台不承载高于其安全保护等级的业务应用系统。

b) 测评对象：云计算平台和业务应用系统定级备案材料。

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

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

测评单元（L4-CNS2-02）

该测评单元包括以下要求：

a) 测评指标:应实现不同云服务客户虚拟网络之间**及同一云服务客户不同虚拟网络之间**的隔离。**(F4)**

b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台。

c) 测评实施包括以下内容：

1) 应核查云服务客户之间是否采取网络隔离措施。

2) 应核查同一云服务客户不同虚拟网络之间是否采取网络隔离措施。

3) 应核查云服务客户之间是否设置并启用网络资源隔离策略。

4) 应核查同一云服务客户不同虚拟网络之间是否设置并启用网络资源隔离策略。

5） 应测试验证不同云服务客户之间的网络隔离措施是否有效。
6） 应测试验证同一云服务客户不同虚拟网络之间的网络隔离措施是否有效。

d） 单元判定：如果1）～6）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。

测评单元（L4-CNS2-03）

该测评单元包括以下要求：

a） 测评指标：**应实现云计算平台的业务网络与管理网络安全隔离。（F4）**
b） 测评对象：网络资源隔离措施、综合网管系统和云管理平台。
c） 测评实施包括以下内容：
1） 应核查业务网络与管理网络之间是否存在隔离措施。
2） 应测试验证业务网络与管理网络之间的隔离措施是否有效。
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。

测评单元（L4-CNS2-04）

该测评单元包括以下要求：

a） 测评指标：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。
b） 测评对象：防火墙、入侵检测系统、入侵保护系统和抗APT攻击系统等安全设备。
c） 测评实施包括以下内容：
1） 应核查云计算平台是否具备为云服务客户提供通信传输、边界防护、入侵防范等安全防护机制的能力。
2） 应核查上述安全防护机制是否满足云服务客户的业务需求。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CNS2-05）

该测评单元包括以下要求：

a） 测评指标：应具有根据云服务客户业务需求自主设置安全策略的能力，包括**划分安全区域、**定义访问路径、选择安全组件、配置安全策略。**（F4）**
b） 测评对象：云管理平台、网络管理平台、网络设备和安全访问路径。
c） 测评实施包括以下内容：
1） 应核查云计算平台是否支持云服务客户自主定义安全策略，包括划分安全区域、定义访问路径、选择安全组件、配置安全策略。
2） 应核查云服务客户是否能够自主设置安全策略，包括划分安全区域、定义访问路径、选择安全组件、配置安全策略。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CNS2-06）

该测评单元包括以下要求：

a） 测评指标：应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。
b） 测评对象：相关开放性接口和安全服务及相关文档。
c） 测评实施包括以下内容：
1） 应核查接口设计文档或开放性服务技术文档是否符合开放性及安全性要求。
2） 应核查云服务客户是否可以接入第三方安全产品或在云计算平台选择第三方安全服务。

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。

测评单元（L4-CNS2-07）

该测评单元包括以下要求：

a) 测评指标：应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以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。
b) 测评对象：系统管理员、相关接口和相关服务。
c) 测评实施包括以下内容：
   1) 应核查是否提供了对虚拟资源的主体和客体设置安全标记的能力。
   2) 应核查是否对虚拟资源的主体和客体设置了安全标记。
   3) 应测试验证是否基于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。

测评单元（L4-CNS2-08）

该测评单元包括以下要求：

a) 测评指标：应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式。
b) 测评对象：网闸等提供通信协议转换或通信协议隔离功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否采取通信协议转换或通信协议隔离等方式进行数据交换。
   2) 应通过发送带通用协议的数据等测试方式，测试验证设备是否能够有效阻断。
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。

测评单元（L4-CNS2-09）

该测评单元包括以下要求：

a) 测评指标：应为第四级业务应用系统划分独立的资源池。
b) 测评对象：网络拓扑和云计算平台建设方案。
c) 测评实施包括以下内容：
   1) 应核查云计算平台建设方案中是否对承载四级业务系统的资源池做出独立划分设计。
   2) 应核查网络拓扑图是否对第四级业务系统划分独立的资源池。
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。

测评单元（L4-CNS2-10）

该测评单元包括以下要求：

a) 测评指标：**对于团体云部署模式，应保证除广域网外为金融行业服务的网络物理硬件不与其他行业共享。（F4）**
b) 测评对象：网络拓扑和云计算平台建设方案。
c) 测评实施包括以下内容：
   1) 应核查云计算平台建设方案中是否对除广域网外为金融行业服务的网络物理硬件做出专用要求。
   2) 应核查网络拓扑图中是否除广域网外为金融行业服务的交换机、路由器等网络设备均为金融行业专用。
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。

测评单元（L4-CNS2-11）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户监控所拥有各网络节点间的流量。（F4）**

b) 测评对象：云计算平台监控措施和云计算平台建设方案。

c) 测评实施：应核查云计算平台是否支持云服务客户监控所拥有各网络节点间的流量。

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。

8.2.3 安全区域边界

8.2.3.1 访问控制

测评单元（L4-ABS2-01）

该测评单元包括以下要求：

a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。

b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备。

c) 测评实施包括以下内容：

1) 应核查是否在虚拟化网络边界部署访问控制机制，并设置访问控制规则。

2) 应核查并测试验证云计算平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效。

3) 应核查并测试验证云计算平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效。

4) 应核查并测试验证不同云服务客户间访问控制规则和访问控制策略是否有效。

5) 应核查并测试验证云服务客户不同安全保护等级业务系统之间访问控制规则和访问控制策略是否有效。

d) 单元判定：如果1）～5）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。

测评单元（L4-ABS2-02）

该测评单元包括以下要求：

a) 测评指标：应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备。

c) 测评实施包括以下内容：

1) 应核查是否在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

2) 应核查不同安全等级网络区域边界的访问控制规则和访问控制策略是否有效。

3) 应测试验证不同安全等级的网络区域间进行非法访问时，是否可以正确拒绝该非法访问。

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。

测评单元（L4-ABS2-03）

该测评单元包括以下要求：

a) 测评指标：**应实现虚拟机之间、虚拟机与资源管理和调度平台之间、虚拟机与外部网络之间的安全访问控制。（F4）**

b) 测评对象：云计算平台。

c) 测评实施：应核查云计算平台是否具备不同层面的访问控制能力，如在虚拟防火墙、虚拟路由器、虚拟交换机上配置访问控制策略，实现虚拟机之间、虚拟机与管理平台之间、虚拟机与外部网络之间访问控制。

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

测评单元（L4-ABS2-04）

该测评单元包括以下要求：

a) 测评指标：**应对云计算平台管理员访问管理网络进行访问控制。（F4）**

b) 测评对象：云计算平台管理员访问控制策略。

c) 测评实施包括以下内容：

1) 应核查是否支持云计算平台管理员访问网络的身份验证和权限控制。

2) 应核查云计算平台对网络资源管理员的访问控制措施是否有效。

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。

测评单元（L4-ABS2-05）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户通过VPN访问云计算平台。（F4）**

b) 测评对象：云计算平台。

c) 测评实施包括以下内容：

1) 核查云计算平台是否支持向云服务客户提供 VPN。

2) 核查云服务客户是否可以通过 VPN 访问云计算平台。

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。

测评单元（L4-ABS2-06）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户自行在虚拟网络边界设置访问控制规则。（F4）**

b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备。

c) 测评实施包括以下内容：

1) 核查云计算平台是否允许云服务客户在虚拟网络边界设置访问控制规则。

2) 核查云服务客户设置的访问控制规则等是否有效。

3) 测试虚拟化网络边界访问控制设备，验证是否可以正确拒绝违反访问控制规则的非法访问。

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。

测评单元（L4-ABS2-07）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户自行划分子网、设置访问控制规则。（F4）**

b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备。

c) 测评实施包括以下内容：

1) 应核查云计算平台是否允许云服务客户自行划分子网、设置访问控制规则。

2) 应核查云服务客户自行划分子网、设置访问控制规则等是否有效。

3) 应测试虚拟化网络边界访问控制设备，验证是否可以正确拒绝违反访问控制规则的非法访问。

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。

8.2.3.2 入侵防范

测评单元（L4-ABS2-08）

该测评单元包括以下要求：

a) 测评指标：应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。

b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否采取了入侵防范措施对网络入侵行为进行防范，如部署抗 APT 攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件。
2) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件的规则库升级方式，核查规则库是否进行及时更新。
3) 应核查部署的抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能，以及报警功能和清洗处置功能。
4) 应测试验证抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证入侵防范设备或相关组件是否能记录攻击类型、攻击时间、攻击流量）。
5) 应测试验证抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件对云服务客户网络攻击行为的报警策略是否有效（如模拟产生攻击动作，验证抗 APT 攻击系统或网络入侵保护系统是否能实时报警）。
6) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具有对 SQL 注入、跨站脚本等攻击行为的发现和阻断能力。
7) 应核查抗 APT 攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否能够检测出具有恶意行为、过分占用计算资源和带宽资源等恶意行为的虚拟机。
8) 应核查云管理平台对云服务客户攻击行为的防范措施，核查是否能够对云服务客户的网络攻击行为进行记录，记录应包括攻击类型、攻击时间和攻击流量等内容。
9) 应核查云管理平台或入侵防范设备是否能够对云计算平台内部发起的恶意攻击或恶意外连行为进行限制，核查是否能够对内部行为进行监控。
10) 通过对外攻击发生器伪造对外攻击行为，核查云服务客户的网络攻击日志，确认是否正确记录相应的攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP 和攻击流量规模等内容。
11) 应核查运行虚拟机监控器（VMM）、容器监控器和云管理平台软件的物理主机，确认其安全加固手段是否能够避免或减少虚拟化共享带来的安全漏洞。

d) 单元判定：如果1）～11）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。

测评单元（L4-ABS2-09）

该测评单元包括以下要求：

a) 测评指标：应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否部署网络攻击行为检测设备或相关组件对虚拟网络节点的网络攻击行为进行防范，并能记录攻击类型、攻击时间、攻击流量等。
   2) 应核查网络攻击行为检测设备或相关组件的规则库是否为最新。
   3) 应测试验证网络攻击行为检测设备或相关组件对异常流量和未知威胁的监控策略是否有效。
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。

测评单元（L4-ABS2-10）

该测评单元包括以下要求：

a) 测评指标：应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。
b) 测评对象：虚拟机、宿主机、抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量的检测功能。

2） 应测试验证对异常流量的监测策略是否有效。

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。

测评单元（L4-ABS2-11）

该测评单元包括以下要求：

a） 测评指标：应在检测到网络攻击行为、异常流量情况时进行告警。

b） 测评对象：虚拟机、宿主机、抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。

c） 测评实施包括以下内容：

1） 应核查检测到网络攻击行为、异常流量时是否进行告警。

2） 应测试验证其对异常流量的监测策略是否有效。

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。

测评单元（L4-ABS2-12）

该测评单元包括以下要求：

a） 测评指标：**应检测和防护云计算平台内部虚拟机发起的针对云计算平台的攻击，能够定位发起攻击的虚拟机，记录攻击类型、攻击时间、攻击流量等信息。（F4）**

b） 测评对象：安全服务、安全组件、监测信息。

c） 测评实施包括以下内容：

1） 应核查云计算平台是否对内部虚拟机发起的针对云计算平台的攻击进行识别、检测与防护。

2） 应核查云计算平台是否能够定位发起攻击的虚拟机，记录攻击类型、攻击时间、攻击流量。

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。

测评单元（L4-ABS2-13）

该测评单元包括以下要求：

a） 测评指标：**云服务客户通过互联网提供金融服务时，应支持DoS/DDoS攻击防护，通过清洗DoS/DDoS攻击流量，保障网络、服务器及上层应用的可用性。（F4）**

b） 测评对象：入侵保护系统、DoS/DDoS防护模块或相关组件。

c） 测评实施包括以下内容：

1） 应核查系统是否具备对 DoS/DDoS 攻击的防护措施。

2） 应核查历史记录或测试验证对 DoS/DDoS 攻击的防护措施是否有效（如模拟产生攻击动作，验证入侵保护系统和相关组件等）。

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。

测评单元（L4-ABS2-14）

该测评单元包括以下要求：

a） 测评指标：**云服务客户通过互联网提供金融服务时，应支持检测Web应用漏洞，拦截SQL注入、XSS攻击等多种Web应用攻击行为。（F4）**

b） 测评对象：入侵保护系统、Web应用防火墙或相关组件。

c） 测评实施包括以下内容：

1） 应核查相关系统或设备是否具备 Web 应用漏洞检测功能，包括拦截 SQL 注入、XSS 攻击相关功能。

2） 应测试验证或核查历史记录判断相关系统或设备的检测措施是否有效。

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。

8.2.3.3 安全审计

测评单元（L4-ABS2-15）

该测评单元包括以下要求：

a) 测评指标：应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。
b) 测评对象：堡垒机或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云服务商（含第三方运维服务商）和云服务客户在远程管理时执行的远程特权命令是否有相关审计记录。
   2) 应测试验证云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ABS2-16）

该测评单元包括以下要求：

a) 测评指标：应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。
b) 测评对象：综合审计系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计。
   2) 应测试验证云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。
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。

8.2.4 安全计算环境

8.2.4.1 身份鉴别

测评单元（L4-CES2-01）

该测评单元包括以下要求：

a) 测评指标：当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。
b) 测评对象：管理终端和云计算平台。
c) 测评实施包括以下内容：
   1) 应核查当进行远程管理时是否建立双向身份验证机制。
   2) 应测试验证上述双向身份验证机制是否有效。
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。

测评单元（L4-CES2-02）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户密码策略管理，密码策略管理应支持密码复杂度策略、密码有效期策略，云服务客户账号的初始密码应支持随机生成，云服务客户首次登录支持强制修改初始密码。（F4）**
b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。
c) 测评实施包括以下内容：
   1) 被测对象为云计算平台时，应核查云计算平台是否支持云服务客户密码策略管理功能，包括密码复杂度策略、密码有效期策略。

2) 被测对象为云计算平台时，应核查云计算平台是否支持云服务客户账号的初始密码随机生成，是否支持云服务客户首次登录强制修改初始密码。
3) 被测对象为云服务客户时，应核查云服务客户是否开启密码复杂度策略、密码有效期策略。
4) 被测对象为云服务客户时，应核查云服务客户是否开启账户的初始密码随机生成功能，是否开启首次登录强制修改初始密码策略。

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。

测评单元（L4-CES2-03）

该测评单元包括以下要求：

a) 测评指标：**应支持为云服务客户随机生成虚拟机登录口令或云服务客户自行设置登录口令。（F4）**
b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。
c) 测评实施包括以下内容：
1) 被测对象为云计算平台时，应核查云计算平台是否支持云服务客户随机生成虚拟机登录口令或自行设置登录口令。
2) 被测对象为云服务客户时，应核查云服务客户是否可随机生成虚拟机登录口令或自行设置登录口令。
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。

测评单元（L4-CES2-04）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户以密钥对方式登录虚拟机时，自主选择云计算平台生成密钥对或自行上传密钥对。（F4）**
b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。
c) 测评实施包括以下内容：
1) 应核查云计算平台是否支持云服务客户以密钥对方式登录虚拟机。
2) 应核查云服务客户是否可以自主选择云计算平台生成密钥对或自行上传密钥对。
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。

测评单元（L4-CES2-05）

该测评单元包括以下要求：

a) 测评指标:**应支持云服务客户自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。（F4）**
b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。
c) 测评实施包括以下内容：
1) 应测试验证云计算平台是否支持云服务客户自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。
2) 应测试验证云服务客户是否可以自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。
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。

测评单元（L4-CES2-06）

该测评单元包括以下要求：

a) 测评指标：**应支持集中管理云服务客户鉴别凭证。（F4）**
b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。
c) 测评实施：应核查云计算平台是否支持集中管理云服务客户鉴别凭证。

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。

测评单元（L4-CES2-07）

该测评单元包括以下要求：

a) 测评指标：**应支持修改云服务客户鉴别凭证前验证云服务客户身份。（F4）**

b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。

c) 测评实施包括以下内容：

1) 应检测云计算平台是否支持修改云服务客户鉴别凭证前验证云服务客户身份。

2) 应检测云服务客户是否在修改鉴别凭证前需要进行身份验证。

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。

测评单元（L4-CES2-08）

该测评单元包括以下要求：

a) 测评指标：**应支持检测云服务客户账户异常并通知云服务客户。（F4）**

b) 测评对象：云计算平台、云服务客户、云计算平台用户身份管理功能。

c) 测评实施包括以下内容：

1) 应检测云计算平台是否支持检测云服务客户账户异常并通知云服务客户。

2) 应检测是否有相关通知记录。

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

8.2.4.2 访问控制

测评单元（L4-CES2-09）

该测评单元包括以下要求：

a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移。

b) 测评对象：虚拟机、虚拟机迁移记录和相关配置。

c) 测评实施包括以下内容：

1) 应核查虚拟机迁移时访问控制策略是否随之迁移。

2) 应测试验证虚拟机迁移后访问控制措施是否随其迁移。

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。

测评单元（L4-CES2-10）

该测评单元包括以下要求：

a) 测评指标：应允许云服务客户设置不同虚拟机之间的访问控制策略。

b) 测评对象：虚拟机和安全组或相关组件。

c) 测评实施包括以下内容：

1) 应核查云服务客户是否能够设置不同虚拟机间访问控制策略。

2) 应测试验证上述访问控制策略是否有效。

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。

测评单元（L4-CES2-11）

该测评单元包括以下要求：

a) 测评指标：**应禁止云服务商或第三方未授权操作云服务客户资源。（F4）**

b) 测评对象：云管理平台。

c) 测评实施：应核查在未授权情况下，云服务商或第三方是否无法操作云服务客户资源。

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。

8.2.4.3 入侵防范

测评单元（L4-CES2-12）

该测评单元包括以下要求：

a) 测评指标：应能检测虚拟机之间的资源隔离失效，并进行告警。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测到虚拟机之间的资源隔离失效并进行告警，如CPU、内存和磁盘资源之间的隔离失效。
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。

测评单元（L4-CES2-13）

该测评单元包括以下要求：

a) 测评指标：应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。
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。

测评单元（L4-CES2-14）

该测评单元包括以下要求：

a) 测评指标：应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。
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。

测评单元（L4-CES2-15）

该测评单元包括以下要求：

a) 测评指标：**应能够检测虚拟机对宿主机资源的异常访问，并进行告警。（F4）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否能够检测虚拟机对宿主机资源的异常访问，并进行告警。
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。

测评单元（L4-CES2-16）

该测评单元包括以下要求：

a) 测评指标：**应对虚拟机启动和运行过程进行完整性保护。（F4）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否采取了措施对虚拟机启动和运行过程进行完整性保护。
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。

测评单元（L4-CES2-17）

该测评单元包括以下要求：

a) 测评指标：**应对虚拟机重要配置文件进行完整性保护。（F4）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否采取了措施对虚拟机重要配置文件进行完整性保护。

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。

8.2.4.4 恶意代码防范

测评单元（L4-CES2-18）

该测评单元包括以下要求：

a) 测评指标：**应支持对后门、木马、蠕虫、webshell等恶意代码的静态检测和行为检测，并对检测出的恶意代码进行控制和隔离。（F4）**

b) 测评对象：云管理平台、云服务客户、防病毒网关和UTM等提供防恶意代码功能的系统或相关组件。

c) 测评实施包括以下内容：

1) 测评对象是云计算平台时，应核查云计算平台是否部署了防恶意代码产品或采取了其他恶意代码防范措施，应核查防恶意代码产品运行是否正常，是否支持对后门、木马、蠕虫、webshell等恶意代码的静态检测和行为检测，应核查恶意代码库是否已经更新到最新，应检查是否支持对检测出的恶意代码进行控制和隔离。

2) 测评对象是云服务客户时，应核查云服务客户是否开启了恶意代码防范服务或采取了其他恶意代码防范措施。

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。

测评单元（L4-CES2-19）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户自行安装防恶意代码软件，并支持更新防恶意代码软件版本和恶意代码库。（F4）**

b) 测评对象：云管理平台、云服务客户、防病毒网关和UTM等提供防恶意代码功能的系统或相关组件。

c) 测评实施包括以下内容：

1) 测评对象是云计算平台时，应核查云计算平台是否支持云服务客户自行安装防恶意代码软件，是否支持更新防恶意代码软件版本和恶意代码库，应核查防恶意代码软件版本和恶意代码库是否为最新。

2) 测评对象是云服务客户时，应核查云服务客户是否可自行安装防恶意代码软件，是否支持更新防恶意代码软件版本和恶意代码库，应核查防恶意代码软件版本和恶意代码库是否为最新。

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

8.2.4.5 镜像和快照保护

测评单元（L4-CES2-20）

该测评单元包括以下要求：

a) 测评指标：应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。

b) 测评对象：虚拟机镜像文件。

c) 测评实施：应核查是否对生成的虚拟机镜像采取必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。

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。

测评单元（L4-CES2-21）

该测评单元包括以下要求：

a) 测评指标：应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。

b) 测评对象：云管理平台和虚拟机镜像、快照或相关组件。

c) 测评实施包括以下内容：

1） 应核查是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。
2） 应测试验证是否能够对镜像、快照进行完整性验证。

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。

测评单元（L4-CES2-22）

该测评单元包括以下要求：

a） 测评指标：应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。
b） 测评对象：云管理平台和虚拟机镜像、快照或相关组件。
c） 测评实施：应核查是否对虚拟机镜像或快照中的敏感资源采用加密、访问控制等技术手段进行保护，防止可能存在的针对快照的非法访问。
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。

测评单元（L4-CES2-23）

该测评单元包括以下要求：

a） 测评指标：**应保证虚拟机镜像和快照文件备份在不同物理服务器。（F4）**
b） 测评对象：云管理平台和虚拟机镜像、快照或相关组件。
c） 测评实施包括以下内容：
1） 应核查云平台虚拟机镜像文件是否备份在不同的物理服务器。
2） 应核查云平台虚拟机快照文件是否备份在不同的物理服务器。
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。

测评单元（L4-CES2-24）

该测评单元包括以下要求：

a） 测评指标：**应支持自动虚拟机快照功能，保证系统能根据快照恢复。（F4）**
b） 测评对象：云管理平台、云服务客户、虚拟机镜像、快照或相关组件。
c） 测评实施包括以下内容：
1） 测评对象是云计算平台时，应核查云计算平台是否支持自动虚拟机快照功能，应检验快照是否可以恢复。
2） 测评对象是云服务客户时，应检验快照是否可以恢复。
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，否则不符合本测评单元指标要求。

8.2.4.6 数据完整性和保密性

测评单元（L4-CES2-25）

该测评单元包括以下要求：

a） 测评指标：应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
b） 测评对象：数据库服务器、数据存储设备和管理文档记录。
c） 测评实施包括以下内容：
1） 应核查云服务客户数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内。
2） 应核查上述数据出境时是否符合国家相关规定。
d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CES2-26）

该测评单元包括以下要求：

a) 测评指标：应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限。
b) 测评对象：云管理平台、数据库、相关授权文档和管理文档。
c) 测评实施包括以下内容：
   1) 应核查云服务客户数据管理权限授权流程、授权方式、授权内容。
   2) 应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查是否有相关授权证明。
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。

测评单元（L4-CES2-27）

该测评单元包括以下要求：

a) 测评指标：应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
b) 测评对象：虚拟机。
c) 测评实施：应核查在虚拟资源迁移过程中，是否采取校验技术或密码技术等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
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。

测评单元（L4-CES2-28）

该测评单元包括以下要求：

a) 测评指标：应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。
b) 测评对象：密钥管理解决方案。
c) 测评实施包括以下内容：
   1) 当云服务客户已部署密钥管理解决方案，应核查密钥管理解决方案是否能保证云服务客户自行实现数据的加解密过程。
   2) 应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能保证云服务客户自行实现数据的加解密过程。
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。

测评单元（L4-CES2-29）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户选择第三方密钥加解密数据，密钥支持云服务客户自管理、云服务商管理和第三方机构管理。（F4）**
b) 测评对象：云计算平台、云服务客户和密钥管理解决方案。
c) 测评实施包括以下内容：
   1) 当测评对象是云计算平台，应核查云计算平台是否支持云服务客户选择第三方密钥管理机制加解密数据，密钥是否支持云服务客户自管理、云服务商管理和第三方机构管理。
   2) 当测评对象是云服务客户，应核查云服务客户是否已部署密钥管理解决方案，是否可以自行选择第三方密钥管理机制加解密数据，并记录所采取的密钥管理机制（如云服务客户自管理、云服务商管理和第三方机构管理等）。
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，否则不符合本测评单元指标要求。

测评单元（L4-CES2-30）

该测评单元包括以下要求：

a) 测评指标：**应支持云服务客户对云计算平台上的数据进行加密存储。（F4）**
b) 测评对象：云计算平台、云服务客户和数据。
c) 测评实施包括以下内容：
   1) 当测评对象是云计算平台，应核查云计算平台是否支持云服务客户对云计算平台上的数据进行加密存储。
   2) 当测评对象是云服务客户，应核查云服务客户是否可以对云计算平台上的数据进行加密存储。
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，否则不符合本测评单元指标要求。

8.2.4.7 数据备份恢复

测评单元（L4-CES2-31）

该测评单元包括以下要求：
a) 测评指标：云服务客户应在本地保存其业务数据的备份。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查是否提供备份措施保证云服务客户可以在本地备份其业务数据。
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。

测评单元（L4-CES2-32）

该测评单元包括以下要求：
a) 测评指标：应提供查询云服务客户数据及备份存储位置的能力。
b) 测评对象：云管理平台或相关组件。
c) 测评实施：应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
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。

测评单元（L4-CES2-33）

该测评单元包括以下要求：
a) 测评指标：云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致。
b) 测评对象：云管理平台、云存储系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本。
   2) 应核查各副本内容是否保持一致。
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。

测评单元（L4-CES2-34）

该测评单元包括以下要求：
a) 测评指标：应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。
b) 测评对象：相关技术措施和手段。
c) 测评实施包括以下内容：
   1) 应核查是否有相关技术手段保证云服务客户能够将业务系统及数据迁移到其他云计算平台和本地系统。
   2) 应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。
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。

测评单元（L4-CES2-35）

该测评单元包括以下要求：

a) 测评指标：**应周期性测试云计算平台的备份系统和备份数据，支持故障识别和备份重建。（F4）**

b) 测评对象：云管理平台或相关组件、备份系统、备份数据、数据备份恢复相关的管理制度。

c) 测评实施包括以下内容：

1) 应核查云服务商是否周期性测试云计算平台的备份系统和备份数据，支持故障识别和备份重建。

2) 应核查云计算平台的备份系统和备份数据是否能够正常进行备份和恢复。

3) 应核查是否具有数据备份系统和备份数据的测试记录。

4) 应核查数据备份恢复相关的管理制度是否有相关的备份要求。

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。

8.2.4.8 剩余信息保护

测评单元（L4-CES2-36）

该测评单元包括以下要求：

a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

b) 测评对象：云计算平台。

c) 测评实施包括以下内容：

1) 应核查虚拟机的内存和存储空间回收时，是否得到完全清除。

2) 应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。

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。

测评单元（L4-CES2-37）

该测评单元包括以下要求：

a) 测评指标：云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除，**不能通过软件工具恢复。（F4）**

b) 测评对象：云存储和云计算平台。

c) 测评实施：应核查当云服务客户删除业务应用数据时，云存储中所有副本是否被删除，且不能通过软件工具恢复。

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。

测评单元（L4-CES2-38）

该测评单元包括以下要求：

a) 测评指标：**对于更换或报废的存储介质，应采取安全删除、强化消磁或者物理损坏磁盘等方式，防止恢复已清除数据。（F4）**

b) 测评对象：存储介质和存储介质相关的管理制度。

c) 测评实施包括以下内容：

1) 应核查存储介质相关的管理制度是否规定对于更换或报废的存储介质，应采取安全删除、强化消磁或者物理损坏磁盘等方式，防止恢复已清除数据。

2) 应核查对于更换或报废的存储介质，是否采取了安全删除、强化消磁或者物理损坏磁盘等方式防止恢复已清除数据。

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。

8.2.5 安全管理中心

8.2.5.1 集中管控

测评单元（L4-SMC2-01）

该测评单元包括以下要求：

a) 测评指标：应能对物理资源和虚拟资源按照策略做统一管理调度与分配。
b) 测评对象：资源调度平台、云管理平台或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否有资源调度平台等提供资源统一管理调度与分配策略。
   2) 应核查是否能够按照上述策略对物理资源和虚拟资源做统一管理调度与分配。
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。

测评单元（L4-SMC2-02）

该测评单元包括以下要求：

a) 测评指标：应保证云计算平台管理流量与云服务客户业务流量分离。
b) 测评对象：网络架构和云管理平台。
c) 测评实施包括以下内容：
   1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离。
   2) 应测试验证云计算平台管理流量与业务流量是否分离。
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。

测评单元（L4-SMC2-03）

该测评单元包括以下要求：

a) 测评指标：应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。
b) 测评对象：云管理平台、综合审计系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集。
   2) 应核查云服务商和云服务客户是否能够实现各自的集中审计。
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。

测评单元（L4-SMC2-04）

该测评单元包括以下要求：

a) 测评指标：应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等运行状况的集中监测，**监测内容包括CPU利用率、带宽使用情况、内存利用率、存储使用情况等。（F4）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等运行状况的集中监测。
   2) 应核查监控内容是否包括 CPU 利用率、带宽使用情况、内存利用率、存储使用情况等。
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。

测评单元（L4-SMC2-05）

该测评单元包括以下要求：

a) 测评指标：**应对异常行为集中监控分析并告警。集中监控服务质量，并可导出集中监控报告。应支持远程监控的可视化展示。（F4）**
b) 测评对象：云管理平台或相关组件。
c) 测评实施包括以下内容：
   1) 应核查云服务商是否对异常行为进行集中监控分析并告警。
   2) 应核查是否可导出集中监控报告。
   3) 应核查是否支持远程监控的可视化展示。
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。

8.2.6 安全建设管理

8.2.6.1 云服务商选择

测评单元（L4-CMS2-01）

该测评单元包括以下要求：
a) 测评指标：应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
b) 测评对象：系统建设负责人和服务合同。
c) 测评实施包括以下内容：
   1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云计算平台及云服务商。
   2) 应核查云服务商提供的相关服务合同是否明确其云计算平台具有与所承载的业务应用系统具有相应或高于的安全保护能力。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-CMS2-02）

该测评单元包括以下要求：
a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标。
b) 测评对象：服务水平协议或服务合同。
c) 测评实施：应核查服务水平协议或服务合同是否规定了云服务的各项服务内容和具体指标等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS2-03）

该测评单元包括以下要求：
a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
b) 测评对象：服务水平协议或服务合同。
c) 测评实施：应核查服务水平协议或服务合同中是否规定了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS2-04）

该测评单元包括以下要求：
a) 测评指标：应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
b) 测评对象：服务水平协议或服务合同。

c) 测评实施：应核查服务水平协议或服务合同是否明确服务合约到期时，云服务商完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
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。

测评单元（L4-CMS2-05）

该测评单元包括以下要求：
a) 测评指标：应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。
b) 测评对象：保密协议或服务合同。
c) 测评实施：应核查保密协议或服务合同是否包含对云服务商不得泄露云服务客户数据的规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.2.6.2 供应链管理

测评单元（L4-CMS2-06）

该测评单元包括以下要求：
a) 测评指标：应确保供应商的选择符合国家有关规定。
b) 测评对象：记录表单类文档。
c) 测评实施：应核查云服务商的选择是否符合国家的有关规定。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS2-07）

该测评单元包括以下要求：
a) 测评指标：应将供应链安全事件信息或威胁信息及时传达到云服务客户。
b) 测评对象：供应链安全事件报告或威胁报告。
c) 测评实施：应核查供应链安全事件报告或威胁报告是否及时传达到云服务客户，报告是否明确相关事件信息或威胁信息。
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。

测评单元（L4-CMS2-08）

该测评单元包括以下要求：
a) 测评指标：应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。
b) 测评对象：供应商重要变更记录、安全风险评估报告和风险预案。
c) 测评实施：应核查供应商的重要变更是否及时传达到云服务客户，是否对每次供应商的重要变更都进行风险评估并采取控制措施。
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。

测评单元（L4-CMS2-09）

该测评单元包括以下要求：
a) 测评指标：**应分析外包服务或采购产品对云服务安全性的影响。（F4）**
b) 测评对象：云服务商所采购外包服务、产品。
c) 测评实施包括以下内容：
   1) 应核查云服务商是否分析外包服务或采购产品对云服务安全性的影响。
   2) 应核查是否具有分析外包服务或采购产品对云服务安全性的影响报告。

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

测评单元（L4-CMS2-10）

该测评单元包括以下要求：

a) 测评指标：**与供应商签订的服务水平协议中的相关指标，不低于拟与客户所签订的服务水平协议中的相关指标。（F4）**

b) 测评对象：云计算平台、供应商、服务水平协议。

c) 测评实施包括以下内容：

1) 应核查云服务商与供应商是否签订服务水平协议。

2) 应核查云服务商与云服务客户是否签订服务水平协议。

3) 应核查云服务商与供应商签订的服务水平协议中的相关指标是否不低于云服务商与云服务客户签订的服务水平协议中的相关指标。

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。

测评单元（L4-CMS2-11）

该测评单元包括以下要求：

a) 测评指标：**当变更供应商时，对供应商变更带来的安全风险进行评估，采取有效措施控制风险。（F4）**

b) 测评对象：云服务商和供应商变更相关的管理制度。

c) 测评实施包括以下内容：

1) 应核查云服务商在进行供应商变更时，是否对供应商变更带来的安全风险进行评估。

2) 应核查云服务商对供应商变更带来的安全风险进行评估后，是否采取有效措施控制风险。

3) 应核查是否具有相应的安全风险评估报告。

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。

8.2.7 安全运维管理

8.2.7.1 云计算环境管理

测评单元（L4-MMS2-01）

该测评单元包括以下要求：

a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

b) 测评对象：运维设备、运维地点、运维记录和相关管理文档。

c) 测评实施：应核查运维地点是否位于中国境内，从境外对境内云计算平台实施远程运维操作的行为是否遵循国家相关规定。

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

8.2.7.2 网络和系统安全管理

测评单元（L4-MMS2-02）

该测评单元包括以下要求：

a) 测评指标：**云服务商应制定相关策略，持续监控设备、资源、服务以及安全措施的有效性，并将安全措施有效性的监控结果定期提供给云服务客户。（F4）**

b) 测评对象：云服务商、云服务客户、相关安全策略。

c) 测评实施包括以下内容：

1) 应核查云服务商是否制定相关安全策略，并持续监控设备、资源、服务以及安全措施的有效性。
2) 应核查云服务商是否形成相应的监控记录。
3) 应核查云服务商是否形成安全措施有效性的监控结果。
4) 应核查云服务商是否定期将监控结果提供给云服务客户，并形成记录文档。

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。

8.2.7.3 应急预案管理

测评单元（L4-MMS2-03）

该测评单元包括以下要求：

a) 测评指标：**云服务提供商应将应急预案提前告知云服务客户。（F4）**
b) 测评对象：云服务商和应急预案。
c) 测评实施：应核查云服务提供商是否将应急预案提前告知云服务客户。
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。

8.3 移动互联安全测评扩展要求

8.3.1 安全物理环境

8.3.1.1 无线接入点的物理位置

测评单元（L4-PES3-01）

该测评单元包括以下要求：

a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。
b) 测评对象：无线接入设备。
c) 测评实施包括以下内容：
   1) 应核查物理位置与无线信号的覆盖范围是否合理。
   2) 应测试验证无线信号是否可以避免电磁干扰。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES3-02）

该测评单元包括以下要求：

a) 测评指标：**应为无线接入设备的安装选择合理位置，避免被非法破坏、替换。（F4）**
b) 测评对象：无线接入设备。
c) 测评实施包括以下内容：
   1) 应核查物理位置与无线信号的覆盖范围是否合理。
   2) 应核查是否采取防破坏、替换措施并定期检查。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2 安全通信网络

8.3.2.1 通信传输

测评单元（L4-CNS3-01）

该测评单元包括以下要求：

a) 测评指标：**应在移动终端与服务器之间建立安全的信息传输通道，例如使用有效安全版本的 TLS 或 IPSec 等协议。（F4）**

b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件的协议。
c) 测评实施：应劫持移动端与服务器之间传输协议，核查传输协议类型和版本是否安全。
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。

测评单元（L4-CNS3-02）

该测评单元包括以下要求：
a) 测评指标：**客户端应用软件与服务器应进行双向认证，可通过密钥、证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。（F4）**
b) 测评对象：客户端认证协议。
c) 测评实施包括以下内容：
1) 应核查客户端应用软件与服务器应是否采用双向协议。
2) 应核查认证方式是否为安全认证方式。
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。

测评单元（L4-CNS3-03）

该测评单元包括以下要求：
a) 测评指标：**通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术。（F4）**
b) 测评对象：客户端发起的资金类报文及保护措施。
c) 测评实施：应核查客户端应用软件发起的资金类交易报文是否具有抗抵赖措施。
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。

测评单元（L4-CNS3-04）

该测评单元包括以下要求：
a) 测评指标：**通过客户端应用软件发起的资金类交易报文或客户敏感信息变更报文，应能够防止重放攻击。（F4）**
b) 测评对象：客户端发起的身份认证或资金类报文及保护措施。
c) 测评实施：应通过获取客户端应用软件发起的资金类交易报文或客户敏感信息变更报文，发起重放攻击等方式，测试验证是否具有抗重放的机制。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3 安全区域边界

8.3.3.1 边界防护

测评单元（L4-ABS3-01）

该测评单元包括以下要求：
a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。
b) 测评对象：无线接入网关设备。
c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3.2 访问控制

测评单元（L4-ABS3-02）

该测评单元包括以下要求：

a) 测评指标：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证。
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。

8.3.3.3 入侵防范

测评单元（L3-ABS3-03）

该测评单元包括以下要求：

a) 测评指标：应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够检测非授权无线接入设备和移动终端的接入行为。
   2) 应测试验证是否能够检测非授权无线接入设备和移动终端的接入行为。
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。

测评单元（L4-ABS3-04）

该测评单元包括以下要求：

a) 测评指标：应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为。
b) 测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够对网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测。
   2) 应核查规则库版本是否及时更新。
d) 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-ABS3-05）

该测评单元包括以下要求：

a) 测评指标：应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态。
b) 测评对象：无线接入设备或相关组件。
c) 测评实施：应核查是否能够检测无线接入设备的SSID广播、WPS等高风险功能的开启状态。
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。

测评单元（L4-ABS3-06）

该测评单元包括以下要求：

a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等。
b) 测评对象：无线接入设备和无线接入网关设备。
c) 测评实施：应核查是否关闭了SSID广播、WEP认证等存在风险的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-ABS3-07）

该测评单元包括以下要求：

a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否分别使用了不同的鉴别密钥。
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。

测评单元（L4-ABS3-08）

该测评单元包括以下要求：

a) 测评指标：应能够阻断非授权无线接入设备或非授权移动终端。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够阻断非授权无线接入设备或非授权移动终端接入。
   2) 应测试验证是否能够阻断非授权无线接入设备或非授权移动终端接入。
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。

8.3.4 安全计算环境

8.3.4.1 移动终端管控

测评单元（L4-CES3-01）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、注册并运行终端管理客户端软件。
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施：应核查移动终端是否安装、注册并运行移动终端客户端软件。
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。

测评单元（L4-CES3-02）

该测评单元包括以下要求：

a) 测评指标：移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施包括以下内容：
   1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略。
   2) 应测试验证是否能够对移动终端进行远程锁定和远程擦除等。
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。

测评单元（L4-CES3-03）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端只用于处理指定业务。
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施：应核查移动终端是否只用于处理指定业务。
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。

8.3.4.2 移动应用管控

测评单元（L3-CES3-04）

该测评单元包括以下要求：

a) 测评指标：应具有选择应用软件安装、运行的功能。
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查是否具有选择应用软件安装、运行的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CES3-05）

该测评单元包括以下要求：

a) 测评指标：应只允许指定证书签名的应用软件安装和运行。
b) 测评对象：移动终端管理客户端。
c) 测评实施：应核查全部移动应用是否由指定证书签名。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CES3-06）

该测评单元包括以下要求：

a) 测评指标：应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。
b) 测评对象：移动终端管理客户端。
c) 测评实施包括以下内容：
   1) 应核查是否具有软件白名单功能。
   2) 应测试验证白名单功能是否能够控制应用软件安装、运行。
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。

测评单元（L4-CES3-07）

该测评单元包括以下要求：

a) 测评指标：应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。
b) 测评对象：移动终端。
c) 测评实施：应核查是否具有接受移动终端管理服务端远程管控的能力。
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。

8.3.4.3 访问控制

测评单元（L4-CES3-08）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。（F4）**
b) 测评对象：移动客户端权限。
c) 测评实施：应核查客户端应用软件向移动终端操作系统申请的权限是否是业务必须获取的权限。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CES3-09）

该测评单元包括以下要求：

a) 测评指标：**应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问。（F4）**
b) 测评对象：移动客户端权限。
c) 测评实施：应核查客户端应用软件数据是否仅能被授权用户或授权应用组件访问。

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。

测评单元（L4-CES3-10）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。（F4）**

b) 测评对象：移动客户端权限。

c) 测评实施包括以下内容：

1) 应核查客户端应用软件访问的文件和数据是否在授权范围。

2) 应核查客户端应用软件是否未访问非业务必需的文件和数据。

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。

8.3.4.4 安全审计

测评单元（L4-CES3-11）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文。（F4）**

b) 测评对象：运行日志。

c) 测评实施包括以下内容：

1) 应核查运行日志是否未打印支付敏感信息。

2) 应核查运行日志是否未打印完整的敏感数据原文。

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。

8.3.4.5 入侵防范

测评单元（L4-CES3-12）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件应配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统。（F4）**

b) 测评对象：移动客户端风险控制策略和措施。

c) 测评实施包括以下内容：

1) 应核查风险控制策略是否有对客户端软件的要求。

2) 应核查客户端软件是否上传相应的风险控制信息至风险控制系统。

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。

测评单元（L4-CES3-13）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件应对软件接口进行保护，防止其他应用对客户端应用软件接口进行非授权调用。（F4）**

b) 测评对象：移动客户端软件接口。

c) 测评实施：应核查客户端应用软件是否对软件接口进行保护，是否能防止其他应用对客户端应用软件接口进行非授权调用。

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。

测评单元（L4-CES3-14）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。（F4）**
b) 测评对象：移动客户端软件抗攻击能力。
c) 测评实施：应核查客户端应用软件是否具备基本的抗攻击能力，是否能抵御静态分析、动态调试等操作。
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。

测评单元（L4-CES3-15）

该测评单元包括以下要求：

a) 测评指标：**客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。（F4）**
b) 测评对象：移动客户端软件抗攻击能力。
c) 测评实施：应核查客户端应用软件是否具有代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。
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。

测评单元（L4-CES3-16）

该测评单元包括以下要求：

a) 测评指标：**客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。（F4）**
b) 测评对象：移动客户端软件防劫持能力。
c) 测评实施：应核查客户端应用软件在安装、启动、更新时是否对自身的完整性和真实性进行校验以抵御篡改、替换或劫持。
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。

8.3.5 安全建设管理

8.3.5.1 移动应用软件采购

测评单元（L4-CMS3-01）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
b) 测评对象：移动终端。
c) 测评实施：应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-CMS3-02）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件由指定的开发者开发。
b) 测评对象：移动终端。
c) 测评实施：应核查移动应用软件是否由指定的开发者开发。
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。

8.3.5.2 移动应用软件开发

测评单元（L4-CMS3-03）

该测评单元包括以下要求：

a) 测评指标：应对移动业务应用软件开发者进行资格审查。
b) 测评对象：系统建设负责人。
c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查。
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。

测评单元（L4-CMS3-04）

该测评单元包括以下要求：
a) 测评指标：应保证开发移动业务应用软件的签名证书合法性。
b) 测评对象：移动业务应用软件的签名证书。
c) 测评实施：应核查开发移动业务应用软件的签名证书是否具有合法性。
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。

8.3.6 安全运维管理

8.3.6.1 配置管理

测评单元（L4-MMS3-01）

该测评单元包括以下要求：
a) 测评指标：应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。
b) 测评对象：记录表单类文档、移动终端管理系统或相关组件。
c) 测评实施：应核查是否建立无线接入设备和合法移动终端配置库，并通过配置库识别非法设备。
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。

8.4 物联网安全测评扩展要求

8.4.1 安全物理环境

8.4.1.1 感知节点设备物理防护

测评单元（L4-PES4-01）

该测评单元包括以下要求：
a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动等，**使用环境与外壳保护等级（IP 代码）范围一致。（F4）**
b) 测评对象：感知节点设备所处物理环境、设计文档或验收文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备所处的物理环境、设计文档或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动、使用环境与外壳保护等级（IP 代码）等能力的说明，是否与实际情况一致。
   2) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动、外壳保护（IP 代码）等的防护措施。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES4-02）

该测评单元包括以下要求：
a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
b) 测评对象：感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容：
   1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致。
   2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES4-03）

该测评单元包括以下要求：
a) 测评指标：感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等。
b) 测评对象：感知节点设备所处物理环境和设计或验收文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备所处物理环境的设计或验收文档，是否具有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明，是否与实际情况一致。
   2) 应核查感知节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等防护措施。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES4-04）

该测评单元包括以下要求：
a) 测评指标：关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）。
b) 测评对象：关键感知节点设备的供电设备和设计或验收文档。
c) 测评实施包括以下内容：
   1) 应核查关键感知节点设备电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障关键感知节点设备长时间工作的电力供应措施。
   2) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。
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。

测评单元（L4-PES4-05）

该测评单元包括以下要求：
a) 测评指标：**感知节点设备的部署应遵循封闭性原则，降低设备被非法拆除、非法篡改的风险。（F4）**
b) 测评对象：感知节点所处物理环境和设计或验收文档。
c) 测评实施包括以下内容：
   1) 应核查关键感知节点设备所处环境是否遵循了封闭性原则。
   2) 应核查关键感知节点是否存在防止非法拆除的物理防护措施。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元的指标要求，否则不符合或部分符合本测评单元的指标要求。

8.4.1.2 感知网关节点设备物理安全要求

测评单元（L4-PES4-06）

该测评单元包括以下要求：
a) 测评指标：**感知网关节点设备应具有持久稳定的电力供应措施。（F4）**
b) 测评对象：感知网关节点设备的供电设备和设计或验收文档。
c) 测评实施包括以下内容：

1) 应核查感知网关节点设备电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障感知网关节点设备持久稳定工作的电力供应措施。
2) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。

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。

测评单元（L4-PES4-07）

该测评单元包括以下要求：

a) 测评指标：**应保证感知网关节点设备所在物理环境具有良好的信号收发能力（如避免信道遭遇屏蔽）。（F4）**
b) 测评对象：设计或验收文档和感知网关节点设备所处物理环境。
c) 测评实施包括以下内容：
   1) 应核查感知网关节点设备所处物理环境的设计或验收文档是否具有感知网关节点设备所处物理环境防强干扰、防屏蔽等能力的说明。
   2) 应核查感知网关节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等保护措施。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-PES4-08）

该测评单元包括以下要求：

a) 测评指标：**感知网关节点设备应具有定位装置。（F4）**
b) 测评对象：感知网关节点设备的功能和系统设计文档或产品白皮书。
c) 测评实施包括以下内容：
   1) 应核查感知网关节点设备是否有 GPS 或类似定位装置设备功能，是否采取了防强干扰、防阻挡屏蔽等措施。
   2) 应核查关键感知网关节点设备的定位功能是否有效和准确。
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。

8.4.2 安全区域边界

8.4.2.1 接入控制

测评单元（L4-ABS4-01）

该测评单元包括以下要求：

a) 测评指标：应保证只有授权的感知节点可以接入，**应保证感知节点、感知网关节点及处理应用层任意两者间相互鉴别和授权，非授权的感知节点、感知网关节点、处理应用层不能相互接入。（F4）**
b) 测评对象：感知节点设备、感知网关节点及处理应用层和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点、感知网关节点及处理应用层任意两者间是否可相互进行鉴别和授权，是否至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。
   2) 应对边界和感知层网络进行渗透测试，测试验证是否不存在绕过相关接入控制措施以及身份鉴别机制的方法。
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。

测评单元（L4-ABS4-02）

该测评单元包括以下要求：

a) 测评指标：**每个感知节点和感知网关节点应具备传感网络中唯一标识，且该标识不应被非授权访问所篡改。（F4）**

b) 测评对象：感知节点和感知网关节点设备的功能和系统设计文档、产品白皮书。
c) 测评实施包括以下内容：
   1) 应核查感知节点和感知网关节点设备的功能和系统设计文档、产品白皮书，是否可创建永久唯一标识符。
   2) 应核查感知节点和感知网关节点设备，创建的传感网络中唯一标识是否不可被非授权访问所篡改。
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。

测评单元（L4-ABS4-03）

该测评单元包括以下要求：
a) 测评指标：**具有指令接收功能的感知节点设备，应保证只有授权过的系统、终端可以对感知节点下发指令。（F4）**
b) 测评对象：感知节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备接入机制设计文档是否具有防止非法系统、终端设备下发指令的设计内容。
   2) 应对边界和感知层网络进行渗透测试，测试验证是否不存在非法下发指令的可能。
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。

测评单元（L4-ABS4-04）

该测评单元包括以下要求：
a) 测评指标：**由第三方平台提供感知节点、感知网关节点中转接入时，第三方平台的安全保护等级应不低于接入的物联网系统的安全保护等级。（F4）**
b) 测评对象：第三方平台和设计文档、安全保护等级报告。
c) 测评实施包括以下内容：
   1) 应核查第三方平台和设计文档、安全保护等级报告是否具有网络接入认证措施实现说明。
   2) 应核查第三方平台的安全保护等级是否不低于接入的物联网系统的安全保护等级。
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。

8.4.2.2 入侵防范

测评单元（L4-ABS4-05）

该测评单元包括以下要求：
a) 测评指标：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。
b) 测评对象：感知节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明。
   2) 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求。
   3) 应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
d) 单元判定：如果 1）至 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。

测评单元（L4-ABS4-06）

该测评单元包括以下要求：
a) 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

b) 测评对象：网关节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明。
   2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求。
   3) 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
d) 单元判定：如果1）至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。

测评单元（L4-ABS4-07）

该测评单元包括以下要求：
a) 测评指标：**当感知网关节点检测到攻击行为时，应上报攻击源IP、攻击类型、攻击时间等信息。（F4）**
b) 测评对象：网关节点设备和报警信息。
c) 测评实施包括以下内容：
   1) 应测试验证当感知网关节点受到攻击行为是否进行报警。
   2) 应测试验证报警信息是否包含攻击源IP、攻击类型、攻击时间等。
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。

测评单元（L4-ABS4-08）

该测评单元包括以下要求：
a) 测评指标：**可编程的感知节点、网关节点禁止运行未授权的代码。（F4）**
b) 测评对象：感知节点设备、网关节点设备的功能、系统设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备、网关节点设备是否有用户权限设置功能，并严格限制默认账户的权限。
   2) 应测试验证感知节点设备、网关节点设备是否可设置用户运行代码的权限。
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。

8.4.3 安全计算环境

8.4.3.1 感知节点设备安全

测评单元（L4-CES4-01）

该测评单元包括以下要求：
a) 测评指标：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。
b) 测评对象：感知节点设备。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更。
   2) 应通过试图接入和控制传感网访问未授权的资源等方式，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。
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。

测评单元（L4-CES4-02）

该测评单元包括以下要求：

a) 测评指标：应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F4）**
b) 测评对象：网关节点设备（包括读卡器）。
c) 测评实施包括以下内容：
   1) 应核查是否对连接的网关节点设备（包括读卡器）进行身份标识与鉴别，是否至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。
   2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
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。

测评单元（L4-CES4-03）

该测评单元包括以下要求：
a) 测评指标：应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F4）**
b) 测评对象：其他感知节点设备（包括路由节点）。
c) 测评实施包括以下内容：
   1) 应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数，是否至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。
   2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
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。

测评单元（L4-CES4-04）

该测评单元包括以下要求：
a) 测评指标：**应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F4）**
b) 测评对象：感知节点设备和系统设计文档。
c) 测评实施：应核查感知节点设备是否具备保存密码、密钥、设备标识等安全相关数据的安全单元。
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。

测评单元（L4-CES4-05）

该测评单元包括以下要求：
a) 测评指标：**针对可编程的感知节点设备，应进行代码安全审计。（F4）**
b) 测评对象：感知节点设备。
c) 测评实施：应核查针对可编程的感知节点设备是否进行了代码安全审计。
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。

8.4.3.2 网关节点设备安全

测评单元（L4-CES4-06）

该测评单元包括以下要求：
a) 测评指标：应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力，**能够对感知终端进行鉴别，至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F4）**
b) 测评对象：网关节点设备。
c) 测评实施包括以下内容：

1） 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心）进行标识并配置了鉴别功能，是否至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。
2） 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

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。

测评单元（L4-CES4-07）

该测评单元包括以下要求：

a） 测评指标：应具备过滤非法节点和伪造节点所发送的数据的能力。
b） 测评对象：网关节点设备。
c） 测评实施包括以下内容：
1） 应核查是否具备过滤非法节点和伪造节点发送的数据的功能。
2） 应测试验证是否能够过滤非法节点和伪造节点发送的数据。
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。

测评单元（L4-CES4-08）

该测评单元包括以下要求：

a） 测评指标：授权用户应能够在设备使用过程中对关键密钥进行在线更新。
b） 测评对象：感知节点设备。
c） 测评实施：应核查感知节点设备是否对其关键密钥进行在线更新。
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。

测评单元（L4-CES4-09）

该测评单元包括以下要求：

a） 测评指标：授权用户应能够在设备使用过程中对关键配置参数进行在线更新。
b） 测评对象：感知节点设备。
c） 测评实施：应核查是否支持对其关键配置参数进行在线更新及在线更新方式是否有效。
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。

测评单元（L4-CES4-10）

该测评单元包括以下要求：

a） 测评指标：**对于具有数据处理能力的网关节点设备，授权用户应能够在设备使用过程中对相关处理逻辑进行在线更新。（F4）**
b） 测评对象：网关节点设备。
c） 测评实施：对于具有数据处理能力的网关节点设备，应核查是否支持对相关处理逻辑进行在线更新，并核查在线更新方式是否有效。
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。

测评单元（L4-CES4-11）

该测评单元包括以下要求：

a） 测评指标：**对于具有数据处理能力的网关节点设备，应具备计算逻辑主动校验功能，防止处理逻辑被恶意篡改。（F4）**
b） 测评对象：网关节点设备。

c) 测评实施：对于具有数据处理能力的网关节点设备，应核查是否具备计算逻辑主动校验功能，并核查校验是否有效。
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。

测评单元（L4-CES4-12）

该测评单元包括以下要求：
a) 测评指标：**应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F4）**
b) 测评对象：感知节点设备和系统设计文档。
c) 测评实施：应核查感知节点设备是否具备保存密码、密钥、设备标识等安全相关数据的安全单元。
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。

测评单元（L4-CES4-13）

该测评单元包括以下要求：
a) 测评指标：**应进行代码安全审计。（F4）**
b) 测评对象：感知节点设备和系统设计文档。
c) 测评实施：应核查是否具有代码安全审计记录。
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。

8.4.3.3 抗数据重放

测评单元（L4-CES4-14）

该测评单元包括以下要求：
a) 测评指标：应能够鉴别数据的新鲜性，避免历史数据的重放攻击。
b) 测评对象：感知节点设备。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放。
   2) 应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。
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。

测评单元（L4-CES4-15）

该测评单元包括以下要求：
a) 测评指标：应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。
b) 测评对象：感知节点设备。
c) 测评实施包括以下内容：
   1) 应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施。
   2) 应测试验证是否能够避免数据的修改重放攻击。
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。

8.4.3.4 数据融合处理

测评单元（L4-CES4-16）

该测评单元包括以下要求：
a) 测评指标：应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。
b) 测评对象：物联网应用系统。

c) 测评实施包括以下内容：
   1) 应核查是否提供对来自传感网的数据进行数据融合处理的功能。
   2) 应测试验证数据融合处理功能是否能够处理不同种类的数据。
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。

测评单元（L4-CES4-17）

该测评单元包括以下要求：
a) 测评指标：应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令。
b) 测评对象：物联网应用系统。
c) 测评实施：应核查是否能够智能处理不同数据之间的依赖关系和制约关系。
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。

8.4.3.5 访问控制

测评单元（L4-CES4-18）

该测评单元包括以下要求：
a) 测评指标：**未经过鉴别和授权的感知节点、感知网关节点、处理应用层不应相互访问。（F4）**
b) 测评对象：感知节点设备、感知网关节点及处理应用层和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知节点、感知网关节点及处理应用层任意两者间是否相互进行鉴别和授权才能访问。
   2) 应核查感知节点、感知网关节点及处理应用层任意两者间是否设置了访问控制机制，机制是否覆盖访问资源及相关操作。
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。

8.4.4 安全运维管理

8.4.4.1 感知节点管理

测评单元（L4-MMS4-01）

该测评单元包括以下要求：
a) 测评指标：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护，**针对可编程的智能设备，应定期扫描处理逻辑、进行固件更新维护操作。（F4）**
b) 测评对象：维护记录、固件更新记录。
c) 测评实施包括以下内容：
   1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，是否对可编程的智能设备定期扫描处理逻辑、进行固件更新。
   2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS4-02）

该测评单元包括以下要求：
a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。
b) 测评对象：感知节点和网关节点设备安全管理文档。

c) 测评实施：应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

测评单元（L4-MMS4-03）

该测评单元包括以下要求：
a) 测评指标：应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。
b) 测评对象：感知节点设备、网关节点设备部署环境的管理制度。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备、网关节点设备部署环境管理文档是否包括负责核查和维护的人员调离工作岗位立即交还相关核查工具和核查维护记录等方面内容。
   2) 应核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS4-04）

该测评单元包括以下要求：
a) 测评指标：**应在经过充分测试评估后，在不影响感知节点、感知网关节点安全稳定运行的情况下进行补丁、固件更新等工作。（F4）**
b) 测评对象：补丁、固件更新管理制度和测评评估记录。
c) 测评实施包括以下内容：
   1) 应核查是否建立补丁、固件更新的操作规范等管理制度，明确进行补丁、固件更新前应经过充分测试评估。
   2) 应核查补丁、固件更新前是否有相应的测试评估记录。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

测评单元（L4-MMS4-05）

该测评单元包括以下要求：
a) 测评指标：**关键感知节点、感知网关节点应通过安全传输通道进行固件与补丁更新，在检测到异常时应能将结果上报至安全管理中心。（F4）**
b) 测评对象：关键感知节点、感知网关节点设备和系统设计文档。
c) 测评实施：应核查关键感知节点、感知网关节点设备是否通过安全传输通道进行固件与补丁更新并能将异常结果上报至安全管理中心。
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。

测评单元（L4-MMS4-06）

该测评单元包括以下要求：
a) 测评指标：**针对监控类的感知节点设备，应设置安全阈值，对如设备长时间静默、电压过低、仓库温湿度与噪音等环境要素超过安全范围等情况，进行在线预警。（F4）**
b) 测评对象：感知节点设备的功能和系统设计文档或产品白皮书。
c) 测评实施：应核查感知节点设备是否有设置安全阈值功能（如设备长时间静默、电压过低、仓库温湿度与噪音等要素），超过安全范围是否可进行在线预警。
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。

测评单元（L4-MMS4-07）

该测评单元包括以下要求：

a) 测评指标：**应对感知节点状态进行监测，发现异常时应定位处理。（F4）**

b) 测评对象：监测记录文档、监测数据分析报告。

c) 测评实施包括以下内容：

1) 应核查是否对感知节点设备状态进行监测，是否形成监测记录文档，是否组织人员对监测记录进行整理并保管。

2) 应核查发现异常时是否对监测记录进行分析、评审，形成监测数据分析报告并定位处理。

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。

9 整体测评

9.1 概述

等级保护对象整体测评应从安全控制点、安全控制点间和区域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区域间测评。

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。

安全控制点间测评是指对同一区域同一类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。

区域间测评是指对互连互通的不同区域之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。

9.2 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，则该安全控制点为符合，否则为不符合或部分符合。

9.3 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，应分析在同一类内，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，则对该测评指标的测评结果予以调整。

9.4 区域间测评

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，应进行区域间安全测评，重点分析等级保护对象中访问控制路径（如不同功能区域间的数据流流向和控制方式等）是否存在区域间的相互补充作用。

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，则对该测评指标的测评结果予以调整。

10 测评结论

10.1 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定级对象造成的安全风险。

10.2 等级测评结论

等级测评报告应给出等级保护对象的等级测评结论，确认等级保护对象达到相应等级保护要求的程度。应结合各类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) 符合：定级对象中未发现安全问题，等级测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为0，综合得分为100分。

b) 基本符合：定级对象中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致定级对象面临高等级安全风险，且综合得分不低于阈值。

c) 不符合：定级对象中存在安全问题，部分符合项和不符合项的统计结果不全为0，而且存在的安全问题会导致定级对象面临高等级安全风险，或者中低风险所占比例超过阈值。

附 录 A
（资料性附录）
测评力度

A.1 概述

测评力度是在等级测评过程中实施测评工作的力度，体现为测评工作的实际投入程度，具体由测评的广度和深度来反映。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工作投入。投入越多，测评力度就越强，测评效果就越有保证。

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，涉及访谈、核查和测试等三种基本测评方法。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：

——访谈深度：为简要、充分、较全面和全面等四种。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；

——核查深度：分别为简要、充分、较全面和全面等四种。简要核查主要是对功能性的文档、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，除了功能性的文档、机制和活动外，还适当需要一些总体或概要设计信息；较全面核查有详细、彻底分析、观察和研究，除了功能性的文档、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，除了功能性的文档、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；

——核查广度：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；

——测试深度：测试的深度体现在执行的测试类型上，包括功能测试、性能测试和渗透测试。功能测试和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；

——测试广度：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.2 等级测评力度

为了检验不同级别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。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。不同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，落实在不同单项测评中具体的测评实施上。

表 A.1 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级别的等级保护对象安全测评中的具体体现。

表 A.1　不同级别的等级保护对象的测评力度要求

测评力度	测评方法	第二级	第三级	第四级
广度	访谈	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
	核查			
	测试			
深度	访谈	充分	较全面	全面
	核查			
	测试	功能测试	功能测试和测试验证	功能测试和测试验证

从表 A.1 可以看到，对不同级别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。

对不同级别的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.1 的要求，以满足相应等级的测评力度要求。在确定测评对象时，应遵循以下原则：

——重要性，应抽查对被测定级对象来说重要的服务器、数据库和网络设备等；

——安全性，应抽查对外暴露的网络边界；

——共享性，应抽查共享设备和数据交换平台/设备；

——全面性，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类型；

——符合性，选择的设备、软件系统等应能符合相应等级的测评强度要求。

附 录 B
（资料性附录）
大数据可参考安全评估方法

B.1 第二级安全评估方法

金融行业大数据系统所定保护等级应不低于第三级，故本标准无第二级大数据安全评估内容。

B.2 第三级安全评估方法

B.2.1 安全物理环境

B.2.1.1 测评单元（BDS-L3-01）

该测评单元包括以下要求：

a) 测评指标：应保证承载大数据存储、处理和分析的设备机房位于中国境内。
b) 测评对象：大数据平台管理员和大数据平台建设方案。
c) 测评实施包括以下内容：
   1) 应访谈大数据平台管理员大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件是否均位于中国境内。
   2) 应核查大数据平台建设方案中是否明确大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件均位于中国境内。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.2 安全通信网络

B.2.2.1 测评单元（BDS-L3-01）

该测评单元包括以下要求：

a) 测评指标：应保证大数据平台不承载高于其安全保护等级的大数据应用。
b) 测评对象：大数据平台和业务应用系统定级材料。
c) 测评实施：应核查大数据平台和大数据平台承载的大数据应用系统相关定级材料，大数据平台安全保护等级是否不低于其承载的业务应用系统的安全保护等级。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

B.2.2.2 测评单元（BDS-L3-02）

该测评单元包括以下要求：

a) 测评指标：应保证大数据平台的管理流量与系统业务流量分离。
b) 测评对象：网络架构和大数据平台。
c) 测评实施包括以下内容：
   1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离。

2) 应核查大数据平台管理流量与大数据服务业务流量是否分离，核查所采取的技术手段和流量分离手段。
3) 应测试验证大数据平台管理流量与业务流量是否分离。

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。

B.2.3 安全计算环境

B.2.3.1 测评单元（BDS-L3-01）

该测评单元包括以下要求：

a) 测评指标：大数据平台应**对导入的数据源进行统一管理，并**对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。**（F3）**
b) 测评对象：大数据平台、数据采集终端、导入服务组件、业务应用系统、数据管理系统和系统管理软件等。
c) 测评实施包括以下内容：
   1) 应核查大数据应用的数据导入是否必须通过大数据平台的统一管控。
   2) 应测试数据源导入管控措施是否能够不被绕过。
   3) 应核查数据采集终端、用户或导入服务组件、数据导出终端、数据导出服务组件在登录时是否采用了身份鉴别措施。
   4) 应测试验证身份鉴别措施是否能够不被绕过。
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。

B.2.3.2 测评单元（BDS-L3-02）

该测评单元包括以下要求：

a) 测评指标:大数据平台应能对不同客户的大数据应用实施标识和鉴别,**身份标识应具有唯一性。（F3）**
b) 测评对象：大数据平台、大数据应用系统和系统管理软件等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台是否对大数据应用实施身份鉴别措施。
   2) 应测试验证身份鉴别措施是否能够不被绕过。
   3) 应测试验证身份标识是否具有唯一性，唯一性由应用用户名、IP、端口等因素确定，相同的身份标识会被合并管控。
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。

B.2.3.3 测评单元（BDS-L3-03）

该测评单元包括以下要求：

a) 测评指标：大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力。
b) 测评对象：大数据平台和大数据应用。
c) 测评实施包括以下内容：
   1) 应核查大数据平台是否为大数据应用提供计算和存储资源集中管控的模块,计算管控包含且不限于对 MapReduce、Spark、Storm、Presto、Flink 等计算框架的管控，存储资源管控包含且不限于对 HDFS、Kudu 等存储组件的管控。

2) 应建立大数据应用测试账户，核查大数据平台是否支持计算和存储资源集中监测和集中管控功能。

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。

B.2.3.4 测评单元（BDS-L3-04）

该测评单元包括以下要求：

a) 测评指标：大数据平台应对其提供的辅助工具或服务组件，实施有效管理，**包括注册/认证、权限设置、工具升级、注销。（F3）**

b) 测评对象：辅助工具、服务组件和大数据平台。

c) 测评实施包括以下内容：

1) 应核查提供的辅助工具或服务组件是否可以进行安装、部署、升级和卸载等。

2) 应核查提供的辅助工具或服务组件是否提供日志。

3) 应核查大数据平台是否采用技术手段或管理手段对辅助工具或服务组件进行统一管理，避免组件冲突。

4) 应核查大数据平台管控业务动作是否包含注册/认证、权限设置、工具升级、注销等环节而无遗漏。

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。

B.2.3.5 测评单元（BDS-L3-05）

该测评单元包括以下要求：

测评指标：大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行。

测评对象：大数据平台、设计文档、建设文档、计算节点和存储节点。

测评实施包括以下内容：

应核查设计文档或建设文档等是否具备屏蔽计算、内存、存储资源故障的措施和技术手段，措施手段应包含且不限于集群健康状态监控、负载均衡（软件/硬件）、故障恢复等。

应测试验证单一计算节点或存储节点关闭时，是否不影响业务正常运行。

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。

B.2.3.6 测评单元（BDS-L3-06）

该测评单元包括以下要求：

a) 测评指标：大数据平台应提供静态脱敏和去标识化的工具或服务组件技术，**静态脱敏包括采用统计、抑制、假名化、泛化、随机化等技术，大数据应用应根据需求对敏感数据进行展示屏蔽。（F3）**

b) 测评对象：设计或建设文档、大数据应用和大数据平台。

c) 测评实施包括以下内容：

1) 应核查大数据平台设计或建设文档是否具备数据静态脱密和去标识化措施或方案，如核查工具或服务组件是否具备配置不同的脱敏算法的能力。

2) 应核查静态脱敏和去标识化工具或服务组件是否进行了策略配置。

3) 应核查大数据平台是否为大数据应用提供静态脱敏和去标识化的工具或服务组件技术。

4) 应测试验证脱敏后的数据是否实现对敏感信息内容的屏蔽和隐藏，验证脱敏处理是否具备不可逆性。
5) 应测试验证脱敏算法是否至少包括统计、抑制、假名化、泛化、随机化等方法，并准确实现对应数据的脱敏处理。
6) 应测试验证大数据应用中的敏感数据展示内容是否为屏蔽后的数据内容。

d) 单元判定：如果 1）～6）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。

B.2.3.7 测评单元（BDS-L3-07）

该测评单元包括以下要求：

a) 测评指标：对外提供服务的大数据平台，平台或**内部其他系统**只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；**授权的颗粒度应达到表级或文件级。（F3）**
b) 测评对象：大数据平台、大数据应用系统、内部其他系统、数据管理系统和系统设计文档等。
c) 测评实施包括以下内容：
   1) 应核查是否由授权主体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，且授权颗粒度达到表级或文件级。
   3) 应测试验证是否不存在可越权访问情形。
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。

B.2.3.8 测评单元（BDS-L3-08）

该测评单元包括以下要求：

a) 测评指标：应**依据**数据分类分级安全管理**要求，针对大数据应用的数据提供相应的安全保护措施。（F3）**
b) 测评对象：大数据平台、大数据应用系统、数据管理系统和系统设计文档等。
c) 测评实施包括以下内容：
   1) 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略。
   2) 应核查大数据平台是否具有分类分级管理功能，是否依据分类分级策略对数据进行分类和等级划分，分类分级结果应可通过自动扫描或者手工指定，且分类分级应当与访问策略、加解密策略、脱敏策略等联动。
   3) 应核查大数据平台、大数据应用和数据管理系统等对不同类别级别的数据在标识、使用、传输和存储等方面是否采取不同安全防护措施，进而根据不同需要对关键数据进行重点防护。
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。

B.2.3.9 测评单元（BDS-L3-09）

该测评单元包括以下要求：

a) 测评指标：大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求。
b) 测评对象：大数据平台、数据管理系统和系统设计文档等。
c) 测评实施包括以下内容：

1） 应核查大数据平台是否依据安全策略对数据设置安全标记。
2） 应核查大数据平台是否为大数据应用提供基于安全标记的细粒度访问控制授权能力。
3） 应测试验证依据安全标记是否实现主体对客体细粒度的访问控制管理功能。

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。

B.2.3.10 测评单元（BDS-L3-10）

该测评单元包括以下要求：

a） 测评指标：大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证与安全保护策略保持一致。
b） 测评对象：大数据平台数据采集终端、导入服务组件、大数据应用系统、数据管理系统和系统管理软件等。
c） 测评实施包括以下内容：
1） 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略。
2） 应核查数据是否依据分类分级策略在数据采集、处理、分析过程中进行分类和等级划分。
3） 应核查是否采取有效措施保障机构内部数据安全保护策略的一致性。
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。

B.2.3.11 测评单元（BDS-L3-11）

该测评单元包括以下要求：

a） 测评指标：**应授予大数据平台的用户、工具或服务组件最小权限，实现组件的管理和服务权限分离，访问控制粒度应达到表级或文件级。（F3）**
b） 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。
c） 测评实施包括以下内容：
1） 应核查大数据平台或大数据应用系统是否能够对平台用户、工具、服务组件等进行权限设置。
2） 应核查权限控制措施是否实现最小化。
3） 应测试验证访问控制策略设置是否达到表级或文件级的控制粒度。
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。

B.2.3.12 测评单元（BDS-L3-12）

该测评单元包括以下要求：

a） 测评指标：**大数据平台在数据建模分析时，需确保敏感数据和个人金融信息位于安全区域，包括不限于数据隔离区、数据沙箱等。（F3）**
b） 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。
c） 测评实施包括以下内容：
1） 应核查大数据平台是否设置并使用了数据隔离区、数据沙箱等安全技术实现单独的系统安全区域。
2） 应核查大数据平台在数据建模分析时敏感数据和个人金融信息的处理和流转处理等均在安全域中。
3） 应测试验证安全区域的控制措施是否不被绕过。

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。

B.2.3.13 测评单元（BDS-L3-13）

该测评单元包括以下要求：

a) 测评指标：涉及重要数据接口、重要服务接口的调用，**应实施访问控制，访问权限在自有的授权管理机制基础上，实现细粒度的权限管控，如表级或文件级的授权控制，**包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。**（F3）**

b) 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。

c) 测评实施包括以下内容：

1) 应核查大数据平台或大数据应用系统是否面向重要数据接口、重要服务接口的调用提供有效访问控制措施，对重要数据接口和重要服务接口的调用是否可单独设置为高危预警行为，并对该调用行为可采取审计或阻断。

2) 应核查访问控制措施是否包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。

3) 应核查访问权限的设置是否实现细粒度的管控，达到表级。

4) 应测试验证访问控制措施是否不被绕过。

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。

B.2.3.14 测评单元（BDS-L3-14）

该测评单元包括以下要求：

a) 测评指标：应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复。

b) 测评对象：大数据平台、管理员、清洗和转换的数据、数据清洗和转换工具或脚本。

c) 测评实施包括以下内容：

1) 应访谈数据清洗转换相关管理员，询问数据清洗后是否较少出现失真或一致性破坏的情况。

2) 应核查清洗和转换的数据，重要数据清洗前后的字段或者内容是否具备一致性，能否避免数据失真。

3) 应核查数据清洗和转换工具或脚本，重要数据是否具备回滚机制等，在产生问题时可进行有效还原和恢复。

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。

B.2.3.15 测评单元（BDS-L3-15）

该测评单元包括以下要求：

a) 测评指标：**应对数据主体访问大数据平台进行限制，限制内容包含单次数据查看量、数据查看频次、总查看次数等。（F3）**

b) 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。

c) 测评实施包括以下内容：

1) 应核查数据主体访问大数据平台是否具备多层次的数据访问控制措施，是否支持单次数据查看量、数据查看频次、总查看次数等方面的管控和限制。

2） 应核查单次数据查看量、数据查看频次、总查看次数等设置是否无法被绕过。

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。

B.2.3.16 测评单元（BDS-L3-16）

该测评单元包括以下要求：

a） 测评指标：**针对大数据应用导出的数据文件，应根据安全需求对数据文件进行脱敏、水印或加密等。（F3）**

b） 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。

c） 测评实施包括以下内容：

1） 应核查大数据平台是否具备对数据文件进行脱敏、水印或加密的技术措施，是否可以通过策略的设定进行控制。

2） 应测试验证大数据应用导出的数据文件是否会进行脱敏、水印或加密。

3） 应核查上述数据文件的控制是否无法被绕过。

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。

B.2.3.17 测评单元（BDS-L3-17）

该测评单元包括以下要求：

a） 测评指标：应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求。

b） 测评对象：大数据平台、数据溯源措施或系统和大数据系统。

c） 测评实施包括以下内容：

1） 应核查数据溯源措施或系统是否对数据采集、处理、分析和挖掘等过程进行溯源。

2） 应核查重要业务数据处理流程是否包含在数据溯源范围中。

3） 应测试验证大数据平台是否对测试产生的数据采集、处理、分析或挖掘的过程进行了记录，是否可溯源测试过程。

4） 应核查是否能支撑数据业务要求，确保重要业务数据可溯源。

5） 对于自研发溯源措施或系统，应核查溯源数据能否满足合规审计要求。

6） 对于采购的溯源措施或系统，应核查系统是否符合国家产品和服务合规审计要求，溯源数据是否符合合规审计要求。

d） 单元判定：如果1）～6）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。

B.2.3.18 测评单元（BDS-L3-18）

该测评单元包括以下要求：

a） 测评指标：大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。

b） 测评对象：大数据平台、大数据应用的审计数据。

c） 测评实施包括以下内容：

1） 应核查对外提供服务的大数据平台，审计数据存储方式和不同大数据应用的审计数据是否隔离存放。

2） 应核查大数据平台是否提供不同客户审计数据收集汇总和集中分析的能力。

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。

B.2.4 安全建设管理

B.2.4.1 测评单元（BDS-L3-01）

该测评单元包括以下要求：

a) 测评指标：应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。

b) 测评对象：大数据应用建设负责人、大数据平台资质及安全服务能力报告和大数据平台服务合同等。

c) 测评实施包括以下内容：

1) 应访谈大数据应用建设负责人，所选择的大数据平台是否满足国家的有关规定。

2) 应查阅大数据平台相关资质及安全服务能力报告，大数据平台是否能为其所承载的大数据应用提供相应等级的安全保护能力。

3) 应核查大数据平台提供者的相关服务合同，大数据平台是否提供了其所承载的大数据应用相应等级的安全保护能力。

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。

B.2.4.2 测评单元（BDS-L3-02）

该测评单元包括以下要求：

a) 测评指标：应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。

b) 测评对象：服务合同、协议或服务水平协议、安全声明等。

c) 测评实施：应核查服务合同、协议或服务水平协议、安全声明等，是否规范了大数据平台提供者的权限与责任，覆盖管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等方面的内容；是否规定了大数据平台的各项服务内容（含安全服务）和具体指标、服务期限等，并有双方签字或盖章。

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。

B.2.4.3 测评单元（BDS-L3-03）

该测评单元包括以下要求：

a) 测评指标：应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

b) 测评对象：数据交换、共享策略和数据交换、共享合同、协议等。

c) 测评实施包括以下内容：

1) 应核查是否建立数据交换、共享的策略，确保内容覆盖对接收方安全防护能力的约束性要求。

2) 应核查数据交换、共享的合同或协议是否明确数据交换、共享的接收方对数据的保护责任。

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。

B.2.4.4 测评单元（BDS-L3-04）

该测评单元包括以下要求：

a) 测评指标：**大数据平台的安全整体规划和安全方案设计内容应包含所提供的数据安全防护能力，并形成配套文件，确保其安全规划符合网络安全法等国家法律法规相关要求。（F3）**

b) 测评对象：大数据应用建设负责人、大数据平台安全规划和方案等。

c) 测评实施包括以下内容：

1) 应核查大数据平台安全规划和设计方案等材料，是否详细描述了大数据平台的安全保护措施，是否符合网络安全法等国家法律法规相关要求。

2) 应核查大数据平台安全规划和方案的配套材料是否完备，包括实施管理办法、实施手册、专家评审意见等。

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。

B.2.5 安全运维管理

B.2.5.1 测评单元（BDS-L3-01）

该测评单元包括以下要求：

a) 测评指标：应**具备数字资产统一注册、管理和使用监控能力并**建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。**（F3）**

b) 测评对象：数字资产安全管理策略。

c) 测评实施包括以下内容：

1) 应核查是否具备技术手段对数字资产统一注册、管理和监控。

2) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确资产的安全管理目标、原则和范围。

3) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确各类数据全生命周期（包括并不限于数据采集、存储、处理、应用、流动、销毁等过程）的操作规范和保护措施，是否与数字资产的安全类别级别相符。

4) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确管理人员的职责。

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。

B.2.5.2 测评单元（BDS-L3-02）

该测评单元包括以下要求：

a) 测评指标：**应维护大数据平台使用和维护的数字资产清单，资产清单应包括资产的价值、所有人、管理员、使用者和安全等级等条目，并根据安全等级制定相应的安全保护措施。（F3）**

b) 测评对象：大数据应用建设负责人、数字资产清单、数字资产安全管理制度。

c) 测评实施包括以下内容：

1) 应访谈大数据应用建设负责人，大数据平台具有哪些数字资产。

2) 查阅是否具备数字资产清单，清单中是否包括资产的价值、所有人、管理员、使用者和安全等级等条目。

3) 应查阅数字资产清单的安全管理制度，制度中是否描述了对应等级的安全防护措施。

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

B.2.5.3 测评单元（BDS-L3-03）

该测评单元包括以下要求：

a) 测评指标：应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施。
b) 测评对象：数据分类分级保护策略。
c) 测评实施包括以下内容。
   1) 应核查大数据平台和大数据应用数据分类分级保护策略是否针对不同类别级别的数据制定不同的安全保护措施。
   2) 应核查数据操作记录是否按照大数据平台和大数据应用数据分类分级保护策略对数据实施保护。
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。

B.2.5.4 测评单元（BDS-L3-04）

该测评单元包括以下要求：

a) 测评指标：应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。
b) 测评对象：数据安全管理相关要求和大数据平台建设方案。
c) 测评实施包括以下内容：
   1) 应核查数据安全管理相关要求是否划分重要数字资产范围，是否明确重要数据自动脱敏或去标识的使用场景和业务处理流程。
   2) 应核查数据自动脱敏或去标识的使用场景和业务处理流程是否和管理要求相符。
d) 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.5.5 测评单元（BDS-L3-05）

该测评单元包括以下要求：

a) 测评指标：应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。
b) 测评对象：数据管理员、数据管理相关制度和数据变更记录表单。
c) 测评实施包括以下内容：
   1) 应访谈数据管理员，是否定期评审数据的类别和级别，如需要变更数据的类别或级别时，是否依据变更审批流程执行。
   2) 应核查数据管理相关制度，是否要求对数据的类别和级别进行定期评审，是否提出数据类别或级别变更的审批要求。
   3) 应核查数据变更记录表单，是否依据变更审批流程执行变更。
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。

B.2.5.6 测评单元（BDS-L3-06）

该测评单元包括以下要求：

a) **应建立数据安全管理规范，**对访问大数据平台的用户进行约束和规范。**（F3）**

b) 测评对象：数据管理员和数据管理相关制度。

c) 测评实施：应访谈数据管理员，是否制定大数据平台数据安全管理制度，对访问大数据平台的用户进行约束和规范。

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。

B.2.5.7 测评单元（BDS-L3-07）

该测评单元包括以下要求：

a) 测评指标：**重要、敏感数据的采集、传输、存储、处理、使用环境应严格控制开源、共享软件的使用，严控开源、共享软件的来源，并对其代码进行安全审计，确保安全、可靠。（F3）**

b) 测评对象：数据管理员和数据管理相关制度。

c) 测评实施包括以下内容：

1) 应访谈数据管理员，是否在重要、敏感数据的生命周期过程中使用了开源、共享等软件，并访谈软件的来源是否可靠，供应商是否符合法律法规要求。

2) 应核查数据管理相关制度，是否对开源、共享等软件的使用进行了规定。

3) 应核查是否具有开源、共享软件的代码审计报告（如使用 fortify 等自动化工具进行安全扫描的报告），并核查报告提及的高危漏洞是否进行了修补。

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。

B.3 第四级安全评估方法

B.3.1 安全物理环境

B.3.1.1 测评单元（BDS-L4-01）

该测评单元包括以下要求：

a) 测评指标：应保证承载大数据存储、处理和分析的设备机房位于中国境内。

b) 测评对象：大数据平台管理员和大数据平台建设方案。

c) 测评实施包括以下内容：

1) 应访谈大数据平台管理员大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件是否均位于中国境内。

2) 应核查大数据平台建设方案中是否明确大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件均位于中国境内。

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

B.3.2 安全通信网络

B.3.2.1 测评单元（BDS-L4-01）

该测评单元包括以下要求：

a) 测评指标：应保证大数据平台不承载高于其安全保护等级的大数据应用。

b) 测评对象：大数据平台和业务应用系统定级材料。
c) 测评实施：应核查大数据平台和大数据平台承载的大数据应用系统相关定级材料，大数据平台安全保护等级是否不低于其承载的业务应用系统的安全保护等级。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

B.3.2.2 测评单元（BDS-L4-02）

该测评单元包括以下要求：
a) 测评指标：应保证大数据平台的管理流量与系统业务流量分离。
b) 测评对象：网络架构和大数据平台。
c) 测评实施包括以下内容：
   1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离。
   2) 应核查大数据平台管理流量与大数据服务业务流量是否分离，核查所采取的技术手段和流量分离手段。
   3) 应测试验证大数据平台管理流量与业务流量是否分离。
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。

B.3.3 安全计算环境

B.3.3.1 测评单元（BDS-L4-01）

该测评单元包括以下要求：
a) 测评指标：大数据平台应**对导入的数据源进行统一管理，并**对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。**（F4）**
b) 测评对象：大数据平台、数据采集终端、导入服务组件、业务应用系统、数据管理系统和系统管理软件等。
c) 测评实施包括以下内容：
   1) 应核查大数据应用的数据导入是否必须通过大数据平台的统一管控。
   2) 应测试数据源导入管控措施是否能够不被绕过。
   3) 应核查数据采集终端、用户或导入服务组件、数据导出终端、数据导出服务组件在登录时是否采用了身份鉴别措施。
   4) 应测试验证身份鉴别措施是否能够不被绕过。
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。

B.3.3.2 测评单元（BDS-L4-02）

该测评单元包括以下要求：
a) 测评指标:大数据平台应能对不同客户的大数据应用实施标识和鉴别,**身份标识应具有唯一性。（F4）**
b) 测评对象：大数据平台、大数据应用系统和系统管理软件等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台是否对大数据应用实施身份鉴别措施。
   2) 应测试验证身份鉴别措施是否能够不被绕过。

3) 应测试验证身份标识是否具有唯一性，唯一性由应用用户名、IP、端口等因素确定，相同的身份标识会被合并管控。

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。

B.3.3.3 测评单元（BDS-L4-03）

该测评单元包括以下要求：

a) 测评指标：大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力。

b) 测评对象：大数据平台和大数据应用。

c) 测评实施包括以下内容：

1) 应核查大数据平台是否为大数据应用提供计算和存储资源集中管控的模块，计算管控包含且不限于对 MapReduce、Spark、Storm、Presto、Flink 等计算框架的管控，存储资源管控包含且不限于对 HDFS、Kudu 等存储组件的管控。

2) 应建立大数据应用测试账户，核查大数据平台是否支持计算和存储资源集中监测和集中管控功能。

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。

B.3.3.4 测评单元（BDS-L4-04）

该测评单元包括以下要求：

a) 测评指标：大数据平台应对其提供的辅助工具或服务组件，实施有效管理，**包括注册/认证、权限设置、工具升级、注销。（F4）**

b) 测评对象：辅助工具、服务组件和大数据平台。

c) 测评实施包括以下内容：

1) 应核查提供的辅助工具或服务组件是否可以进行安装、部署、升级和卸载等。

2) 应核查提供的辅助工具或服务组件是否提供日志。

3) 应核查大数据平台是否采用技术手段或管理手段对辅助工具或服务组件进行统一管理，避免组件冲突。

4) 应核查大数据平台管控业务动作是否包含注册/认证、权限设置、工具升级、注销等环节而无遗漏。

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。

B.3.3.5 测评单元（BDS-L4-05）

该测评单元包括以下要求：

a) 测评指标：大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行。

b) 测评对象：大数据平台、设计文档、建设文档、计算节点和存储节点。

c) 测评实施包括以下内容：

1) 应核查设计文档或建设文档等是否具备屏蔽计算、内存、存储资源故障的措施和技术手段，措施手段包含且不限于集群健康状态监控、负载均衡（软件/硬件）、故障恢复等。

2) 应测试验证单一计算节点或存储节点关闭时，是否不影响业务正常运行。

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。

B.3.3.6 测评单元（BDS-L4-06）

该测评单元包括以下要求：

a) 测评指标：大数据平台应提供静态脱敏和去标识化的工具或服务组件技术，**静态脱敏包括采用统计、抑制、假名化、泛化、随机化等技术，大数据应用应根据需求对敏感数据进行展示屏蔽。（F4）**

b) 测评对象：设计或建设文档、大数据应用和大数据平台。

c) 测评实施包括以下内容：

1) 应核查大数据平台设计或建设文档是否具备数据静态脱密和去标识化措施或方案，如核查工具或服务组件是否具备配置不同的脱敏算法的能力。

2) 应核查静态脱敏和去标识化工具或服务组件是否进行了策略配置。

3) 应核查大数据平台是否为大数据应用提供静态脱敏和去标识化的工具或服务组件技术。

4) 应测试验证脱敏后的数据是否实现对敏感信息内容的屏蔽和隐藏，验证脱敏处理是否具备不可逆性。

5) 应测试验证脱敏算法至少应该包括统计、抑制、假名化、泛化、随机化等方法，并准确实现对应数据的脱敏处理。

6) 应测试验证大数据平台可以实现数据流出的数据实时、透明脱敏，大数据应用中的敏感数据展示内容为屏蔽后的数据内容。

d) 单元判定：如果 1）～6）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。

B.3.3.7 测评单元（BDS-L4-07）

该测评单元包括以下要求：

a) 测评指标：对外提供服务的大数据平台，平台或**内部其他系统**只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；**授权的颗粒度应达到记录或字段级。（F4）**

b) 测评对象：大数据平台、大数据应用系统、内部其他系统、数据管理系统和系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否由授权主体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，且授权颗粒度达到记录或字段级。

3) 应测试验证是否不存在可越权访问情形。

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。

B.3.3.8 测评单元（BDS-L4-08）

该测评单元包括以下要求：

a) 测评指标：应**依据**数据分类分级安全管理**要求，针对大数据应用的数据提供相应的安全保护措施。（F4）**

b) 测评对象：大数据平台、大数据应用系统、数据管理系统和系统设计文档等。

c) 测评实施包括以下内容：

1) 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略。

2) 应核查大数据平台是否具有分类分级管理功能，是否依据分类分级策略对数据进行分类和等级划分，分类分级结果应可通过自动扫描或者手工指定，且分类分级应当与访问策略、加解密策略、脱敏策略等联动。
3) 应核查大数据平台、大数据应用和数据管理系统等对不同类别级别的数据，是否可以在合理安全访问的基础上对数据进行跟踪和标识。

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。

B.3.3.9 测评单元（BDS-L4-09）

该测评单元包括以下要求：

a) 测评指标：大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求，**访问控制粒度达到记录或字段级。（F4）**
b) 测评对象：大数据平台、数据管理系统和系统设计文档等。
c) 测评实施包括以下内容：
1) 应核查大数据平台是否依据安全策略对数据设置安全标记。
2) 应核查大数据平台是否为大数据应用提供基于安全标记的细粒度访问控制授权能力。
3) 应测试验证依据安全标记是否实现主体对客体细粒度的访问控制管理功能。
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。

B.3.3.10 测评单元（BDS-L4-10）

该测评单元包括以下要求：

a) 测评指标：大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证与安全保护策略保持一致。
b) 测评对象：大数据平台数据采集终端、导入服务组件、大数据应用系统、数据管理系统和系统管理软件等。
c) 测评实施包括以下内容：
1) 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略。
2) 应核查数据是否依据分类分级策略在数据采集、处理、分析过程中进行分类和等级划分。
3) 应核查是否采取有效措施保障机构内部数据安全保护策略的一致性。
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。

B.3.3.11 测评单元（BDS-L4-11）

该测评单元包括以下要求：

a) 测评指标：**应授予大数据平台的用户、工具或服务组件最小权限，实现组件的管理和服务权限分离，访问控制粒度应达到记录或字段级。（F4）**
b) 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。
c) 测评实施包括以下内容：
1) 应核查大数据平台或大数据应用系统是否能够对平台用户、工具、服务组件等进行权限设置。
2) 应核查权限控制措施是否实现最小化。

3） 应测试验证访问控制策略设置是否达到记录或字段级的控制粒度。

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。

B.3.3.12 测评单元（BDS-L4-12）

该测评单元包括以下要求：

a） 测评指标：**大数据平台在数据建模分析时，需确保敏感数据和个人金融信息位于安全区域，包括但不限于数据隔离区、数据沙箱等。（F4）**

b） 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。

c） 测评实施包括以下内容：

1） 应核查大数据平台是否设置并使用了数据隔离区、数据沙箱等安全技术实现单独的系统安全区域。

2） 应核查大数据平台在数据建模分析时敏感数据和个人金融信息的处理和流转处理等是否均在安全域中。

3） 应测试验证安全区域的控制措施是否不被绕过。

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。

B.3.3.13 测评单元（BDS-L4-13）

该测评单元包括以下要求：

a） 测评指标：涉及重要数据接口、重要服务接口的调用，应实施访问控制，**访问权限在自有的授权管理机制基础上，实现细粒度的权限管控，如记录或字段级的授权控制，**包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。**（F4）**

b） 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。

c） 测评实施包括以下内容：

1） 应核查大数据平台或大数据应用系统是否面向重要数据接口、重要服务接口的调用提供有效访问控制措施，对重要数据接口和重要服务接口的调用应可单独设置为高危预警行为，并对该调用行为可采取审计或阻断。

2） 应核查访问控制措施是否包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。

3） 应核查访问权限的设置是否实现细粒度的管控，达到记录或字段级。

4） 应测试验证访问控制措施是否不被绕过。

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。

B.3.3.14 测评单元（BDS-L4-14）

该测评单元包括以下要求：

a） 测评指标：应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复。

b） 测评对象：大数据平台、管理员、清洗和转换的数据、数据清洗和转换工具或脚本。

c） 测评实施包括以下内容：

1） 应访谈数据清洗转换相关管理员，询问数据清洗后是否较少出现失真或一致性破坏的情况。
2） 应核查清洗和转换的数据，重要数据清洗前后的字段或者内容是否具备一致性，能否避免数据失真。
3） 应核查数据清洗和转换工具或脚本，重要数据是否具备回滚机制等，在产生问题时可进行有效还原和恢复。

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。

B.3.3.15 测评单元（BDS-L4-15）

该测评单元包括以下要求：

a） 测评指标：**应对数据主体访问大数据平台进行限制，限制内容包含单次数据查看量、数据查看频次、总查看次数等。（F4）**
b） 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。
c） 测评实施包括以下内容：
1） 应核查数据主体访问大数据平台是否具备多层次的数据访问控制措施，是否支持单次数据查看量、数据查看频次、总查看次数等方面的管控和限制。
2） 应核查单次数据查看量、数据查看频次、总查看次数等设置是否无法被绕过。
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。

B.3.3.16 测评单元（BDS-L4-16）

该测评单元包括以下要求：

a） 测评指标：**针对大数据应用导出的数据文件，应根据安全需求对数据文件进行脱敏、水印或加密等。（F4）**
b） 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。
c） 测评实施包括以下内容：
1） 应核查大数据平台是否具备对数据文件进行脱敏、水印或加密的技术措施，是否可以通过策略的设定进行控制。
2） 应测试验证大数据应用导出的数据文件是否会进行脱敏、水印或加密。
3） 应核查上述数据文件的控制是否无法被绕过。
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。

B.3.3.17 测评单元（BDS-L4-17）

该测评单元包括以下要求：

a） 测评指标：应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求。
b） 测评对象：大数据平台、数据溯源措施或系统和大数据系统。
c） 测评实施包括以下内容：
1） 应核查数据溯源措施或系统是否对数据采集、处理、分析和挖掘等过程进行溯源。
2） 应核查重要业务数据处理流程是否包含在数据溯源范围中。

3) 应测试验证大数据平台是否对测试产生的数据采集、处理、分析或挖掘的过程进行了记录，是否可溯源测试过程。
4) 应核查是否能支撑数据业务要求，确保重要业务数据可溯源。
5) 对于自研发溯源措施或系统，应核查溯源数据能否满足合规审计要求。
6) 对于采购的溯源措施或系统，应核查系统是否符合国家产品和服务合规审计要求，溯源数据是否符合合规审计要求。

d) 单元判定：如果 1）～6）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。

B.3.3.18 测评单元（BDS-L4-18）

该测评单元包括以下要求：

a) 测评指标：大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。
b) 测评对象：大数据平台、大数据应用的审计数据。
c) 测评实施包括以下内容：
1) 应核查对外提供服务的大数据平台，审计数据存储方式和不同大数据应用的审计数据是否隔离存放。
2) 应核查大数据平台是否提供不同客户审计数据收集汇总和集中分析的能力。
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。

B.3.4 安全建设管理

B.3.4.1 测评单元（BDS-L4-01）

该测评单元包括以下要求：

a) 测评指标：应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。
b) 测评对象：大数据应用建设负责人、大数据平台资质及安全服务能力报告和大数据平台服务合同等。
c) 测评实施包括以下内容：
1) 应访谈大数据应用建设负责人，所选择的大数据平台是否满足国家的有关规定。
2) 应查阅大数据平台相关资质及安全服务能力报告，大数据平台是否能为其所承载的大数据应用提供相应等级的安全保护能力。
3) 应核查大数据平台提供者的相关服务合同，大数据平台是否提供了其所承载的大数据应用相应等级的安全保护能力。
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。

B.3.4.2 测评单元（BDS-L4-02）

该测评单元包括以下要求：

a) 测评指标：应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。
b) 测评对象：服务合同、协议或服务水平协议、安全声明等。

c) 测评实施：应核查服务合同、协议或服务水平协议、安全声明等，是否规范了大数据平台提供者的权限与责任，覆盖管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等方面的内容；是否规定了大数据平台的各项服务内容（含安全服务）和具体指标、服务期限等，并有双方签字或盖章。

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。

B.3.4.3 测评单元（BDS-L4-03）

该测评单元包括以下要求：

a) 测评指标：应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

b) 测评对象：数据交换、共享策略和数据交换、共享合同、协议等。

c) 测评实施包括以下内容：

1) 应核查是否建立数据交换、共享的策略，确保内容覆盖对接收方安全防护能力的约束性要求。

2) 应核查数据交换、共享的合同或协议是否明确数据交换、共享的接收方对数据的保护责任。

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。

B.3.4.4 测评单元（BDS-L4-04）

该测评单元包括以下要求：

a) 测评指标：**大数据平台的安全整体规划和安全方案设计内容应包含所提供的数据安全防护能力，并形成配套文件，确保其安全规划符合网络安全法等国家法律法规相关要求。（F4）**

b) 测评对象：大数据应用建设负责人、大数据平台安全规划和方案等。

c) 测评实施包括以下内容：

1) 应核查大数据平台安全规划和设计方案等材料，是否详细描述了大数据平台的安全保护措施，是否符合网络安全法等国家法律法规相关要求。

2) 应核查大数据平台安全规划和方案的配套材料是否完备，包括实施管理办法、实施手册、专家评审意见等。

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。

B.3.5 安全运维管理

B.3.5.1 测评单元（BDS-L4-01）

该测评单元包括以下要求：

a) 测评指标：应**具备数字资产统一注册、管理和使用监控能力并**建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。**（F4）**

b) 测评对象：数字资产安全管理策略。

c) 测评实施包括以下内容：

1) 应核查是否具备技术手段对数字资产统一注册、管理和监控。

2) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确资产的安全管理目标、原则和范围。
3) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确各类数据全生命周期（包括并不限于数据采集、存储、处理、应用、流动、销毁等过程）的操作规范和保护措施，是否与数字资产的安全类别级别相符。
4) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确管理人员的职责。

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。

B.3.5.2 测评单元（BDS-L4-02）

该测评单元包括以下要求：

a) 测评指标：**应维护大数据平台使用和维护的数字资产清单，资产清单应包括资产的价值、所有人、管理员、使用者和安全等级等条目，并根据安全等级制定相应的安全保护措施。（F4）**
b) 测评对象：大数据应用建设负责人、数字资产清单、数字资产安全管理制度。
c) 测评实施包括以下内容：
1) 应访谈大数据应用建设负责人，是否知晓大数据平台具有哪些数字资产。
2) 查阅是否具备数字资产清单，清单中是否包括资产的价值、所有人、管理员、使用者和安全等级等条目。
3) 应查阅数字资产清单的安全管理制度，制度中是否描述了对应等级的安全防护措施。
d) 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.3.5.3 测评单元（BDS-L4-03）

该测评单元包括以下要求：

a) 测评指标：应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施。
b) 测评对象：数据分类分级保护策略。
c) 测评实施包括以下内容：
1) 应核查大数据平台和大数据应用数据分类分级保护策略是否针对不同类别级别的数据制定不同的安全保护措施。
2) 应核查数据操作记录是否按照大数据平台和大数据应用数据分类分级保护策略对数据实施保护。
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。

B.3.5.4 测评单元（BDS-L4-04）

该测评单元包括以下要求：

a) 测评指标：应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。
b) 测评对象：数据安全管理相关要求和大数据平台建设方案。
c) 测评实施包括以下内容：
1) 应核查数据安全管理相关要求是否划分重要数字资产范围，是否明确重要数据自动脱敏或去标识的使用场景和业务处理流程。

2） 应核查数据自动脱敏或去标识的使用场景和业务处理流程是否和管理要求相符。

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

B.3.5.5 测评单元（BDS-L4-05）

该测评单元包括以下要求：

a） 测评指标：应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

b） 测评对象：数据管理员、数据管理相关制度和数据变更记录表单。

c） 测评实施包括以下内容：

1） 应访谈数据管理员，是否定期评审数据的类别和级别，如需要变更数据的类别或级别时，是否依据变更审批流程执行。

2） 应核查数据管理相关制度，是否要求对数据的类别和级别进行定期评审，是否提出数据类别或级别变更的审批要求。

3） 应核查数据变更记录表单，是否依据变更审批流程执行变更。

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。

B.3.5.6 测评单元（BDS-L4-06）

该测评单元包括以下要求：

a） 测评指标：**应建立数据安全管理规范，对访问大数据平台的用户进行约束和规范。（F4）**

b） 测评对象：数据管理员和数据管理相关制度。

c） 测评实施：应访谈数据管理员，是否制定大数据平台数据安全管理制度，对访问大数据平台的用户进行约束和规范。

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。

B.3.5.7 测评单元（BDS-L4-07）

该测评单元包括以下要求：

a） 测评指标：**重要、敏感数据的采集、传输、存储、处理、使用环境应严格控制开源、共享软件的使用，严控开源、共享软件的来源，并对其代码进行安全审计，确保安全、可靠。（F4）**

b） 测评对象：数据管理员和数据管理相关制度。

c） 测评实施包括以下内容：

1） 应访谈数据管理员，是否在重要、敏感数据的生命周期过程中使用了开源、共享等软件，并访谈软件的来源是否可靠，供应商是否符合法律法规要求。

2） 应核查数据管理相关制度，是否对开源、共享等软件的使用进行了规定。

3） 应核查是否具有开源、共享软件的代码审计报告（如使用 fortify 等自动化工具进行安全扫描的报告），并核查报告提及的高危漏洞是否进行了修补。

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。

附 录 C
（规范性附录）
测评单元编号说明

C.1 测评单元编码规则

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 2 位组成，第 1 位为字母 L，第 2 位为数字，其中 2 为第二级，3 为第三级，4 为第四级。

第 2 组由 4 位组成，前 3 位为字母，第 4 位为数字。字母代表类：PES 为安全物理环境，CNS 为安全通信网络，ABS 为安全区域边界，CES 为安全计算环境，SMC 为安全管理中心，PSS 为安全管理制度，ORS 为安全管理机构，HRS 为安全管理人员，CMS 为安全建设管理，MMS 为安全运维管理，详细缩写说明见 C.3。数字代表应用场景：1 为安全测评通用要求部分，2 为云计算安全测评扩展要求部分，3 为移动互联安全测评扩展要求部分，4 为物联网安全测评扩展要求部分。

第 3 组由 2 位数字组成，按类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 L2-PES1-01，代表源自安全测评通用要求部分的第二级安全物理环境类的第 1 个指标。

C.2 大数据可参考安全评估方法编号说明

测评单元编号为三组数据，格式为 XXX—XX—XXX，各组含义和编码规则如下：

第 1 组由 3 位组成，BDS 代表大数据可参考安全评估方法。

第 2 组由 2 位组成，第 1 位为字母 L，第 2 位为数字，其中 2 为第二级，3 为第三级，4 为第四级。

第 3 组由 2 位数字组成，按照基本要求中的安全控制措施进行顺序编号。

示例：测评单元编号为 BDS-L2-01，代表源自大数据可参考安全评估方法的第二级的第 1 个指标。

C.3 专用缩略语

下列专用缩略语适用于本文件。

ABS：安全区域边界（Area Boundary Security）

BDS：大数据系统（Big Data System）

CES：安全计算环境（Computing Environment Security）

CMS：安全建设管理（Construction Management Security）

CNS：安全通信网络（Communication Network Security）

MMS：安全运维管理（Maintenance Management Security）

ORS：安全管理机构（Organization and Resource Security）

PES：安全物理环境（Physical Environment Security）

PSS：安全管理制度（Policy and System Security）

HRS：安全管理人员（Human Resource Security）

SMC：安全管理中心（Security Management Center）

参 考 文 献

[1] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[2] 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
[3] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
[4] GB/T 37721—2019 信息安全技术 信息技术大数据分析系统功能要求
[5] GB/T 37093—2018 信息安全技术 物联网感知层接入通信网的安全要求
[6] JR/T 0011 银行集中式数据中心规范
[7] JR/T 0013 金融业星型网间互联安全规范
[8] JR/T 0023 证券公司信息技术管理规范
[9] JR/T 0026 银行业计算机信息系统雷电防护技术规范
[10] JR/T 0044 银行业信息系统灾难恢复管理规范
[11] JR/T 0055.4 银行联网联合技术规范第4部分：数据安全传输控制
[12] JR/T 0060 证券期货业信息系统安全等级保护基本要求
[13] JR/T 0067 证券期货业信息系统安全等级保护测评要求
[14] JR/T 0068—2020 网上银行系统信息安全通用规范
[15] JR/T 0166—2018 云计算技术金融应用规范 技术架构
[16] JR/T 0167—2018 云计算技术金融应用规范 安全技术要求
[17] 中国证券业协会.证券公司集中交易安全管理技术指引（中证协发〔2006〕81号），2006-08-01
[18] 中国证券业协会.证券营业部信息技术指引（中证协发〔2009〕154号），2009-09-07
[19] 中国保监会.保险业重大突发事件应急处理规定（保监会令〔2003〕3号），2003-12-18