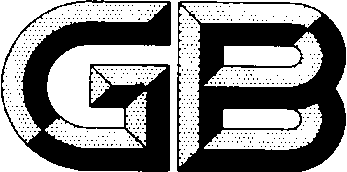
ICS 35.040

L80



中华人民共和国国家标准

GB/T 28448.3—XXXX

|  |
| --- |
|  |

信息安全技术

网络安全等级保护测评要求

第3部分：移动互联安全扩展要求

Information security technology-

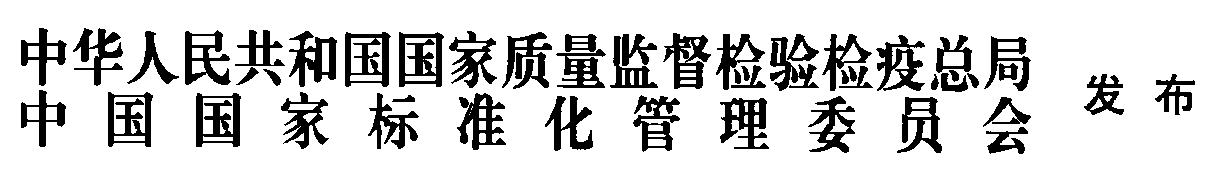
Evaluation requirement for cybersecurity classified protection

Part3：Special security requirements for the mobile interconnection

|  |
| --- |
|  |
|  |

XXXX - XX - XX发布

XXXX - XX - XX实施

1. 

目  次

[前言 VII](#_Toc465867189)

[引言 VIII](#_Toc465867190)

[1　范围 1](#_Toc465867191)

[2　规范性引用文件 1](#_Toc465867192)

[3　术语和定义 1](#_Toc465867193)

[3.1 1](#_Toc465867194)

[3.2 1](#_Toc465867195)

[3.3 1](#_Toc465867196)

[3.4 1](#_Toc465867197)

[3.5 2](#_Toc465867198)

[4　安全等级保护测评概述 2](#_Toc465867199)

[4.1　安全等级保护测评方法 2](#_Toc465867200)

[4.2　单项测评和整体测评 2](#_Toc465867201)

[5　第一级测评要求 2](#_Toc465867202)

[5.1　安全技术单项测评 2](#_Toc465867203)

[5.1.1　物理和环境安全 2](#_Toc465867204)

[5.1.1.1　物理位置选择 2](#_Toc465867205)

[5.1.2　网络和通信安全 3](#_Toc465867206)

[5.1.2.1　结构安全 3](#_Toc465867207)

[5.1.2.2　边界防护 4](#_Toc465867208)

[5.1.2.3　访问控制 4](#_Toc465867209)

[5.1.2.4　通信完整性和保密性 4](#_Toc465867210)

[5.1.3　设备和计算安全 5](#_Toc465867211)

[5.1.3.1　身份鉴别 5](#_Toc465867212)

[5.1.3.2　应用管控 5](#_Toc465867213)

[5.1.3.3　入侵防范 6](#_Toc465867214)

[5.1.3.4　恶意代码防范 6](#_Toc465867215)

[5.1.4　应用和数据安全 6](#_Toc465867216)

[5.2　安全管理单项测评 7](#_Toc465867217)

[5.2.1　安全策略和管理制度 7](#_Toc465867218)

[5.2.1.1　管理制度 7](#_Toc465867219)

[5.2.2　安全管理机构和人员 7](#_Toc465867220)

[5.2.2.1　岗位设置 7](#_Toc465867221)

[5.2.2.2　安全意识教育和培训 7](#_Toc465867222)

[5.2.3　安全建设管理 8](#_Toc465867223)

[5.2.3.1　安全方案设计 8](#_Toc465867224)

[5.2.3.2　产品采购和使用 8](#_Toc465867225)

[5.2.3.3　工程实施 8](#_Toc465867226)

[5.2.3.4　测试验收 9](#_Toc465867227)

[5.2.3.5　系统交付 9](#_Toc465867228)

[5.2.3.6　安全服务商选择 10](#_Toc465867229)

[5.2.4　安全运维管理 10](#_Toc465867230)

[5.2.4.1　设备维护管理 10](#_Toc465867231)

[5.2.4.2　漏洞和风险管理 11](#_Toc465867232)

[5.2.4.3　应用软件来源管理 11](#_Toc465867233)

[5.2.4.4　恶意代码防范管理 12](#_Toc465867234)

[5.2.4.5　备份与恢复管理 12](#_Toc465867235)

[6　第二级测评要求 13](#_Toc465867236)

[6.1　安全技术单项测评 13](#_Toc465867237)

[6.1.1　物理和环境安全 13](#_Toc465867238)

[6.1.1.1　物理位置选择 13](#_Toc465867239)

[6.1.2　网络和通信安全 13](#_Toc465867240)

[6.1.2.1　结构安全 13](#_Toc465867241)

[6.1.2.2　边界防护 14](#_Toc465867242)

[6.1.2.3　访问控制 14](#_Toc465867243)

[6.1.2.4　入侵防范 15](#_Toc465867244)

[6.1.2.5　通信完整性和保密性 16](#_Toc465867245)

[6.1.2.6　安全审计 17](#_Toc465867246)

[6.1.2.7　网络设备防护 18](#_Toc465867247)

[6.1.3　设备和计算安全 18](#_Toc465867248)

[6.1.3.1　身份鉴别 19](#_Toc465867249)

[6.1.3.2　应用管控 19](#_Toc465867250)

[6.1.3.3　入侵防范 20](#_Toc465867251)

[6.1.3.4　恶意代码防范 21](#_Toc465867252)

[6.1.3.5　资源控制 21](#_Toc465867253)

[6.1.4　应用和数据安全 22](#_Toc465867254)

[6.1.4.1　身份鉴别 22](#_Toc465867255)

[6.1.4.2　软件审核与检测 23](#_Toc465867256)

[6.1.4.3　数据完整性 23](#_Toc465867257)

[6.1.4.4　数据保密性 24](#_Toc465867258)

[6.2　安全管理单项测评 25](#_Toc465867259)

[6.2.1　安全策略和管理制度 25](#_Toc465867260)

[6.2.1.1　管理制度 25](#_Toc465867261)

[6.2.2　安全管理机构和人员 26](#_Toc465867262)

[6.2.2.1　岗位设置 26](#_Toc465867263)

[6.2.2.2　授权和审批 26](#_Toc465867264)

[6.2.2.3　安全意识教育和培训 26](#_Toc465867265)

[6.2.3　安全建设管理 27](#_Toc465867266)

[6.2.3.1　安全方案设计 27](#_Toc465867267)

[6.2.3.2　产品采购和使用 28](#_Toc465867268)

[6.2.3.3　移动应用软件开发 28](#_Toc465867269)

[6.2.3.4　工程实施 30](#_Toc465867270)

[6.2.3.5　测试验收 31](#_Toc465867271)

[6.2.3.6　系统交付 31](#_Toc465867272)

[6.2.3.7　安全服务商选择 32](#_Toc465867273)

[6.2.4　安全运维管理 33](#_Toc465867274)

[6.2.4.1　设备维护管理 33](#_Toc465867275)

[6.2.4.2　漏洞和风险管理 34](#_Toc465867276)

[6.2.4.3　应用软件来源管理 34](#_Toc465867277)

[6.2.4.4　恶意代码防范管理 35](#_Toc465867278)

[6.2.4.5　备份与恢复管理 35](#_Toc465867279)

[6.2.4.6　安全事件处置 36](#_Toc465867280)

[7　第三级测评要求 36](#_Toc465867281)

[7.1　安全技术单项测评 37](#_Toc465867282)

[7.1.1　物理和环境安全 37](#_Toc465867283)

[7.1.1.1　物理位置选择 37](#_Toc465867284)

[7.1.2　网络和通信安全 37](#_Toc465867285)

[7.1.2.1　结构安全 37](#_Toc465867286)

[7.1.2.2　边界防护 38](#_Toc465867287)

[7.1.2.3　访问控制 38](#_Toc465867288)

[7.1.2.4　入侵防范 40](#_Toc465867289)

[7.1.2.5　无线通信完整性和保密性 41](#_Toc465867290)

[7.1.2.6　安全审计 42](#_Toc465867291)

[7.1.2.7　网络设备防护 42](#_Toc465867292)

[7.1.3　设备和计算安全 43](#_Toc465867293)

[7.1.3.1　身份鉴别 43](#_Toc465867294)

[7.1.3.2　移动终端管控 44](#_Toc465867295)

[7.1.3.3　应用管控 45](#_Toc465867296)

[7.1.3.4　安全审计 46](#_Toc465867297)

[7.1.3.5　入侵防范 47](#_Toc465867298)

[7.1.3.6　恶意代码防范 49](#_Toc465867299)

[7.1.3.7　资源控制 49](#_Toc465867300)

[7.1.4　应用和数据安全 50](#_Toc465867301)

[7.1.4.1　身份鉴别 50](#_Toc465867302)

[7.1.4.2　软件审核与检测 52](#_Toc465867303)

[7.1.4.3　数据完整性 53](#_Toc465867304)

[7.1.4.4　数据保密性 53](#_Toc465867305)

[7.1.4.5　备份和恢复 55](#_Toc465867306)

[7.2　安全管理单项测评 56](#_Toc465867307)

[7.2.1　安全策略和管理制度 56](#_Toc465867308)

[7.2.1.1　管理制度 56](#_Toc465867309)

[7.2.2　安全管理机构和人员 57](#_Toc465867310)

[7.2.2.1　岗位设置 57](#_Toc465867311)

[7.2.2.2　人员配备 58](#_Toc465867312)

[7.2.2.3　授权和审批 59](#_Toc465867313)

[7.2.2.4　安全意识教育和培训 60](#_Toc465867314)

[7.2.3　安全建设管理 60](#_Toc465867315)

[7.2.3.1　安全方案设计 60](#_Toc465867316)

[7.2.3.2　产品采购和使用 61](#_Toc465867317)

[7.2.3.3　移动应用软件开发 62](#_Toc465867318)

[7.2.3.4　工程实施 65](#_Toc465867319)

[7.2.3.5　测试验收 65](#_Toc465867320)

[7.2.3.6　系统交付 65](#_Toc465867321)

[7.2.3.7　安全服务商选择 67](#_Toc465867322)

[7.2.4　安全运维管理 68](#_Toc465867323)

[7.2.4.1　资产管理 68](#_Toc465867324)

[7.2.4.2　设备维护管理 69](#_Toc465867325)

[7.2.4.3　风险评估和漏洞管理 70](#_Toc465867326)

[7.2.4.4　应用软件来源管理 70](#_Toc465867327)

[7.2.4.5　恶意代码防范管理 71](#_Toc465867328)

[7.2.4.6　配置管理 72](#_Toc465867329)

[7.2.4.7　监控和审计管理 73](#_Toc465867330)

[7.2.4.8　备份与恢复管理 74](#_Toc465867331)

[7.2.4.9　安全事件处置 75](#_Toc465867332)

[8　第四级测评要求 76](#_Toc465867333)

[8.1　安全技术单项测评 76](#_Toc465867334)

[8.1.1　物理和环境安全 76](#_Toc465867335)

[8.1.1.1　物理位置选择 76](#_Toc465867336)

[8.1.2　网络和通信安全 76](#_Toc465867337)

[8.1.2.1　结构安全 76](#_Toc465867338)

[8.1.2.2　边界防护 77](#_Toc465867339)

[8.1.2.3　访问控制 77](#_Toc465867340)

[8.1.2.4　入侵防范 79](#_Toc465867341)

[8.1.2.5　无线通信完整性和保密性 80](#_Toc465867342)

[8.1.2.6　安全审计 81](#_Toc465867343)

[8.1.2.7　网络设备防护 82](#_Toc465867344)

[8.1.3　设备和计算安全 83](#_Toc465867345)

[8.1.3.1　身份鉴别 83](#_Toc465867346)

[8.1.3.2　移动终端管控 84](#_Toc465867347)

[8.1.3.3　应用管控 85](#_Toc465867348)

[8.1.3.4　安全审计 86](#_Toc465867349)

[8.1.3.5　入侵防范 87](#_Toc465867350)

[8.1.3.6　恶意代码防范 88](#_Toc465867351)

[8.1.3.7　资源控制 89](#_Toc465867352)

[8.1.4　应用和数据安全 90](#_Toc465867353)

[8.1.4.1　身份鉴别 90](#_Toc465867354)

[8.1.4.2　软件审核与检测 92](#_Toc465867355)

[8.1.4.3　数据完整性 92](#_Toc465867356)

[8.1.4.4　数据保密性 93](#_Toc465867357)

[8.1.4.5　备份和恢复 95](#_Toc465867358)

[8.2　安全管理单项测评 96](#_Toc465867359)

[8.2.1　安全策略和管理制度 96](#_Toc465867360)

[8.2.1.1　管理制度 96](#_Toc465867361)

[8.2.2　安全管理机构和人员 97](#_Toc465867362)

[8.2.2.1　岗位设置 97](#_Toc465867363)

[8.2.2.2　人员配备 98](#_Toc465867364)

[8.2.2.3　授权和审批 99](#_Toc465867365)

[8.2.2.4　安全意识教育和培训 100](#_Toc465867366)

[8.2.3　安全建设管理 100](#_Toc465867367)

[8.2.3.1　安全方案设计 100](#_Toc465867368)

[8.2.3.2　产品采购和使用 101](#_Toc465867369)

[8.2.3.3　移动应用软件开发 102](#_Toc465867370)

[8.2.3.4　工程实施 105](#_Toc465867371)

[8.2.3.5　测试验收 105](#_Toc465867372)

[8.2.3.6　系统交付 105](#_Toc465867373)

[8.2.3.7　安全服务商选择 107](#_Toc465867374)

[8.2.4　安全运维管理 108](#_Toc465867375)

[8.2.4.1　资产管理 108](#_Toc465867376)

[8.2.4.2　设备维护管理 109](#_Toc465867377)

[8.2.4.3　风险评估和漏洞管理 110](#_Toc465867378)

[8.2.4.4　应用软件来源管理 110](#_Toc465867379)

[8.2.4.5　恶意代码防范管理 111](#_Toc465867380)

[8.2.4.6　配置管理 112](#_Toc465867381)

[8.2.4.7　监控和审计管理 113](#_Toc465867382)

[8.2.4.8　备份与恢复管理 114](#_Toc465867383)

[8.2.4.9　安全事件处置 115](#_Toc465867384)

[9　第五级测评要求 116](#_Toc465867385)

[附录A（资料性附录）　测评力度 117](#_Toc465867386)

[附录B（资料性附录）　测评单元编号说明 119](#_Toc465867387)

[参考文献 121](#_Toc465867388)

前  言

GB/T 28448《信息安全技术 网络安全等级保护测评要求》已经或计划发布以下部分：

——第1部分：安全通用要求；

——第2部分：云计算安全扩展要求；

——第3部分：移动互联安全扩展要求；

——第4部分：物联网安全扩展要求；

——第5部分：工控控制安全扩展要求；

——第6部分：大数据安全扩展要求。

本部分为GB/T 28448的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分起草单位：公安部信息安全等级保护评估中心、国家信息中心、中国移动通信有限公司研究院、北京鼎普科技股份有限公司、北京洋浦伟业科技发展有限公司、东巽科技（北京）有限公司。

* + 本部分主要起草人：于东升、黎水林、李明、任卫红、马力、袁静、陈广勇、曲洁、黄顺京、国强、岑荣伟、刘斐、何申、王江波、张宗喜、阚志刚、陈彪、李薛。

引  言

国家标准GB/T 28448-2012 《信息安全技术 信息系统安全等级保护测评要求》作为GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》的配套要求在开展信息系统安全等级保护测评工作中起到了重要作用。为了适应移动互联、云计算、大数据、物联网和工控系统等新技术、新应用情况下网络安全等级保护工作的开展，需要对原国家标准GB/T 22239-2008及配套标准GB/T 28448-2012进行修订与完善。

* + 对GB/T 28448-2012修订完成后，测评要求标准成为由多个部分组成的系列标准，本标准是网络安全等级保护测评要求中的第3部分—移动互联安全扩展要求。本部分对采用移动互联技术的等级保护对象进行安全等级保护测试评估的技术活动提出要求，为评价采用移动互联技术的等级保护对象是否符合 GB/T 22239.3-20XX 《信息安全技术 网络安全等级保护基本要求 第3部分：移动互联安全扩展要求》提供了获取证据的途径和方法，指导测评人员从信息安全等级保护的角度对采用移动互联技术的等级保护对象进行测试评估。

信息安全技术  
网络安全等级保护测评要求  
第3部分：移动互联安全扩展要求

范围

* + 本部分规定了不同等级保护对象的移动互联安全扩展测评要求。
  + 本部分适用于信息安全测评服务机构、等级保护对象的主管部门及运营使用单位对采用移动互联技术的等级保护对象的安全等级保护状况进行安全测试评估。信息安全监管职能部门依法进行的网络安全等级保护监督检查可以参考使用。

规范性引用文件

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

术语和定义

* + GB/T 25069-2010和GB/T 22239.3-20XX界定的以及下列术语和定义适用于本文件。



移动终端 mobile device

* + 在移动业务中使用的智能终端设备，包括手机、PAD、PC等通用终端和专用终端设备。



无线接入设备 wireless access point

* + 采用无线通信技术将移动终端接入有线网络的通信设备。本标准的无线接入设备是指为移动应用软件使用的专用设备（如Wi-Fi接入设备等），不包括向公共开放使用的无线接入设备。



无线接入网关 wireless access gateway

* + 部署在无线网络与有线网络之间，对传统移动应用软件进行安全防护的设备。



移动应用软件 mobile application

* + 在移动终端中运行的一般软件，包括通用移动应用软件以及等级保护对象的业务移动应用软件。本标准“应用安全”要求包括通用移动应用软件安全要求和等级保护对象的业务移动应用软件安全要求。



移动终端管理系统 mobile device management system（MDMS）

* + 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。

安全等级保护测评概述

1. 安全等级保护测评方法

等级保护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，给出达到特定级别安全保护能力的评判。等级保护测评实施的详细流程和方法参见GB/T 28449-20XX。

本标准中针对每一个要求项的测评就构成一个单项测评，单项测评中的每一个具体测评实施要求项（以下简称“测评要求项”）是与安全控制点下面所包括的要求项（测评指标）相对应的。在对每一要求项进行测评时，可能用到访谈、检查和测试三种测试方法，也可能用到其中一种或两种。测评实施的内容完全覆盖了GB/T 22239.3-20XX中所有要求项的测评要求，使用时应当从单项测评的测评实施中抽取出对于GB/T 22239.3-20XX中每一个要求项的测评要求，并按照这些测评要求开发测评指导书，以规范和指导安全等级测评活动。

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

1. 单项测评和整体测评

安全等级保护测评分为单项测评和整体测评。

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

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

第一级测评要求

1. 安全技术单项测评

物理和环境安全

1. 物理位置选择
   * + - 1. 测评单元（L1-PES1-01）

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。（本条款引用自GB/T 22239.3-20XX 5.1.1.1）

测评对象

无线接入设备和网络管理员。

测评实施

应访谈网络管理员，询问无线网络设备的覆盖范围与处理能力是否满足业务需求；

应检查无线接入设备的物理位置与无线信号的覆盖范围；

应使用无线信号探测工具测试无线信号的覆盖范围，判断是否存在过度覆盖的情况。

单项判定

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

网络和通信安全

1. 结构安全
   * + - 1. 测评单元（L1-NCS3-01）
2. 测评指标

应保证无线接入网关的处理能力满足基本业务需要。（本条款引用自GB/T 22239.3-20XX 5.1.2.1）

测评对象

无线接入网关和网络管理员。

测评实施

应访谈网络管理员，询问无线接入网关的业务处理能力是否满足基本业务需求；

应检查一段业务高峰时期内无线接入网关的CPU使用率和内存使用率。

单项判定

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

* + - * 1. 测评单元（L1-NCS3-02）

1. 测评指标

应保证无线接入设备的带宽满足基本业务需要。（本条款引用自GB/T 22239.3-20XX 5.1.2.1）

测评对象

无线接入网关和网络管理员。

测评实施

应访谈网络管理员，询问无线接入设备的网络带宽；

应检查一段业务高峰时期内带宽使用峰值，判断是否满足业务需求。

单项判定

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

* + - * 1. 测评单元（L1-NCS3-03）

1. 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，密钥长度不小于8位。（本条款引用自GB/T 22239.3-20XX 5.1.2.1）

测评对象

无线接入设备。

测评实施

应检查无线接入设备是否开启接入认证功能并使用除WEP方式以外的其它方式进行认证，密钥长度不小于8位。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 边界防护
   * + - 1. 测评单元（L1-NCS3-04）
2. 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。（本条款引用自GB/T 22239.3-20XX 5.1.2.2）

测评对象

无线接入网关。

测评实施

应检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。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 访问控制
   * + - 1. 测评单元（L1-NCS3-05）
2. 测评指标

应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信。（本条款引用自GB/T 22239.3-20XX 5.1.2.3）

测评对象

无线接入网关。

测评实施

应检查无线接入网关设置的访问控制规则有哪些，检查是否只开启了必要的通信接口。

单项判定

如果为肯定，则等级保护对象合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 通信完整性和保密性
   * + - 1. 测评单元（L1-NCS3-06）
2. 测评指标

应采用校验技术保证通信过程中数据的完整性。（本条款引用自GB/T 22239.3-20XX 5.1.2.4）

测评对象

移动应用设计文档和网络管理员。

测评实施

应访谈网络管理员，询问采用哪种校验技术保证无线网络通信过程中数据的完整性；

应检查设计、验收文档或源代码，查看是否有关于保护无线通信完整性的描述。

单项判定

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

设备和计算安全

1. 身份鉴别
   * + - 1. 测评单元（L1-ECS3-01）
2. 测评指标

应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别。（本条款引用自GB/T 22239.3-20XX 5.1.3.1）

测评对象

移动终端和移动终端管理系统。

测评实施

应检查移动终端登录、移动终端管理系统登录的身份鉴别策略，查看是否提供了身份鉴别措施；

应测试移动终端、移动终端管理系统的登录口令复杂度。

单项判定

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

* + - * 1. 测评单元（L1-ECS3-02）

1. 测评指标

移动终端应具有登录失败处理功能。（本条款引用自GB/T 22239.3-20XX 5.1.3.1）

测评对象

移动终端。

测评实施

应检查移动终端是否启用了登录失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等；

应测试移动终端的登录失败处理功能。

单项判定

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

1. 应用管控
   * + - 1. 测评单元（L1-ECS3-03）
2. 测评指标

移动终端管理客户端应具有选择应用软件安装、运行的功能。（本条款引用自GB/T 22239.3-20XX 5.1.3.2）

测评对象

移动终端管理系统。

测评实施

应检查移动终端管理客户端是否具有选择应用软件安装、运行的功能。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 入侵防范
   * + - 1. 测评单元（L1-ECS3-04）
2. 测评指标

移动终端应遵循最小安装的原则，仅安装需要的组件和应用程序。（本条款引用自GB/T 22239.3-20XX 5.1.3.3）

测评对象

移动终端。

测评实施

应检查移动终端中是否安装多余组件和应用程序；

应检查移动终端操作系统版本，查看补丁是否得到了及时更新。

单项判定

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

1. 恶意代码防范
   * + - 1. 测评单元（L1-ECS3-05）
2. 测评指标

移动终端应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库。（本条款引用自GB/T 22239.3-20XX 5.1.3.4）

测评对象

移动终端和安全管理员。

测评实施

应访谈安全管理员，询问移动终端恶意代码防护策略以及定期查杀频率；

应检查移动终端是否安装了防恶意代码产品；

应检查移动终端防恶意代码产品软件版本和恶意代码库版本。

单项判定

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

应用和数据安全

* + - * 1. 数据完整性
        2. 测评单元（L1-ADS3-01）

1. 测评指标

移动应用软件应采用校验技术保证重要数据存储的完整性。（本条款引用自GB/T 22239.3-20XX 5.1.4.1）

测评对象

移动应用设计文档和应用管理员。

测评实施

应访谈应用管理员，采用哪种校验技术保证存储过程中数据的完整性；

应检查应用系统的设计、验收文档或源代码，查看是否有关于能检测重要业务数据存储过程中完整性受到破坏的描述。

单项判定

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

1. 安全管理单项测评

安全策略和管理制度

1. 管理制度
   * + - 1. 测评单元（L1-PSS3-01）
2. 测评指标

应建立等级保护对象移动互联安全管理规范，并纳入等级保护对象管理安全制度。（本条款引用自GB/T 22239.3-20XX 5.2.1.1）

测评对象

管理制度类文档。

测评实施

应检查安全管理制度，查看是否包括移动互联安全管理的相关内容。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全管理机构和人员

1. 岗位设置
   * + - 1. 测评单元（L1-ORS3-01）
2. 测评指标

应将移动互联管理纳入等级保护对象管理员职责。（本条款引用自GB/T 22239.3-20XX 5.2.2.1）

测评对象

信息安全负责人和管理制度类文档。

测评实施

应访谈信息安全负责人，询问是否设置了移动互联相关管理岗位，岗位职责是否明确。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全意识教育和培训
   * + - 1. 测评单元（L1-ORS3-02）
2. 测评指标

应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。（本条款引用自GB/T 22239.3-20XX 5.2.2.2）

测评对象

信息安全负责人和管理制度类文档。

测评实施

应访谈信息安全负责人，询问是否对各类人员进行移动互联安全教育和岗位技能培训，告知相关的安全知识、安全责任和惩戒措施等。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全建设管理

1. 安全方案设计
   * + - 1. 测评单元（L1-CMS3-01）
2. 测评指标

应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施。（本条款引用自GB/T 22239.3-20XX 5.2.3.1）

测评对象

系统建设负责人。

测评实施

应访谈系统建设负责人，询问是否依据风险分析的结果补充和调整过安全措施，具体做过哪些调整。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 产品采购和使用
   * + - 1. 测评单元（L1-CMS3-02）
2. 测评指标

应确保移动互联安全产品采购和使用符合国家的有关规定。（本条款引用自GB/T 22239.3-20XX 5.2.3.2）

测评对象

系统建设负责人。

测评实施

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

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 工程实施
   * + - 1. 测评单元（L1-CMS3-03）
2. 测评指标

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。（本条款引用自GB/T 22239.3-20XX 5.2.3.3）

测评对象

系统建设负责人。

测评实施

应访系统建设负责人，询问是否指定专门部门或人员对移动互联工程实施过程进行进度和质量控制，具体由何部门/何人负责。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 测试验收
   * + - 1. 测评单元（L1-CMS3-04）
2. 测评指标

应对系统的移动互联部分进行必要的安全性测试验收。（本条款引用自GB/T 22239.3-20XX 5.2.3.4）

测评对象

系统建设负责人。

测评实施

应访谈系统建设负责人，询问在移动应用系统建设完成后是否对其进行安全性测试验收；

应检查是否具有移动互联工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；

应检查是否具有移动应用系统测试验收报告。

单项判定

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

1. 系统交付
   * + - 1. 测评单元（L1-CMS3-05）
2. 测评指标

应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；（本条款引用自GB/T 22239.3-20XX 5.2.3.5）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否具有移动应用系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L1-CMS3-06）

1. 测评指标

应对负责系统移动互联运行维护的技术人员进行相应的技能培训。（本条款引用自GB/T 22239.3-20XX 5.2.3.5）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问移动应用系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全服务商选择
   * + - 1. 测评单元（L1-CMS3-07）
2. 测评指标

应确保移动互联安全服务商的选择符合国家的有关规定；（本条款引用自GB/T 22239.3-20XX 5.2.3.6）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问系统选择的安全服务商有哪些，是否符合国家有关规定。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L1-CMS3-08）

1. 测评指标

应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任。（本条款引用自GB/T 22239.3-20XX 5.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全运维管理

1. 设备维护管理
   * + - 1. 测评单元（L1-MMS3-01）
2. 测评指标

应对各种移动互联设备（包括无线接入设备）维护纳入等级保护对象进行管理。（本条款引用自GB/T 22239.3-20XX 5.2.4.1）

测评对象

管理制度类文档。

测评实施

应检查设备管理制度，查看是否将各种移动互联设备（包括无线接入设备）维护纳入管理制度内并进行管理。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 漏洞和风险管理
   * + - 1. 测评单元（L1-MMS3-02）
2. 测评指标

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患定期进行修补。（本条款引用自GB/T 22239.3-20XX 5.2.4.2）

测评对象

安全管理员和记录表单类文档。

测评实施

应访谈安全管理员，询问采取哪些措施识别移动互联安全漏洞和隐患，并在评估后对发现的安全漏洞和隐患进行修补；

应检查移动互联安全漏洞管理记录。

单项判定

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

1. 应用软件来源管理
   * + - 1. 测评单元（L1-MMS3-03）
2. 测评指标

应保证移动终端安装、运行的应用软件来自可靠证书签名或可靠分发渠道。（本条款引用自GB/T 22239.3-20XX 5.2.4.3）

测评对象

安全管理员。

测评实施

应访谈安全管理员，移动终端安装、运行的应用软件是否来自可靠证书签名或可靠分发

渠道。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 恶意代码防范管理
   * + - 1. 测评单元（L1-MMS3-04）
2. 测评指标

应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。（本条款引用自GB/T 22239.3-20XX 5.2.4.4）

测评对象

系统运维负责人。

测评实施

应访谈系统运维负责人，询问是否对员工进行移动互联基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查等。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 备份与恢复管理
   * + - 1. 测评单元（L1-MMS3-05）
2. 测评指标

应识别需要定期备份的移动终端中的关键业务信息、系统数据及软件系统等；（本条款引用自GB/T 22239.3-20XX 5.2.4.5）

测评对象

系统运维负责人和管理制度类文档。

测评实施

应访谈系统运维负责人，询问是否识别出需要定期备份移动应用软件中的业务信息、系统数据和软件系统，主要有哪些。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L1-MMS3-06）

1. 测评指标

应规定备份信息的备份方式、备份频度、存储介质、保存期等。（本条款引用自GB/T 22239.3-20XX 5.2.4.5）

测评对象

管理制度类文档。

测评实施

应检查备份管理文档，查看其是否明确了备份方式、备份频度、存储介质和保存期等方面内容。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

第二级测评要求

1. 安全技术单项测评

物理和环境安全

1. 物理位置选择
   * + - 1. 测评单元（L2-PES3-01）
2. 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。（本条款引用自GB/T 22239.3-20XX 6.1.1）

测评对象

无线接入设备和网络管理员。

测评实施

应访谈网络管理员，询问无线网络设备的覆盖范围与处理能力是否满足业务需求；

应检查无线接入设备的物理位置与无线信号的覆盖范围；

应使用无线信号探测工具测试无线信号的覆盖范围，判断是否存在过度覆盖的情况。

单项判定

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

网络和通信安全

1. 结构安全
   * + - 1. 测评单元（L2-NCS3-01）
2. 测评指标

应保证无线接入网关的处理能力满足业务高峰期需要。（本条款引用自GB/T 22239.3-20XX 6.1.2.1）

测评对象

无线接入网关和网络管理员。

测评实施

应访谈网络管理员，询问无线接入网关的业务处理能力是否满足基本业务需求；

应检查一段业务高峰时期内无线接入网关的CPU使用率和内存使用率。

单项判定

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

* + - * 1. 测评单元（L2-NCS3-02）

1. 测评指标

应保证无线接入设备的带宽满足业务高峰期需要。（本条款引用自GB/T 22239.3-20XX 6.1.2.1）

测评对象

无线接入设备和网络管理员。

测评实施

应访谈网络管理员，询问无线接入设备的网络带宽；

应检查一段业务高峰时期内带宽使用峰值，判断是否满足业务需求。

单项判定

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

* + - * 1. 测评单元（L2-NCS3-03）

1. 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，密钥长度不小于8位并且由数字、字母和特殊字符两种或两种以上进行组合。（本条款引用自GB/T 22239.3-20XX 6.1.2.1）

1. 测评对象

无线接入设备。

1. 测评实施

应检查无线接入设备是否开启接入认证功能并使用除WEP方式以外的其它方式进行认

证，密钥长度不小于8位，且密码由数字、字母和特殊字符两种或两种以上进行组合。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 边界防护
   * + - 1. 测评单元（L2-NCS3-04）
2. 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。（本条款引用自GB/T 22239.3-20XX 6.1.2.2）

1. 测评对象

无线接入网关。

1. 测评实施

应检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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 访问控制
   * + - 1. 测评单元（L2-NCS3-05）
2. 测评指标

应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信。（本条款引用自GB/T 22239.3-20XX 6.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关设置的访问控制规则有哪些，检查是否只开启了必要的通信接口。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-NCS3-06）

1. 测评指标

应对来自移动终端的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过。（本条款引用自GB/T 22239.3-20XX 6.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关，查看配置的访问控制策略是否对数据流量、数据包和协议等进行检查，并进行数据流控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 入侵防范
   * + - 1. 测评单元（L2-NCS3-07）
2. 测评指标

应能够检测、记录非授权无线接入设备。（本条款引用自GB/T 22239.3-20XX 6.1.2.4）

1. 测评对象

入侵防范设备和网络管理员。

1. 测评实施

应访谈网络管理员，询问无线网络的入侵防范措施有哪些；询问无线网络入侵防范设备具备哪些防范功能；

应检查入侵防范设备是否能够检测、记录非授权无线接入设备。

1. 单项判定

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

* + - * 1. 测评单元（L2-NCS3-08）

1. 测评指标

应能够对非授权移动终端接入的行为进行检测、记录。（本条款引用自GB/T 22239.3-20XX 6.1.2.4）

测评对象

入侵防范设备。

测评实施

应检查入侵防范设备是否能够检测、记录非授权无线接入终端的接入行为。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-NCS3-09）

1. 测评指标

应具备对针对无线接入设备的网络扫描、DoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录。（本条款引用自GB/T 22239.3-20XX 6.1.2.4）

1. 测评对象

入侵防范设备。

1. 测评实施

应检查入侵防范设备，是否能够对网络扫描、DoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录；

应检查网络入侵防范设备的规则库版本，查看其规则库是否及时更新。

1. 单项判定

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

* + - * 1. 测评单元（L2-NCS3-010）

1. 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。（本条款引用自GB/T 22239.3-20XX 6.1.2.4）

1. 测评对象

入侵防范设备。

1. 测评实施

应检查入侵防范设备，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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 通信完整性和保密性
   * + - 1. 测评单元（L2-NCS3-011）
2. 测评指标

应保证无线通信过程中数据的完整性。（本条款引用自GB/T 22239.3-20XX 6.1.2.5）

1. 测评对象

移动应用设计文档和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问采用哪种校验技术保证无线网络通信过程中数据的完整性；
3. 应检查设计、验收文档或源代码，查看是否有关于保护无线通信完整性的描述。
4. 单项判定

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

* + - * 1. 测评单元（L2-NCS3-012）

1. 测评指标

应保证无线通信过程中敏感信息字段或整个报文的保密性。（本条款引用自GB/T 22239.3-20XX 6.1.2.5）

测评对象

移动应用设计文档、移动应用软件和网络管理员。

测评实施

应访谈网络管理员，询问采用哪种校验技术保证无线网络通信过程中数据的保密性；

应检查设计、验收文档或源代码，查看是否有采用加密技术保护无线通信保密性的

描述；

应测试无线通信过程中重要数据是否进行了加密。

单项判定

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

1. 安全审计
   * + - 1. 测评单元（L2-NCS3-013）
2. 测评指标

应启用设备安全审计功能，审计覆盖到每个移动终端，对重要的终端行为和重要安全事件进行审计。（本条款引用自GB/T 22239.3-20XX 6.1.2.6）

1. 测评对象

无线接入设备和网络管理员。

1. 测评实施

应访谈网络管理员，询问网络采用了何种审计机制，采用了哪些审计策略，用以实现对无线网络的安全审计；

应检查无线接入网关及无线接入设备，是否开启安全审计功能，查看审计策略是否包括设备运行状况、网络流量、管理账户的登录及重要操作等；

应检查网络中是否部署了审计措施，对每个移动终端的重要行为和重要安全事件进行审计。

1. 单项判定

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

1. 网络设备防护
   * + - 1. 测评单元（L2-NCS3-014）
2. 测评指标

应能发现系统移动终端、无线接入设备、无线接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自GB/T 22239.3-20XX 6.1.2.7）

测评对象

移动终端、无线接入设备、无线接入网关设备和网络管理员。

测评实施

应访谈网络管理员，询问系统移动终端、无线接入设备、无线接入网关等设备的补丁管理采用何种机制；

应检查系统移动终端、无线接入设备、无线接入网关等设备的补丁是否得到了及时更新。

单项判定

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

* + - * 1. 测评单元（L2-NCS3-015）

1. 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。（本条款引用自GB/T 22239.3-20XX 6.1.2.7）

1. 测评对象

无线接入设备和无线接入网关。

1. 测评实施

应检查无线接入设备和无线接入网关是否关闭了“SSID广播、WEP认证” 等存在风

险的功能。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-NCS3-016）

1. 测评指标

应禁止多个AP使用同一个鉴别密钥。（本条款引用自GB/T 22239.3-20XX 6.1.2.7）

1. 测评对象

无线接入设备。

1. 测评实施

应检查无线接入设备是否分别使用了不同的鉴别密钥。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

设备和计算安全

1. 身份鉴别
   * + - 1. 测评单元（L2-ECS3-01）
2. 测评指标

应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别。（本条款引用自GB/T 22239.3-20XX 6.1.3.1）

1. 测评对象

移动终端和移动终端管理系统。

1. 测评实施

应检查移动终端登录、移动终端管理系统登录的身份鉴别策略，查看是否提供了身份鉴别措施；

应测试移动终端、移动终端管理系统的登录口令复杂度。

1. 单项判定

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

* + - * 1. 测评单元（L2-ECS3-02）

1. 测评指标

移动终端应具有登录失败处理功能。（本条款引用自GB/T 22239.3-20XX 6.1.3.1）

测评对象

移动终端。

测评实施

应检查移动终端是否启用了登录失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等；

应测试移动终端的登录失败处理功能。

单项判定

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

1. 应用管控
   * + - 1. 测评单元（L2-ECS3-03）
2. 测评指标

移动终端管理客户端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。（本条款引用自GB/T 22239.3-20XX 6.1.3.2）

测评对象

移动终端管理系统。

测评实施

应检查移动终端管理客户端是否具有软件白名单功能；

应测试使用白名单控制应用软件安装、运行。

单项判定

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

* + - * 1. 测评单元（L2-ECS3-04）

1. 测评指标

移动终端管理客户端应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问。（本条款引用自GB/T 22239.3-20XX 6.1.3.2）

测评对象

移动终端管理系统。

测评实施

应检查移动终端管理客户端是否具有应用软件权限控制功能；

应测试是否可以对移动终端中资源的访问进行限制。

单项判定

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

* + - * 1. 测评单元（L2-ECS3-05）

1. 测评指标

移动终端管理客户端应只允许可靠证书签名的应用软件安装和运行。（本条款引用自GB/T 22239.3-20XX 6.1.3.2）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查移动终端管理客户端所允许使用的签名证书。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 入侵防范
   * + - 1. 测评单元（L2-ECS3-06）
2. 测评指标

移动终端应遵循最小安装的原则，仅安装需要的组件和应用程序。（本条款引用自GB/T 22239.3-20XX 6.1.3.3）

测评对象

移动终端。

测评实施

应检查移动终端中是否安装多余组件和应用程序；

应检查移动终端操作系统版本，查看补丁是否得到了及时更新。

单项判定

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

* + - * 1. 测评单元（L2-ECS3-07）

1. 测评指标

移动终端应能发现可能存在的漏洞，及时修补漏洞。（本条款引用自GB/T 22239.3-20XX 6.1.3.3）

测评对象

移动终端。

测评实施

应检查移动终端操作系统版本，查看补丁是否得到了及时更新；

应检查移动终端是否能够发现系统漏洞并及时修补。

单项判定

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

* + - * 1. 测评单元（L2-ECS3-08）

1. 测评指标

移动终端应能够发现用户权限异常改变的情况。（本条款引用自GB/T 22239.3-20XX 6.1.3.3）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否能够发现用户权限异常改变的情况。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 恶意代码防范
   * + - 1. 测评单元（L2-ECS3-09）
2. 测评指标

移动终端应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库。（本条款引用自GB/T 22239.3-20XX 6.1.3.4）

测评对象

移动终端和安全管理员。

测评实施

应访谈安全管理员，询问移动终端恶意代码防护策略以及定期查杀频率；

应检查移动终端是否安装了查杀恶意代码的防恶意代码产品；

应检查移动终端防恶意代码产品软件版本和恶意代码库版本。

单项判定

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

1. 资源控制
   * + - 1. 测评单元（L2-ECS3-10）
2. 测评指标

应将移动终端处理访问不同等级等级保护对象的进行应用级隔离。（本条款引用自GB/T 22239.3-20XX 6.1.3.5）

1. 测评对象

安全管理员。

1. 测评实施

应访谈安全管理员，询问移动终端采用哪种安全隔离手段或措施对不同等级等级保护对

象进行应用级隔离。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-ECS3-11）

1. 测评指标

应将移动终端处理访问等级保护对象的应用软件、数据存储区与处理访问非等级保护对象的应用软件、数据存储区等进行隔离。（本条款引用自GB/T 22239.3-20XX 6.1.3.5）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否采用安全沙箱或其它安全区域隔离措施进行应用级隔离。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-ECS3-12）

1. 测评指标

应限制用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权。（本条款引用自GB/T 22239.3-20XX 6.1.3.5）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查对移动终端的用户或进程可访问资源的限定，防止移动终端被提权。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

应用和数据安全

1. 身份鉴别
   * + - 1. 测评单元（L2-ADS3-01）
2. 测评指标

使用口令登录时，应强制用户首次登录时修改初始口令，对用户的鉴别信息进行复杂度检查。（本条款引用自GB/T 22239.3-20XX 6.1.4.1）

测评对象

移动应用软件。

测评实施

应检查移动应用软件，查看是否提供身份标识和鉴别功能；

应检查移动应用软件，查看是否采用了措施保证身份标识具有唯一性，是否强制用户首次登录时修改初始口令，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用。

单项判定

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

* + - * 1. 测评单元（L2-ADS3-02）

1. 测评指标

用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。（本条款引用自GB/T 22239.3-20XX 6.1.4.1）

测评对象

移动应用软件。

测评实施

应测试移动应用软件，可通过试图以合法和非法用户分别登录系统，查看是否成功，验证身份标识和鉴别功能是否有效；

应测试移动应用软件，可通过重置鉴别信息，查看是否成功，验证鉴别信息重置是否有效。

单项判定

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

1. 软件审核与检测
   * + - 1. 测评单元（L2-ADS3-03）
2. 测评指标

应保证等级保护对象业务移动应用软件开发结束后经合规性审核。（本条款引用自GB/T 22239.3-20XX 6.1.4.2）

测评对象

移动应用设计文档和系统建设负责人。

测评实施

应访谈建设负责人，询问是否在移动应用软件开发结束后进行规性审核；

应检查是否有移动应用软件规性审核报告。

单项判定

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

1. 数据完整性
   * + - 1. 测评单元（L2-ADS3-04）
2. 测评指标

移动应用软件应采用校验技术或密码技术保证通信过程中数据的完整性。（本条款引用自GB/T 22239.3-20XX 6.1.4.3）

测评对象

移动应用设计文档、移动应用软件和应用管理员。

测评实施

应访谈应用管理员，采用哪种校验技术或密码技术保证通信和存储过程中数据的完整性；

应检查移动应用软件设计、验收文档或源代码，查看是否有关于能检测数据通信和存储过程中完整性受到破坏的描述；

应测试移动应用软件，可通过获取通信双方的数据包，查看通信报文中是否含有校验码。

单项判定

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

* + - * 1. 测评单元（L2-ADS3-05）

1. 测评指标

移动应用软件应采用校验技术或密码技术保证重要数据存储的完整性。（本条款引用自GB/T 22239.3-20XX 6.1.4.3）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看是否配备检测系统管理数据、鉴别信息和业务数据在存储过程中完整性受到破坏的功能。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 数据保密性
   * + - 1. 测评单元（L2-ADS3-06）
2. 测评指标

移动应用软件应采用密码技术保证重要数据在本地存储时的保密性。（本条款引用自GB/T 22239.3-20XX 6.1.4.4）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看其鉴别信息和主要数据是否采用加密或其他有效措施实现了

存储保密性。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-ADS3-07）

1. 测评指标

移动应用软件应对通信过程中的敏感信息字段进行加密。（本条款引用自GB/T 22239.3-20XX 6.1.4.4）

测评对象

移动应用软件。

测评实施

应检查移动应用软件，查看其管理数据和鉴别信息是否采用加密或其他有效措施实现了

传输保密性。

单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全管理单项测评

安全策略和管理制度

1. 管理制度
   * + - 1. 测评单元（L2-PSS3-01）
2. 测评指标

应建立等级保护对象移动互联安全管理规范，并纳入等级保护对象管理安全制度；（本条款引用自GB/T 22239.3-20XX 6.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括移动互联安全管理规范等相关内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-PSS3-02）

1. 测评指标

应对管理人员或移动终端操作人员执行的日常管理操作建立操作规程。（本条款引用自GB/T 22239.3-20XX 6.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括人员日常管理操作规程。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全管理机构和人员

1. 岗位设置
   * + - 1. 测评单元（L2-ORS3-01）
2. 测评指标

应将移动互联管理纳入等级保护对象管理员职责。（本条款引用自GB/T 22239.3-20XX 6.2.2.1）

1. 测评对象

信息安全负责人和管理制度类文档。

1. 测评实施

应访谈信息安全负责人，询问是否设置了移动互联相关管理岗位，岗位职责是否明确。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 授权和审批
   * + - 1. 测评单元（L2-ORS3-02）
2. 测评指标

应针对移动互联系统变更、重要操作、物理访问和系统接入等事项执行审批过程。（本条款引用自GB/T 22239.3-20XX 6.2.2.2）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否针对移动应用系统变更、重要操作、物理访问和系统接入等事项执行审批过

程，是否有相关审批记录表单。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全意识教育和培训
   * + - 1. 测评单元（L2-ORS3-03）
2. 测评指标

应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。（本条款引用自GB/T 22239.3-20XX 6.2.2.3）

1. 测评对象

信息安全负责人。

1. 测评实施

应访谈信息安全负责人，询问是否对各类人员进行移动互联安全教育和岗位技能培训，

告知相关的安全知识、安全责任和惩戒措施等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全建设管理

1. 安全方案设计
   * + - 1. 测评单元（L2-CMS3-01）
2. 测评指标

应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施；（本条款引用自GB/T 22239.3-20XX 6.2.3.1）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否依据风险分析的结果补充和调整过安全措施，具体做过哪些调整。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-02）

1. 测评指标

应根据等级保护对象的安全保护等级进行移动互联安全方案设计；（本条款引用自GB/T 22239.3-20XX 6.2.3.1）

1. 测评对象

安全规划设计类文档。

1. 测评实施

应检查移动应用系统的安全设计方案，查看方案是否描述系统的安全保护等级，是否描述系统的安全保护策略，是否根据系统的安全级别选择了安全措施；

应检查移动应用系统的安全设计方案，查看是否详细描述安全措施的实现内容，是否有安全产品的功能、性能和部署等描述，是否有安全建设的费用和计划等。

1. 单项判定

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

1. 产品采购和使用
   * + - 1. 测评单元（L2-CMS3-03）
2. 测评指标

应确保移动互联安全产品采购和使用符合国家的有关规定。（本条款引用自GB/T 22239.3-20XX 6.2.3.2）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问移动应用软件使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 移动应用软件开发
   * + - 1. 测评单元（L2-CMS3-04）
2. 测评指标

应要求对移动业务应用软件开发者进行资格审查；（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否对开发者进行资格审查。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-05）

1. 测评指标

应确保开发移动业务应用软件的签名证书合法性；（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

移动应用软件。

1. 测评实施

应检查开发移动业务应用软件的签名证书是否具有合法性。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-06）

1. 测评指标

应要求移动应用软件开发完提供软件设计文档和使用指南；（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

移动应用设计文档。

1. 测评实施

应检查是否具备软件设计文档和使用指南。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-07）

1. 测评指标

应要求应用软件开发使用的工具来源可靠；（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应检查应用软件开发使用的工具来源。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-08）

1. 测评指标

自行开发移动应用软件，应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应检查开发环境与实际运行环境是否物理分开，测试数据和测试结果受到控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-09）

1. 测评指标

自行开发移动应用软件，应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查是否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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-010）

1. 测评指标

自行开发移动应用软件，应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查是否包含移动应用软件设计的相关文档并对文档使用进行控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-011）

1. 测评指标

自行开发移动应用软件，应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。（本条款引用自GB/T 22239.3-20XX 6.2.3.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查是否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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 工程实施
   * + - 1. 测评单元（L2-CMS3-012）
2. 测评指标

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。（本条款引用自GB/T 22239.3-20XX 6.2.3.4）

1. 测评对象

系统建设负责人。

1. 测评实施

应访系统建设负责人，询问是否指定专门部门或人员对移动互联工程实施过程进行进度和质量控制，具体由何部门/何人负责。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 测试验收
   * + - 1. 测评单元（L2-CMS3-013）
2. 测评指标

应对系统的移动互联部分进行安全性测试验收。（本条款引用自GB/T 22239.3-20XX 6.2.3.5）

测评对象

系统建设负责人。

测评实施

应访谈系统建设负责人，询问在移动应用系统建设完成后是否对其进行安全性测试验收；

应检查是否具有移动互联工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；

应检查是否具有移动应用软件测试验收报告。

单项判定

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

1. 系统交付
   * + - 1. 测评单元（L2-CMS3-014）
2. 测评指标

应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；（本条款引用自GB/T 22239.3-20XX 6.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否具有移动应用系统交付清单，查看交付清单是否说明系统交付的各类设备、

软件、文档等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-015）

1. 测评指标

应对负责系统移动互联运行维护的技术人员进行相应的技能培训；（本条款引用自GB/T 22239.3-20XX 6.2.3.6）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问移动应用系统正式运行前是否对运行维护人员进行过培训，

针对哪些方面进行过培训。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-016）

1. 测评指标

应确保提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档。（本条款引用自GB/T 22239.3-20XX 6.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全服务商选择
   * + - 1. 测评单元（L2-CMS3-017）
2. 测评指标

应确保移动互联安全服务商的选择符合国家的有关规定；（本条款引用自GB/T 22239.3-20XX 6.2.3.7）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问系统选择的安全服务商有哪些，是否符合国家有关规定。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-018）

1. 测评指标

应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任；（本条款引用自GB/T 22239.3-20XX 6.2.3.7）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保

密范围、安全责任、违约责任、协议的有效期限和责任人的签字等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-CMS3-019）

1. 测评指标

应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务。（本条款引用自GB/T 22239.3-20XX 6.2.3.7）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查与服务商签订的相关协议等文档，查看其内容是否协议的有效期限和责任人的签

字等整个服务供应链各方需履行的信息安全相关义务。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全运维管理

1. 设备维护管理
   * + - 1. 测评单元（L2-MMS3-01）
2. 测评指标

应对各种移动互联设备（包括无线接入设备）维护纳入等级保护对象进行管理。（本条款引用自GB/T 22239.3-20XX 6.2.4.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查设备管理制度，查看是否将各种移动互联设备（包括无线接入设备）维护纳入管理制度内并进行管理。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 漏洞和风险管理
   * + - 1. 测评单元（L2-MMS3-02）
2. 测评指标

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。（本条款引用自GB/T 22239.3-20XX 6.2.4.2）

1. 测评对象

安全管理员和记录表单类文档。

1. 测评实施

应访谈安全管理员，询问采取哪些措施识别移动互联安全漏洞和隐患，并在评估后对发现的安全漏洞和隐患进行修补；

应检查移动互联安全漏洞管理记录。

1. 单项判定

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

1. 应用软件来源管理
   * + - 1. 测评单元（L2-MMS3-03）
2. 测评指标

应保证移动终端安装、运行的应用软件来自可靠证书签名或可靠分发渠道；（本条款引用自GB/T 22239.3-20XX 6.2.4.3）

1. 测评对象

安全管理员。

1. 测评实施

应访谈安全管理员，移动终端安装、运行的应用软件是否来自可靠证书签名或可靠分发

渠道。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-MMS3-04）

1. 测评指标

应保证移动终端安装、运行的等级保护对象业务移动应用软件由经审核的开发者开发。（本条款引用自GB/T 22239.3-20XX 6.2.4.3）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动终端安装、运行的移动应用软件是否由经审核的开发者开发。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 恶意代码防范管理
   * + - 1. 测评单元（L2-MMS3-05）
2. 测评指标

应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；（本条款引用自GB/T 22239.3-20XX 6.2.4.4）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问是否对员工进行移动互联基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 备份与恢复管理
   * + - 1. 测评单元（L2-MMS3-06）
2. 测评指标

应识别需要定期备份的移动终端中的重要业务信息、系统数据及软件系统等；（本条款引用自GB/T 22239.3-20XX 6.2.4.5）

1. 测评对象

系统运维负责人和管理制度类文档。

1. 测评实施

应访谈系统运维负责人，询问是否识别出需要定期备份移动应用软件中的业务信息、系统数据和软件系统，主要有哪些。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-MMS3-07）

1. 测评指标

应规定备份信息的备份方式、备份频度、存储介质、保存期等。（本条款引用自GB/T 22239.3-20XX 6.2.4.5）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查备份管理文档，查看其是否明确了备份方式、备份频度、存储介质和保存期等方

面内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全事件处置
   * + - 1. 测评单元（L2-MMS3-08）
2. 测评指标

应报告所发现的移动互联安全弱点和可疑事件；（本条款引用自GB/T 22239.3-20XX 6.2.4.6）

1. 测评对象

系统运维负责人和记录表单类文档。

1. 测评实施

应访谈系统运维负责人，询问是否有报告所发现的移动互联安全弱点和可疑事件的相关流程与文件。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L2-MMS3-09）

1. 测评指标

应明确移动互联安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。（本条款引用自GB/T 22239.3-20XX 6.2.4.6）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查移动互联安全事件的报告和处置流程，查看其是否明确了安全事件的现场处理、

事件报告和后期恢复的管理职责等方面内容。

1. 单项判定
   * 如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

第三级测评要求

1. 安全技术单项测评

物理和环境安全

1. 物理位置选择
   * + - 1. 测评单元（L3-PES3-01）
2. 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。（本条款引用自GB/T 22239.3-20XX 7.1.1）

测评对象

无线接入设备和网络管理员。

测评实施

应访谈网络管理员，询问无线网络设备的覆盖范围与处理能力是否满足业务需求；

应检查无线接入设备的物理位置与无线信号的覆盖范围；

应使用无线信号探测工具测试无线信号的覆盖范围，判断是否存在过度覆盖的情况。

单项判定

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

网络和通信安全

1. 结构安全
   * + - 1. 测评单元（L3-NCS3-01）
2. 测评指标

应保证无线接入网关的处理能力满足业务高峰期需要。（本条款引用自GB/T 22239.3-20XX 7.1.2.1）

测评对象

无线接入网关和网络管理员。

测评实施

应访谈网络管理员，询问无线接入网关的业务处理能力是否满足基本业务需求；

应检查一段业务高峰时期内无线接入网关的CPU使用率和内存使用率。

单项判定

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

* + - * 1. 测评单元（L3-NCS3-02）

1. 测评指标

应保证无线接入设备的带宽满足业务高峰期需要。（本条款引用自GB/T 22239.3-20XX 7.1.2.1）

测评对象

无线接入设备和网络管理员。

测评实施

应访谈网络管理员，询问无线接入设备的网络带宽；

应检查一段业务高峰时期内带宽使用峰值，判断是否满足业务需求。

单项判定

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

* + - * 1. 测评单元（L3-NCS3-03）

1. 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或国产算法进行加密。（本条款引用自GB/T 22239.3-20XX 7.1.2.1）

1. 测评对象

无线接入设备。

1. 测评实施

应检查无线接入设备是否开启接入认证功能，且认证过程采用认证服务器或国产算法进

行加密。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 边界防护
   * + - 1. 测评单元（L3-NCS3-04）
2. 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。（本条款引用自GB/T 22239.3-20XX 7.1.2.2）

1. 测评对象

无线接入网关。

1. 测评实施

应检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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 访问控制
   * + - 1. 测评单元（L3-NCS3-05）
2. 测评指标

应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信。（本条款引用自GB/T 22239.3-20XX 7.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关设置的访问控制规则有哪些，检查是否只开启了必要的通信接口。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-NCS3-06）

1. 测评指标

应对来自移动终端的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过。（本条款引用自GB/T 22239.3-20XX 7.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关，查看配置的访问控制策略是否对数据流量、数据包和协议等进行检查，并进行数据流控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-NCS3-07）

1. 测评指标

应在无线接入网关上对进出无线网络的数据进行内容过滤。（本条款引用自GB/T 22239.3-20XX 7.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关是否具备并开启了数据内容过滤功能。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-NCS3-08）

1. 测评指标

应设置访问控制规则限制移动终端可访问的等级保护对象资源。（本条款引用自GB/T 22239.3-20XX 7.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关及无线接入设备，是否设置了访问控制规则，限制终端用户的访问

权限。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 入侵防范
   * + - 1. 测评单元（L3-NCS3-09）
2. 测评指标

应能够检测、记录、定位非授权无线接入设备。（本条款引用自GB/T 22239.3-20XX 7.1.2.4）

1. 测评对象

入侵防范设备和网络管理员。

1. 测评实施

应访谈网络管理员，询问无线网络的入侵防范措施有哪些；询问无线网络入侵防范设备具备哪些防范功能；

应检查入侵防范设备是否能够检测、记录、定位非授权无线接入设备。

1. 单项判定

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

* + - * 1. 测评单元（L3-NCS3-10）

1. 测评指标

应能够对非授权移动终端接入的行为进行检测、记录、定位。（本条款引用自GB/T 22239.3-20XX 7.1.2.4）

1. 测评对象

入侵防范设备。

1. 测评实施

应检查入侵防范设备是否能够检测、记录、定位非授权无线接入终端的接入行为。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-NCS3-11）

1. 测评指标

应具备对针对无线接入设备的网络扫描、DoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位。（本条款引用自GB/T 22239.3-20XX 7.1.2.4）

测评对象

入侵防范设备。

测评实施

应检查无线网络入侵防范设备，是否能够对网络扫描、DoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；

应检查网络入侵防范设备的规则库版本，查看其规则库是否及时更新。

单项判定

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

* + - * 1. 测评单元（L3-NCS3-12）

1. 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。（本条款引用自GB/T 22239.3-20XX 7.1.2.4）

1. 测评对象

入侵防范设备。

1. 测评实施

应检查入侵防范设备，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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 无线通信完整性和保密性
   * + - 1. 测评单元（L3-NCS3-13）
2. 测评指标

应采用密码技术保证无线通信过程中数据的完整性。（本条款引用自GB/T 22239.3-20XX 7.1.2.5）

1. 测评对象

移动应用设计文档和网络管理员。

1. 测评实施

应访谈网络管理员，询问是否采用加密技术保证无线网络通信过程中数据的完整性；

应检查设计、验收文档或源代码，查看是否有采用加密技术保护无线通信完整性的描述。

1. 单项判定

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

* + - * 1. 测评单元（L3-NCS3-14）

1. 测评指标

应采用密码技术保证无线通信过程中敏感信息字段或整个报文的保密性。（本条款引用自GB/T 22239.3-20XX 7.1.2.5）

测评对象

移动应用设计文档、移动应用软件和网络管理员。

测评实施

应访谈网络管理员，询问是否采用加密技术保证无线网络通信过程中数据的保密性；

应检查设计、验收文档或源代码，查看是否有采用国产加密技术保护无线通信保密性的描述；

应测试无线通信过程中重要数据是否进行了加密。

单项判定

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

1. 安全审计
   * + - 1. 测评单元（L3-NCS3-15）
2. 测评指标

应启用设备安全审计功能，审计覆盖到每个移动终端，对重要的终端行为和重要安全事件进行审计。（本条款引用自GB/T 22239.3-20XX 7.1.2.6）

1. 测评对象

无线接入网关、无线接入设备和网络管理员。

1. 测评实施

应访谈网络管理员，询问网络采用了何种审计机制，采用了哪些审计策略，用以实现对无线网络的安全审计；

应检无线接入网关及无线接入设备，是否开启安全审计功能，查看审计策略是否包括设备运行状况、网络流量、管理账户的登录及重要操作等。

1. 单项判定

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

* + - * 1. 测评单元（L3-NCS3-16）

1. 测评指标

应能对移动终端接入的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。（本条款引用自GB/T 22239.3-20XX 7.1.2.6）

1. 测评对象

无线接入网关、无线接入设备和网络管理员。

1. 测评实施

应检查审计措施是否能够对移动终端的用户接入行为及访问互联网的用户行为进行审

计和数据分析。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 网络设备防护
   * + - 1. 测评单元（L3-NCS3-17）
2. 测评指标

应能发现系统移动终端、无线接入设备、无线接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自GB/T 22239.3-20XX 7.1.2.7）

测评对象

移动终端、无线接入设备、无线接入网关设备和网络管理员。

测评实施

应访谈网络管理员，询问系统移动终端、无线接入设备、无线接入网关等设备的补丁管理采用何种机制；

应检查系统移动终端、无线接入设备、无线接入网关等设备的补丁是否得到了及时更新。

单项判定

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

* + - * 1. 测评单元（L3-NCS3-18）

1. 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。（本条款引用自GB/T 22239.3-20XX 7.1.2.7）

1. 测评对象

无线接入设备和无线接入网关。

1. 测评实施

应检查无线接入设备和无线接入网关是否关闭了“SSID广播、WEP认证” 等存在风

险的功能。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-NCS3-19）

1. 测评指标

应禁止多个AP使用同一个鉴别密钥。（本条款引用自GB/T 22239.3-20XX 7.1.2.7）

1. 测评对象

无线接入设备。

1. 测评实施

应检查无线接入设备是否分别使用了不同的鉴别密钥。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

设备和计算安全

1. 身份鉴别
   * + - 1. 测评单元（L3-ECS3-01）
2. 测评指标

应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别。（本条款引用自GB/T 22239.3-20XX 7.1.3.1）

1. 测评对象

移动终端和移动终端管理系统。

1. 测评实施

应检查移动终端登录、移动终端管理系统登录的身份鉴别策略，查看是否提供了身份鉴别措施；

应测试移动终端、移动终端管理系统的登录口令复杂度。

1. 单项判定

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

* + - * 1. 测评单元（L3-ECS3-02）

1. 测评指标

移动终端应具有登录失败处理功能，应配置并启用限制非法登录次数等措施。（本条款引用自GB/T 22239.3-20XX 7.1.3.1）

测评对象

移动终端。

测评实施

应检查移动终端是否启用了登录失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等；

应检查登录失败处理功能的具体配置，包括登录次数、超时时间等；

应测试移动终端的登录失败处理功能。

单项判定

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

1. 移动终端管控
   * + - 1. 测评单元（L3-ECS3-03）
2. 测评指标

应保证移动终端只用于处理与等级保护对象相关业务。（本条款引用自GB/T 22239.3-20XX 7.1.3.2）

1. 测评对象

移动终端和安全管理员。

1. 测评实施

应访谈安全管理员，询问移动终端管理的全流程管理策略；

应检查移动终端上安装的业务应用，查看是否只安装了必要的业务应用。

1. 单项判定

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

* + - * 1. 测评单元（L3-ECS3-04）

1. 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。（本条款引用自GB/T 22239.3-20XX 7.1.3.2）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ECS3-05）

1. 测评指标

移动终端应接受等级保护对象移动终端管理服务端的设备生命周期管理、设备远程控制、设备安全管控。（本条款引用自GB/T 22239.3-20XX 7.1.3.2）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端管理系统的安全策略，查看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、设备安全管控及设备生命周期管理等策略。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 应用管控
   * + - 1. 测评单元（L3-ECS3-06）
2. 测评指标

移动终端管理客户端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。（本条款引用自GB/T 22239.3-20XX 7.1.3.3）

测评对象

移动终端管理系统。

测评实施

应检查移动终端管理客户端是否具有软件白名单功能；

应测试使用白名单控制应用软件安装、运行。

单项判定

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

* + - * 1. 测评单元（L3-ECS3-07）

1. 测评指标

移动终端管理客户端应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问。（本条款引用自GB/T 22239.3-20XX 7.1.3.3）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查移动终端管理客户端是否具有应用软件权限控制功能；

应测试是否可以对移动终端中资源的访问进行限制。

1. 单项判定

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

* + - * 1. 测评单元（L3-ECS3-08）

1. 测评指标

移动终端管理客户端应只允许等级保护对象管理者指定证书签名的应用软件安装和运行。（本条款引用自GB/T 22239.3-20XX 7.1.3.3）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查移动终端管理客户端所允许使用的签名证书。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ECS3-09）

1. 测评指标

移动终端管理客户端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。（本条款引用自GB/T 22239.3-20XX 7.1.3.3）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查移动终端管理客户端是否具有接受移动终端管理服务端远程管控的能力。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全审计
   * + - 1. 测评单元（L3-ECS3-10）
2. 测评指标

应启用移动终端安全审计功能，对终端用户重要操作及软件行为进行审计。（本条款引用自GB/T 22239.3-20XX 7.1.3.4）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否启用安全审计功能并制定审计策略，根据审计策略对终端用户重要

操作及软件行为进行审计。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ECS3-11）

1. 测评指标

审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。（本条款引用自GB/T 22239.3-20XX 7.1.3.4）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端安全审计记录，查看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等内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ECS3-12）

1. 测评指标

应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。（本条款引用自GB/T 22239.3-20XX 7.1.3.4）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端安全审计记录的备份策略，是否能够避免受到未预期的删除、修改或覆

盖等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 入侵防范
   * + - 1. 测评单元（L3-ECS3-13）
2. 测评指标

移动终端应遵循最小安装的原则，仅安装需要的组件和应用程序。（本条款引用自GB/T 22239.3-20XX 7.1.3.5）

测评对象

移动终端。

测评实施

应检查移动终端中是否安装多余组件和应用程序；

应检查移动终端操作系统版本，查看补丁是否得到了及时更新。

单项判定

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

* + - * 1. 测评单元（L3-ECS3-14）

1. 测评指标

移动终端应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自GB/T 22239.3-20XX 7.1.3.5）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端操作系统版本，查看补丁是否得到了及时更新；

应检查移动终端是否能够发现系统漏洞并及时修补。

1. 单项判定

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

* + - * 1. 测评单元（L3-ECS3-15）

1. 测评指标

移动终端应关闭不需要的系统服务、默认共享和高危端口。（本条款引用自GB/T 22239.3-20XX 7.1.3.5）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否应关闭不需要的系统服务、默认共享和高危端口。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ECS3-16）

1. 测评指标

移动终端应能够发现用户权限异常改变的情况。（本条款引用自GB/T 22239.3-20XX 7.1.3.5）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否能够发现用户权限异常改变的情况。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 恶意代码防范
   * + - 1. 测评单元（L3-ECS3-17）
2. 测评指标

移动终端应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库。（本条款引用自GB/T 22239.3-20XX 7.1.3.6）

测评对象

移动终端和安全管理员

测评实施

应访谈安全管理员，询问移动终端恶意代码防护策略以及定期查杀频率；

应检查移动终端是否安装了查杀恶意代码的防恶意代码产品；

应检查移动终端防恶意代码产品软件版本和恶意代码库版本。

单项判定

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

* + - * 1. 测评单元（L3-ECS3-18）

1. 测评指标

移动终端应支持移动业务应用软件仅运行在安全容器内，防止被恶意代码攻击。（本条款引用自GB/T 22239.3-20XX 7.1.3.6）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否支持移动业务应用软件仅运行在安全容器内，防止被恶意代码攻击。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 资源控制
   * + - 1. 测评单元（L3-ECS3-19）
2. 测评指标

应将移动终端处理访问不同等级等级保护对象的运行环境进行系统级隔离。（本条款引用自GB/T 22239.3-20XX 7.1.3.7）

1. 测评对象

安全管理员。

1. 测评实施

应访谈安全管理员，询问移动终端采用哪种安全隔离手段或措施对不同等级等级保护对

象进行系统级隔离。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ECS3-20）

1. 测评指标

应将移动终端处理访问等级保护对象的运行环境与非处理访问等级保护对象运行环境进行系统级隔离。（本条款引用自GB/T 22239.3-20XX 7.1.3.7）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否采用安装双操作系统进行安全隔离。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ECS3-21）

1. 测评指标

应限制用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权。（本条款引用自GB/T 22239.3-20XX 7.1.3.7）

1. 测评对象

移动终端。

1. 测评实施

应检查对移动终端的用户或进程可访问资源的限定，防止移动终端被提权。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

应用和数据安全

1. 身份鉴别
   * + - 1. 测评单元（L3-ADS3-01）
2. 测评指标

使用口令登录时，应强制用户首次登录时修改初始口令，对用户的鉴别信息进行复杂度检查。（本条款引用自GB/T 22239.3-20XX 7.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看是否提供身份标识和鉴别功能；

应检查移动应用软件，查看是否采用了措施保证身份标识具有唯一性，是否强制用户首次登录时修改初始口令，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用。

1. 单项判定

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

* + - * 1. 测评单元（L3-ADS3-02）

1. 测评指标

用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。（本条款引用自GB/T 22239.3-20XX 7.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施

应测试移动应用软件，可通过重置鉴别信息，查看是否成功，验证鉴别信息重置是否有效。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ADS3-03）

1. 测评指标

移动应用软件应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求。（本条款引用自GB/T 22239.3-20XX 7.1.4.1）

测评对象

移动应用软件。

测评实施

应测试移动应用软件，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效；

应渗透测试移动应用软件，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。

单项判定

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

* + - * 1. 测评单元（L3-ADS3-04）

1. 测评指标

移动应用软件应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。（本条款引用自GB/T 22239.3-20XX 7.1.4.1）

1. 测评对象

移动应用软件和应用管理员。

1. 测评实施

应检查移动应用软件，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数；

应测试移动应用软件，可通过多次输入错误的密码，验证登录失败处理功能是否有效。

1. 单项判定

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

* + - * 1. 测评单元（L3-ADS3-05）

1. 测评指标

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。（本条款引用自GB/T 22239.3-20XX 7.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看是否采用了两种或两种以上组合的身份鉴别技术来进行身份

鉴别。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 软件审核与检测
   * + - 1. 测评单元（L3-ADS3-06）
2. 测评指标

应保证等级保护对象业务移动应用软件开发后、上线前经专业测评机构安全检测。（本条款引用自GB/T 22239.3-20XX 7.1.4.2）

测评对象

移动应用软件和系统建设负责人。

测评实施

应访谈系统建设负责人，询问是否在移动应用软件开发结束后，上线前进行了专业测评机构的安全检测；

应检查移动应用软件，查看是否有专业测评机构安全检测报告。

单项判定

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

1. 数据完整性
   * + - 1. 测评单元（L3-ADS3-07）
2. 测评指标

移动应用软件应采用密码技术保证通信过程中数据的完整性。（本条款引用自GB/T 22239.3-20XX 7.1.4.3）

1. 测评对象

移动应用软件和应用管理员。

1. 测评实施

应访谈应用管理员，采用哪种密码技术保证通信过程中数据的完整性；

应检查移动应用软件设计、验收文档或源代码，查看是否有关于能检测数据通信和存储过程中完整性受到破坏的描述；

应测试移动应用软件，可通过获取通信双方的数据包，查看通信报文中是否进行完整性保护。

1. 单项判定

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

* + - * 1. 测评单元（L3-ADS3-08）

1. 测评指标

移动应用软件应采用校验技术或密码技术保证重要数据存储时的完整性，并在检测到完整性错误时采取必要的恢复措施。（本条款引用自GB/T 22239.3-20XX 7.1.4.3）

测评对象

移动应用软件和应用管理员。

测评实施

应检查移动应用软件，查看是否配备检测系统管理数据、鉴别信息和业务数据在存储过程中完整性受到破坏的功能；

应检查移动应用软件采取的恢复措施。

单项判定

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

1. 数据保密性
   * + - 1. 测评单元（L3-ADS3-09）
2. 测评指标

移动应用软件应采用密码技术保证重要数据在本地存储时的保密性。（本条款引用自GB/T 22239.3-20XX 7.1.4.4）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看其鉴别信息和主要数据是否采用加密或其他有效措施实现了

存储保密性。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ADS3-10）

1. 测评指标

应确保移动应用软件之间的重要数据不能被互操作。（本条款引用自GB/T 22239.3-20XX 7.1.4.4）

1. 测评对象

移动应用软件。

1. 测评实施

应测试移动应用软件，验证移动应用软件之间的重要数据是否能被互操作。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ADS3-11）

1. 测评指标

应确保移动应用软件数据文件所在的存储空间，被释放或重新分配前可得到完全清除。（本条款引用自GB/T 22239.3-20XX 7.1.4.4）

1. 测评对象

系统设计文档和移动应用软件。

1. 测评实施

应检查设计、验收文档或源代码，查看其是否有关于系统在释放或再分配数据文件所在存储空间给其他用户前如何将其进行完全清除的描述；

应测试移动应用软件，用某用户登录系统并进行操作后，在该用户退出后用另一用户登录，试图操作（读取、修改或删除等）其他用户产生的文件、目录和数据库记录等资源，查看操作是否成功，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）。

1. 单项判定

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

* + - * 1. 测评单元（L3-ADS3-12）

1. 测评指标

移动应用软件应对通信过程中的敏感信息字段或整个报文进行密码加密。（本条款引用自GB/T 22239.3-20XX 7.1.4.4）

测评对象

移动应用软件。

测评实施

应检查移动应用软件，查看其管理数据、鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输保密性；

应测试移动应用软件，可通过用嗅探工具获取通信数据包，查看是否为密文。

单项判定

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

1. 备份和恢复
   * + - 1. 测评单元（L3-ADS3-13）
2. 测评指标

移动应用软件应仅采集和保存业务必需的用户个人信息。（本条款引用自GB/T 22239.3-20XX 7.1.4.5）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看移动应用软件所采集和保存的用户个人信息是否为业务必须

的信息。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ADS3-14）

1. 测评指标

应禁止移动应用软件未授权访问、使用用户个人信息。（本条款引用自GB/T 22239.3-20XX 7.1.4.5）

1. 测评对象

移动应用软件。

1. 测评实施

应测试移动应用软件，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；

应测试移动应用软件，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限；

应渗透测试移动应用软件，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。

1. 单项判定

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

* + - * 1. 测评单元（L3-ADS3-15）

1. 测评指标

移动应用软件应提供移动终端重要数据备份与恢复功能。（本条款引用自GB/T 22239.3-20XX 7.1.4.5）

测评对象

移动应用软件。

测评实施

应检查是否对移动应用软件的重要信息进行了备份；

应检查备份方式（如是否为完全数据备份）、频率和介质存放方式是否达到相关标准的要求，是否定期对备份数据进行恢复测试。

单项判定

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

* + - * 1. 测评单元（L3-ADS3-16）

1. 测评指标

移动应用软件应将重要数据定时批量传送至备用位置。（本条款引用自GB/T 22239.3-20XX 7.1.4.5）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件是否将重要信息定时批量传送至备用位置，以及备份方式（如是否为完全数据备份）、频率和介质存放方式等。

1. 单项判定
   * 如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。
2. 安全管理单项测评

安全策略和管理制度

1. 管理制度
   * + - 1. 测评单元（L3-PSS3-01）
2. 测评指标

应建立等级保护对象移动互联安全管理制度，并纳入等级保护对象管理安全制度；（本条款引用自GB/T 22239.3-20XX 7.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括移动互联安全管理规范等相关内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

* + - * 1. 测评单元（L3-PSS3-02）

1. 测评指标

应对管理人员或移动终端操作人员执行的日常管理操作建立操作规程；（本条款引用自GB/T 22239.3-20XX 7.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括人员日常管理操作规程。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

* + - * 1. 测评单元（L3-PSS3-03）

1. 测评指标

应在等级保护对象管理制度中建立移动终端管理服务端操作使用管理规定。（本条款引用自GB/T 22239.3-20XX 7.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括移动终端管理服务端操作使用的相关内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

安全管理机构和人员

1. 岗位设置
   * + - 1. 测评单元（L3-ORS3-01）
2. 测评指标

应将移动互联管理纳入等级保护对象管理员职责；（本条款引用自GB/T 22239.3-20XX 7.2.2.1）

1. 测评对象

信息安全负责人和管理制度类文档。

1. 测评实施

应访谈信息安全负责人，询问是否设置了移动互联相关管理岗位，岗位职责是否明确。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ORS3-02）

1. 测评指标

应设立移动互联信息安全管理工作的职能部门，并制定各负责人的职责；（本条款引用自GB/T 22239.3-20XX 7.2.2.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查部门与岗位职责文档，查看是否明确了移动互联安全部门、安全岗位的职责。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ORS3-03）

1. 测评指标

应为移动终端管理服务端设置专职管理员、操作员，并纳入职能部门职责。（本条款引用自GB/T 22239.3-20XX 7.2.2.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查是否针对移动终端管理服务端设置了专职管理员岗位、操作员岗位，并纳入职能

部门职责。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

1. 人员配备
   * + - 1. 测评单元（L3-ORS3-04）
2. 测评指标

应保证移动终端管理服务端配备专职管理员、操作员和审计员。（本条款引用自GB/T 22239.3-20XX 7.2.2.2）

1. 测评对象

信息安全负责人和记录表单类文档。

1. 测评实施
2. 应访谈信息安全负责人，询问是否设置了移动终端管理端专职管理员、操作员及审计员；
3. 应检查岗位职责文档，查看是否明确了移动终端管理端相关岗位的职责。
4. 单项判定

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

1. 授权和审批
   * + - 1. 测评单元（L3-ORS3-05）
2. 测评指标

应根据各个部门和岗位的职责明确移动互联管理授权审批事项、审批部门和批准人；（本条款引用自GB/T 22239.3-20XX 7.2.2.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查岗位职责文档，查看移动互联管理授权审批事项、审批部门和审批人是否明确。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ORS3-06）

1. 测评指标

应针对移动互联系统变更、重要操作、物理访问和系统接入等事项执行审批过程；（本条款引用自GB/T 22239.3-20XX 7.2.2.3）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否针对移动应用系统变更、重要操作、物理访问和系统接入等事项执行审批过

程，是否有相关审批记录表单。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ORS3-07）

1. 测评指标

应保证移动终端管理服务端设置专职管理员、操作员权限由审批部门或批准人批准。（本条款引用自GB/T 22239.3-20XX 7.2.2.3）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查岗位职责文档，或会议纪要，查看移动终端管理服务端的专职管理员、操作员权

限的审批过程是否合理，是否由审批部门或审批人批准。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全意识教育和培训
   * + - 1. 测评单元（L3-ORS3-08）
2. 测评指标

应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；（本条款引用自GB/T 22239.3-20XX 7.2.2.4）

1. 测评对象

信息安全负责人。

1. 测评实施

应访谈信息安全负责人，询问是否对各类人员进行移动互联安全教育和岗位技能培训，

告知相关的安全知识、安全责任和惩戒措施等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

* + - * 1. 测评单元（L3-ORS3-09）

1. 测评指标

应对移动终端管理服务端设置专职管理员、操作员进行专项安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。（本条款引用自GB/T 22239.3-20XX 7.2.2.4）

1. 测评对象

信息安全负责人。

1. 测评实施

应访谈信息安全负责人，询问是否对移动终端管理服务端的专职管理员、操作员进行移

动互联安全教育和岗位技能培训，告知相关的安全知识、安全责任和惩戒措施等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

安全建设管理

1. 安全方案设计
   * + - 1. 测评单元（L3-CMS3-01）
2. 测评指标

应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施；（本条款引用自GB/T 22239.3-20XX 7.2.3.1）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否依据风险分析的结果补充和调整过安全措施，具体做过哪些调整。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-02）

1. 测评指标

应根据等级保护对象的安全保护等级进行移动互联安全方案设计，并纳入系统总体方案设计；（本条款引用自GB/T 22239.3-20XX 7.2.3.1）

1. 测评对象

安全规划设计类文档。

1. 测评实施
2. 应检查移动应用系统的安全设计方案，查看方案是否描述系统的安全保护等级，是否描述系统的安全保护策略，是否根据系统的安全级别选择了安全措施；
3. 应检查移动应用系统的安全设计方案，查看是否详细描述安全措施的实现内容，是否有安全产品的功能、性能和部署等描述，是否有安全建设的费用和计划等。
4. 单项判定

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

* + - * 1. 测评单元（L3-CMS3-03）

1. 测评指标

应组织相关部门和安全专家对系统移动互联安全方案设计进行论证和审定，经过批准后才能正式实施。（本条款引用自GB/T 22239.3-20XX 7.2.3.1）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查相关评审记录，查看在系统建设实施前，是否对系统移动互联安全方案进行论证

和审定。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

1. 产品采购和使用
   * + - 1. 测评单元（L3-CMS3-04）
2. 测评指标

应确保移动互联安全产品采购和使用符合国家的有关规定；（本条款引用自GB/T 22239.3-20XX 7.2.3.2）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈移动应用系统建设负责人，询问移动应用系统使用的有关信息安全产品是否符合

国家的有关规定，如安全产品获得了销售许可证等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-05）

1. 测评指标

相关密码产品使用应符合国家密码管理相关规定。（本条款引用自GB/T 22239.3-20XX 7.2.3.2）

1. 测评对象

密码产品。

1. 测评实施

应检查移动应用系统所使用的密码产品的相关证书。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 移动应用软件开发
   * + - 1. 测评单元（L3-CMS3-06）
2. 测评指标

应要求对移动业务应用软件开发者进行资格审查；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否对开发者进行资格审查。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-07）

1. 测评指标

应确保开发移动业务应用软件的签名证书合法性；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

软件的签名证书。

1. 测评实施

应检查开发移动业务应用软件的签名证书是否具有合法性。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-08）

1. 测评指标

应要求移动应用软件开发完提供软件设计文档、使用指南及软件源代码；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

软件开发类文档。

1. 测评实施

应检查是否具备软件设计文档，使用指南及软件源代码。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-09）

1. 测评指标

应要求应用软件开发使用的工具来源可靠；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，检查应用软件开发使用的工具来源。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-010）

1. 测评指标

自行开发移动应用软件，应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，检查开发环境与实际运行环境物理是否分开，测试数据和测试结果是否受到控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-011）

1. 测评指标

自行开发移动应用软件，应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查是否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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-012）

1. 测评指标

自行开发移动应用软件，应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查是否包含移动应用软件设计的相关文档并对文档使用进行控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-013）

1. 测评指标

自行开发移动应用软件，应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；（本条款引用自GB/T 22239.3-20XX 7.2.3.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查是否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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 工程实施
   * + - 1. 测评单元（L3-CMS3-014）
2. 测评指标

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。（本条款引用自GB/T 22239.3-20XX 7.2.3.4）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否指定专门部门或人员对移动互联工程实施过程进行进度和质量控制，具体由何部门/何人负责。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 测试验收
   * + - 1. 测评单元（L3-CMS3-015）
2. 测评指标

应对系统的移动互联部分进行安全性测试验收。（本条款引用自GB/T 22239.3-20XX 7.2.3.5）

1. 测评对象

系统建设负责人。

1. 测评实施
2. 应访谈系统建设负责人，询问在移动应用系统建设完成后是否对其进行安全性测试验收；
3. 应检查是否具有移动互联工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；
4. 应检查是否具有移动应用软件测试验收报告。
5. 单项判定

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

1. 系统交付
   * + - 1. 测评单元（L3-CMS3-016）
2. 测评指标

应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；（本条款引用自GB/T 22239.3-20XX 7.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否具有移动应用系统交付清单，查看交付清单是否说明系统交付的各类设备、

软件、文档等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-017）

1. 测评指标

应对负责系统移动互联运行维护的技术人员进行相应的技能培训；（本条款引用自GB/T 22239.3-20XX 7.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应访谈系统建设负责人，询问移动应用软件正式运行前是否对运行维护人员进行过培训，

针对哪些方面进行过培训。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-018）

1. 测评指标

应确保提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档；（本条款引用自GB/T 22239.3-20XX 7.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-019）

1. 测评指标

应确保提供移动终端管理服务端建设过程中的文档和指导用户进行系统运行维护的文档。（本条款引用自GB/T 22239.3-20XX 7.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否提供移动终端管理服务端建设过程中的文档和指导用户进行系统运行维护

的文档。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全服务商选择
   * + - 1. 测评单元（L3-CMS3-020）
2. 测评指标

应确保移动互联安全服务商的选择符合国家的有关规定；（本条款引用自GB/T 22239.3-20XX 7.2.3.7）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问系统选择的安全服务商有哪些，是否符合国家有关规定。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-021）

1. 测评指标

应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任；（本条款引用自GB/T 22239.3-20XX 7.2.3.7）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否具有与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是

否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-022）

1. 测评指标

应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；（本条款引用自GB/T 22239.3-20XX 7.2.3.7）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查与服务商签订的相关协议等文档，查看其内容是否协议的有效期限和责任人的签

字等整个服务供应链各方需履行的信息安全相关义务。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-CMS3-023）

1. 测评指标

应选择安全可靠应用软件分发运营商。（本条款引用自GB/T 22239.3-20XX 7.2.3.7）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人。检查应用软件分发运营商的相关资质与相关证书。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全运维管理

1. 资产管理
   * + - 1. 测评单元（L3-MMS3-01）
2. 测评指标

应编制并保存与等级保护对象相关的移动终端资产清单，包括资产责任部门、重要程度和使用人等内容；（本条款引用自GB/T 22239.3-20XX 7.2.4.1）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查资产清单，查看是否针对责任部门、重要程度和使用人等内容编制资产清单。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-02）

1. 测评指标

应根据资产的重要程度对移动终端进行标识管理，根据其价值选择相应的管理措施。（本条款引用自GB/T 22239.3-20XX 7.2.4.1）

1. 测评对象

资产清单、管理制度类文档、记录表单类文档。

1. 测评实施

应检查资产清单及资产管理文档，查看是否根据资产的重要程度对移动终端进行标识管

理，根据其价值选择相应的管理措施。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 设备维护管理
   * + - 1. 测评单元（L3-MMS3-03）
2. 测评指标

应对各种移动互联设备（包括无线接入设备及移动终端）维护纳入等级保护对象进行管理；（本条款引用自GB/T 22239.3-20XX 7.2.4.2）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查设备管理制度，查看是否将各种移动互联设备（包括无线接入设备）维护纳入管理制度内并进行管理。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-04）

1. 测评指标

应确保移动终端在报废或重用前应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；（本条款引用自GB/T 22239.3-20XX 7.2.4.2）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查管理制度类文档文档，查看设备使用管理流程，确认设备在报废、重用前采取必要的技术措施，确保设备上的敏感信息被彻底消除。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-05）

1. 测评指标

应在移动终端设备丢失后进行远程数据擦除。（本条款引用自GB/T 22239.3-20XX 7.2.4.2）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查管理制度类文档，移动终端设备丢失后应进行远程数据擦除，确保数据不会外泄。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 风险评估和漏洞管理
   * + - 1. 测评单元（L3-MMS3-06）
2. 测评指标

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。（本条款引用自GB/T 22239.3-20XX 7.2.4.3）

1. 测评对象

安全管理员和记录表单类文档。

1. 测评实施
2. 应访谈安全管理员，询问采取哪些措施识别移动互联安全漏洞和隐患，并在评估后对发现的安全漏洞和隐患进行修补；
3. 应检查移动互联安全漏洞管理记录。
4. 单项判定

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

1. 应用软件来源管理
   * + - 1. 测评单元（L3-MMS3-07）
2. 测评指标

应保证移动终端安装、运行的应用软件来自等级保护对象管理者指定证书签名或可靠分发渠道；（本条款引用自GB/T 22239.3-20XX 7.2.4.4）

1. 测评对象

安全管理员。

1. 测评实施

应访谈安全管理员，移动终端安装、运行的应用软件是否来自信息系统管理者指定证书

签名或可靠分发渠道。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-08）

1. 测评指标

应保证移动终端安装、运行的移动应用软件由经审核的开发者开发。（本条款引用自GB/T 22239.3-20XX 7.2.4.4）

1. 测评对象

安全管理员。

1. 测评实施

应访谈安全管理员，检查移动终端安装、运行的移动应用软件是否由经审核的开发者开发。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 恶意代码防范管理
   * + - 1. 测评单元（L3-MMS3-09）
2. 测评指标

应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；（本条款引用自GB/T 22239.3-20XX 7.2.4.5）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问是否对员工进行移动互联基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-010）

1. 测评指标

应对截获的恶意代码进行及时分析处理。（本条款引用自GB/T 22239.3-20XX 7.2.4.5）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问移动终端采用何种机制对移动应用软件的使用进行管理。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-011）

1. 测评指标

应保证移动终端管理服务端将移动应用软件运行策略推送给移动终端。（本条款引用自GB/T 22239.3-20XX 7.2.4.5）

1. 测评对象

移动终端管理系统。

1. 测评实施

应查看移动终端管理服务端是否能够将移动应用软件运行策略推送给移动终端。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 配置管理
   * + - 1. 测评单元（L3-MMS3-012）
2. 测评指标

移动终端管理服务端应记录和保存移动终端基本配置信息，包括操作系统、软件组件版本、移动终端各种设备或软件组件的配置参数等；（本条款引用自GB/T 22239.3-20XX 7.2.4.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查记录表单类文档，查看配置记录是否包含完整的移动终端基本配置信息，包括操作系统、软件组件版本、移动终端各种设备或软件组件的配置参数等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-013）

1. 测评指标

移动终端管理服务端应将移动终端基本配置信息改变纳入系统变更范畴，实施对配置信息改变控制，并及时更新基本配置信息库；（本条款引用自GB/T 22239.3-20XX 7.2.4.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查记录表单类文档，查看移动终端基本配置信息改变是否被纳入系统变更范畴，是否实施对配置信息改变控制，并及时更新基本配置信息库。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-014）

1. 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。（本条款引用自GB/T 22239.3-20XX 7.2.4.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查记录表单类文档，查看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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 监控和审计管理
   * + - 1. 测评单元（L3-MMS3-015）
2. 测评指标

应确保移动终端管理服务端对移动终端状态、资源使用、软件运行等进行监控和审计；（本条款引用自GB/T 22239.3-20XX 7.2.4.7）

1. 测评对象

系统运维负责人。

1. 测评实施
2. 应访谈系统运维负责人，询问移动应用系统采用何种管理机制；
3. 应查看移动终端管理服务端的管理功能，是否能够对移动终端状态、资源使用、软件运行等进行监控和审计。
4. 单项判定

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

* + - * 1. 测评单元（L3-MMS3-016）

1. 测评指标

应对上线后的业务移动应用软件进行监测。（本条款引用自GB/T 22239.3-20XX 7.2.4.7）

1. 测评对象

移动终端管理系统。

1. 测评实施

应查看移动终端管理服务端的管理功能，是否能够对业务移动应用软件进行监测。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 备份与恢复管理
   * + - 1. 测评单元（L3-MMS3-017）
2. 测评指标

应识别需要定期备份的移动终端中的重要业务信息、系统数据及软件系统等；（本条款引用自GB/T 22239.3-20XX 7.2.4.8）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问是否识别出需要定期备份移动应用软件中的业务信息、系统数据和软件系统，主要有哪些。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-018）

1. 测评指标

应规定备份信息的备份方式、备份频度、存储介质、保存期等；（本条款引用自GB/T 22239.3-20XX 7.2.4.8）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查管理制度类文档，查看其是否明确了备份方式、备份频度、存储介质和保存期等方面内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-019）

1. 测评指标

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。（本条款引用自GB/T 22239.3-20XX 7.2.4.8）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查管理制度类文档，查看其是否明确了业务数据的重要程度，是否制定了备份、恢复策略，是否明确了备份恢复措施。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全事件处置
   * + - 1. 测评单元（L3-MMS3-020）
2. 测评指标

应报告所发现的移动互联安全弱点和可疑事件；（本条款引用自GB/T 22239.3-20XX 7.2.4.9）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问是否有报告所发现的移动互联安全弱点和可疑事件的相关流程与文件。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-021）

1. 测评指标

应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责；（本条款引用自GB/T 22239.3-20XX 7.2.4.9）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查移动互联安全事件的报告和处置流程，查看其是否明确了安全事件的现场处理、

事件报告和后期恢复的管理职责等方面内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L3-MMS3-022）

1. 测评指标

应针对移动互联系统发生的安全事件制定应急处置预案。（本条款引用自GB/T 22239.3-20XX 7.2.4.9）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查应急预案，查看是否建立了针对移动互联系统安全事件的专项应急处置预案。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

第四级测评要求

1. 安全技术单项测评

物理和环境安全

1. 物理位置选择
   * + - 1. 测评单元（L4-PES3-01）
2. 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。（本条款引用自GB/T 22239.3-20XX 8.1.1）

1. 测评对象

无线接入设备和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问无线网络设备的覆盖范围与处理能力是否满足业务需求；
3. 应检查无线接入设备的物理位置与无线信号的覆盖范围；
4. 应使用无线信号探测工具测试无线信号的覆盖范围，判断是否存在过度覆盖的情况。
5. 单项判定

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

网络和通信安全

1. 结构安全
   * + - 1. 测评单元（L4-NCS3-01）
2. 测评指标

应保证无线接入网关的处理能力满足业务高峰期需要。（本条款引用自GB/T 22239.3-20XX 8.1.2.1）

1. 测评对象

无线接入网关和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问无线接入网关的业务处理能力是否满足基本业务需求；
3. 应检查一段业务高峰时期内无线接入网关的CPU使用率和内存使用率。
4. 单项判定

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

* + - * 1. 测评单元（L4-NCS3-02）

1. 测评指标

应保证无线接入设备的带宽满足业务高峰期需要。（本条款引用自GB/T 22239.3-20XX 8.1.2.1）

1. 测评对象

无线接入设备和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问无线接入设备的网络带宽；
3. 应检查一段业务高峰时期内带宽使用峰值，判断是否满足业务需求。
4. 单项判定

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

* + - * 1. 测评单元（L4-NCS3-03）

1. 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或国产算法进行加密。（本条款引用自GB/T 22239.3-20XX 8.1.2.1）

1. 测评对象

无线接入设备。

1. 测评实施

应检查无线接入设备是否开启接入认证功能，且认证过程采用认证服务器或国产算法进

行加密。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 边界防护
   * + - 1. 测评单元（L4-NCS3-04）
2. 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。（本条款引用自GB/T 22239.3-20XX 8.1.2.2）

1. 测评对象

无线接入网关。

1. 测评实施

应检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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 访问控制
   * + - 1. 测评单元（L4-NCS3-05）
2. 测评指标

应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信。（本条款引用自GB/T 22239.3-20XX 8.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关设置的访问控制规则有哪些，检查是否只开启了必要的通信接口。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-NCS3-06）

1. 测评指标

应对来自移动终端的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过。（本条款引用自GB/T 22239.3-20XX 8.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关，查看配置的访问控制策略是否对数据流量、数据包和协议等进行检查，并进行数据流控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-NCS3-07）

1. 测评指标

应在无线接入网关上对进出无线网络的数据进行内容过滤。（本条款引用自GB/T 22239.3-20XX 8.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关是否具备并开启了数据内容过滤功能。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-NCS3-08）

1. 测评指标

应设置访问控制规则限制移动终端可访问的等级保护对象资源。（本条款引用自GB/T 22239.3-20XX 8.1.2.3）

1. 测评对象

无线接入网关。

1. 测评实施

应检查无线接入网关及无线接入设备，是否设置了访问控制规则，限制终端用户的访问

权限。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 入侵防范
   * + - 1. 测评单元（L4-NCS3-09）
2. 测评指标

应能够检测、记录、定位非授权无线接入设备。（本条款引用自GB/T 22239.3-20XX 8.1.2.4）

1. 测评对象

入侵防范设备和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问无线网络的入侵防范措施有哪些；询问无线网络入侵防范设备具备哪些防范功能；
3. 应检查入侵防范设备是否能够检测、记录、定位非授权无线接入设备。
4. 单项判定

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

* + - * 1. 测评单元（L4-NCS3-10）

1. 测评指标

应能够对非授权移动终端接入的行为进行检测、记录、定位并阻断。（本条款引用自GB/T 22239.3-20XX 8.1.2.4）

1. 测评对象

入侵防范设备。

1. 测评实施

应检查入侵防范设备是否能够检测、记录、定位并阻断非授权无线接入终端的接入行为。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-NCS3-11）

1. 测评指标

应具备对针对无线接入设备的网络扫描、DoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位。（本条款引用自GB/T 22239.3-20XX 8.1.2.4）

1. 测评对象

入侵防范设备。

1. 测评实施
2. 应检查无线网络入侵防范设备，是否能够对网络扫描、DoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；
3. 应检查网络入侵防范设备的规则库版本，查看其规则库是否及时更新。
4. 单项判定

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

* + - * 1. 测评单元（L4-NCS3-12）

1. 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。（本条款引用自GB/T 22239.3-20XX 8.1.2.4）

1. 测评对象

入侵防范设备。

1. 测评实施

应检查入侵防范设备，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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 无线通信完整性和保密性
   * + - 1. 测评单元（L4-NCS3-13）
2. 测评指标

应采用国产密码技术保证无线通信过程中数据的完整性。（本条款引用自GB/T 22239.3-20XX 8.1.2.5）

1. 测评对象

移动应用设计文档和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问是否采用加密技术保证无线网络通信过程中数据的完整性；
3. 应检查设计、验收文档或源代码，查看是否有采用加密技术保护无线通信完整性的描述。
4. 单项判定

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

* + - * 1. 测评单元（L4-NCS3-14）

1. 测评指标

应采用国产密码技术保证无线通信过程中敏感信息字段或整个报文的保密性。（本条款引用自GB/T 22239.3-20XX 8.1.2.5）

1. 测评对象

移动应用设计文档、移动应用软件和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问是否采用加密技术保证无线网络通信过程中数据的保密性；
3. 应检查设计、验收文档或源代码，查看是否有采用国产加密技术保护无线通信保密性的描述；
4. 应测试无线通信过程中的重要数据是否进行了加密。
5. 单项判定

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

1. 安全审计
   * + - 1. 测评单元（L4-NCS3-15）
2. 测评指标

应启用设备安全审计功能，审计覆盖到每个移动终端，对所有终端行为和所有安全事件进行审计。（本条款引用自GB/T 22239.3-20XX 8.1.2.6）

1. 测评对象

无线接入网关、无线接入设备和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问网络采用了何种审计机制，采用了哪些审计策略，用以实现对无线网络的安全审计；
3. 应检无线接入网关及无线接入设备，是否开启安全审计功能，查看审计策略是否包括设备运行状况、网络流量、管理账户的登录及重要操作等。
4. 单项判定

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

* + - * 1. 测评单元（L4-NCS3-16）

1. 测评指标

应能对移动终端接入的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。（本条款引用自GB/T 22239.3-20XX 8.1.2.6）

1. 测评对象

无线接入网关、无线接入设备和网络管理员。

1. 测评实施

应检查审计措施是否能够对移动终端的用户接入行为及访问互联网的用户行为进行审

计和数据分析。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 网络设备防护
   * + - 1. 测评单元（L4-NCS3-17）
2. 测评指标

应能发现系统移动终端、无线接入设备、无线接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自GB/T 22239.3-20XX 8.1.2.7）

1. 测评对象

移动终端、无线接入设备、无线接入网关设备和网络管理员。

1. 测评实施
2. 应访谈网络管理员，询问系统移动终端、无线接入设备、无线接入网关等设备的补丁管理采用何种机制；
3. 应检查系统移动终端、无线接入设备、无线接入网关等设备的补丁是否得到了及时更新。
4. 单项判定

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

* + - * 1. 测评单元（L4-NCS3-18）

1. 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。（本条款引用自GB/T 22239.3-20XX 8.1.2.7）

1. 测评对象

无线接入设备和无线接入网关。

1. 测评实施

应检查无线接入设备和无线接入网关是否关闭了“SSID广播、WEP认证” 等存在风

险的功能。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-NCS3-19）

1. 测评指标

应禁止多个AP使用同一个鉴别密钥。（本条款引用自GB/T 22239.3-20XX 8.1.2.7）

1. 测评对象

无线接入设备。

1. 测评实施

应检查无线接入设备是否分别使用了不同的鉴别密钥。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

设备和计算安全

1. 身份鉴别
   * + - 1. 测评单元（L4-ECS3-01）
2. 测评指标

应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别。（本条款引用自GB/T 22239.3-20XX 8.1.3.1）

1. 测评对象

移动终端和移动终端管理系统。

1. 测评实施
2. 应检查移动终端登录、移动终端管理系统登录的身份鉴别策略，查看是否提供了身份鉴别措施；
3. 应测试移动终端、移动终端管理系统的登录口令复杂度。
4. 单项判定

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

* + - * 1. 测评单元（L4-ECS3-02）

1. 测评指标

移动终端应具有登录失败处理功能，应配置并启用限制非法登录次数等措施。（本条款引用自GB/T 22239.3-20XX 8.1.3.1）

1. 测评对象

移动终端。

1. 测评实施
2. 应检查移动终端是否启用了登录失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等；
3. 应检查登录失败处理功能的具体配置，包括登录次数、超时时间等；
4. 应测试移动终端的登录失败处理功能。
5. 单项判定

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

1. 移动终端管控
   * + - 1. 测评单元（L4-ECS3-03）
2. 测评指标

应保证移动终端只用于处理与等级保护对象相关业务。（本条款引用自GB/T 22239.3-20XX 8.1.3.2）

1. 测评对象

移动终端和安全管理员。

1. 测评实施
2. 应访谈安全管理员，询问移动终端管理的全流程管理策略；
3. 应检查移动终端上安装的业务应用，查看是否只安装了必要的业务应用。
4. 单项判定

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

* + - * 1. 测评单元（L4-ECS3-04）

1. 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。（本条款引用自GB/T 22239.3-20XX 8.1.3.2）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-05）

1. 测评指标

移动终端应接受等级保护对象移动终端管理服务端的设备生命周期管理、设备远程控制、设备安全管控。（本条款引用自GB/T 22239.3-20XX 8.1.3.2）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端管理系统的安全策略，查看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、设备安全管控及设备生命周期管理等策略。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 应用管控
   * + - 1. 测评单元（L4-ECS3-06）
2. 测评指标

移动终端管理客户端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。（本条款引用自GB/T 22239.3-20XX 8.1.3.3）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查移动终端管理客户端是否具有软件白名单功能，并根据白名单控制应用软件安装、

运行。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-07）

1. 测评指标

移动终端管理客户端应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问。（本条款引用自GB/T 22239.3-20XX 8.1.3.3）

1. 测评对象

移动终端管理系统。

1. 测评实施
2. 应检查移动终端管理客户端是否具有应用软件权限控制功能；
3. 应测试是否可以对移动终端中资源的访问进行限制。
4. 单项判定

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

* + - * 1. 测评单元（L4-ECS3-08）

1. 测评指标

移动终端管理客户端应只允许等级保护对象管理者指定证书签名的应用软件安装和运行。（本条款引用自GB/T 22239.3-20XX 8.1.3.3）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查移动终端管理客户端所允许使用的签名证书。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-09）

1. 测评指标

移动终端管理客户端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。（本条款引用自GB/T 22239.3-20XX 8.1.3.3）

1. 测评对象

移动终端管理系统。

1. 测评实施

应检查移动终端管理客户端是否具有接受移动终端管理服务端远程管控的能力。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全审计
   * + - 1. 测评单元（L4-ECS3-10）
2. 测评指标

应启用移动终端安全审计功能，对终端用户所有操作及软件行为进行审计。（本条款引用自GB/T 22239.3-20XX 8.1.3.4）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否启用安全审计功能并制定审计策略，根据审计策略对终端用户重要

操作及软件行为进行审计。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-11）

1. 测评指标

审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。（本条款引用自GB/T 22239.3-20XX 8.1.3.4）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端安全审计记录，查看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等内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-12）

1. 测评指标

应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。（本条款引用自GB/T 22239.3-20XX 8.1.3.4）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端安全审计记录的备份策略，是否能够避免受到未预期的删除、修改或覆

盖等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 入侵防范
   * + - 1. 测评单元（L4-ECS3-13）
2. 测评指标

移动终端应遵循最小安装的原则，仅安装需要的组件和应用程序。（本条款引用自GB/T 22239.3-20XX 8.1.3.5）

1. 测评对象

移动终端。

1. 测评实施
2. 应检查移动终端中是否安装多余组件和应用程序；
3. 应检查移动终端操作系统版本，查看补丁是否得到了及时更新。
4. 单项判定

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

* + - * 1. 测评单元（L4-ECS3-14）

1. 测评指标

移动终端应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。（本条款引用自GB/T 22239.3-20XX 8.1.3.5）

1. 测评对象

移动终端。

1. 测评实施
2. 应检查移动终端操作系统版本，查看补丁是否得到了及时更新；
3. 应检查移动终端是否能够发现系统漏洞并及时修补。
4. 单项判定

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

* + - * 1. 测评单元（L4-ECS3-15）

1. 测评指标

移动终端应关闭不需要的系统服务、默认共享和不需要的端口。（本条款引用自GB/T 22239.3-20XX 8.1.3.5）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否应关闭不需要的系统服务、默认共享和高危端口。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-16）

1. 测评指标

移动终端应能够发现并阻止用户权限异常改变的情况。（本条款引用自GB/T 22239.3-20XX 8.1.3.5）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否能够发现并阻止用户权限异常改变的情况。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 恶意代码防范
   * + - 1. 测评单元（L4-ECS3-17）
2. 测评指标

移动终端应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库。（本条款引用自GB/T 22239.3-20XX 8.1.3.6）

1. 测评对象

移动终端和安全管理员。

1. 测评实施
2. 应访谈安全管理员，询问移动终端恶意代码防护策略以及定期查杀频率；
3. 应检查移动终端是否安装了查杀恶意代码的防恶意代码产品；
4. 应检查移动终端防恶意代码产品软件版本和恶意代码库版本。
5. 单项判定

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

* + - * 1. 测评单元（L4-ECS3-18）

1. 测评指标

移动终端应支持移动业务应用软件仅运行在安全容器内，防止被恶意代码攻击。（本条款引用自GB/T 22239.3-20XX 8.1.3.6）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否支持移动业务应用软件仅运行在安全容器内，防止被恶意代码攻击。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 资源控制
   * + - 1. 测评单元（L4-ECS3-19）
2. 测评指标

应禁止同一移动终端处理访问不同等级保护对象的运行环境。（本条款引用自GB/T 22239.3-20XX 8.1.3.7）

1. 测评对象

安全管理员。

1. 测评实施

应访谈安全管理员，询问移动终端是否禁止同一终端访问不同的等级保护对象。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-20）

1. 测评指标

应禁止同一移动终端处理访问等级保护对象与非等级保护对象的运行环境。（本条款引用自GB/T 22239.3-20XX 8.1.3.7）

1. 测评对象

移动终端。

1. 测评实施

应检查移动终端是否采用安装双操作系统进行安全隔离。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ECS3-21）

1. 测评指标

应禁止用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权。（本条款引用自GB/T 22239.3-20XX 8.1.3.7）

1. 测评对象

移动终端。

1. 测评实施

应检查对移动终端的用户或进程可访问资源的限定，防止移动终端被提权。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

应用和数据安全

1. 身份鉴别
   * + - 1. 测评单元（L4-ADS3-01）
2. 测评指标

使用口令登录时，应强制用户首次登录时修改初始口令，对用户的鉴别信息进行复杂度检查。（本条款引用自GB/T 22239.3-20XX 8.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施
2. 应检查移动应用软件，查看是否提供身份标识和鉴别功能；
3. 应检查移动应用软件，查看是否采用了措施保证身份标识具有唯一性，是否强制用户首次登录时修改初始口令，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用。
4. 单项判定

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

* + - * 1. 测评单元（L4-ADS3-02）

1. 测评指标

用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。（本条款引用自GB/T 22239.3-20XX 8.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施

应测试移动应用软件，可通过重置鉴别信息，查看是否成功，验证鉴别信息重置是否有

效。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ADS3-03）

1. 测评指标

移动应用软件应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求。（本条款引用自GB/T 22239.3-20XX 8.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施
2. 应测试移动应用软件，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效；
3. 应渗透测试移动应用软件，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。
4. 单项判定

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

* + - * 1. 测评单元（L4-ADS3-04）

1. 测评指标

移动应用软件应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。（本条款引用自GB/T 22239.3-20XX 8.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施
2. 应检查移动应用软件，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数；
3. 应测试移动应用软件，可通过多次输入错误的密码，验证登录失败处理功能是否有效。
4. 单项判定

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

* + - * 1. 测评单元（L4-ADS3-05）

1. 测评指标

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。（本条款引用自GB/T 22239.3-20XX 8.1.4.1）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看是否采用了两种或两种以上组合的身份鉴别技术来进行身份

鉴别。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 软件审核与检测
   * + - 1. 测评单元（L4-ADS3-06）
2. 测评指标

应保证等级保护对象业务移动应用软件开发后、上线前经专业测评机构安全检测。（本条款引用自GB/T 22239.3-20XX 8.1.4.2）

1. 测评对象

移动应用软件和系统建设负责人。

1. 测评实施
2. 应访谈系统建设负责人，询问是否在移动应用软件开发结束后，上线前进行了专业测评机构的安全检测；
3. 应检查移动应用软件，查看是否有专业测评机构安全检测报告。
4. 单项判定

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

1. 数据完整性
   * + - 1. 测评单元（L4-ADS3-07）
2. 测评指标

移动应用软件应采用国产密码技术保证通信过程中数据的完整性。（本条款引用自GB/T 22239.3-20XX 8.1.4.3）

1. 测评对象

移动应用软件和应用管理员。

1. 测评实施
2. 应访谈应用管理员，采用哪种密码技术保证通信过程中数据的完整性；
3. 应检查移动应用软件设计、验收文档或源代码，查看是否有关于能检测数据通信和存储过程中完整性受到破坏的描述；
4. 应测试移动应用软件，可通过获取通信双方的数据包，查看通信报文中是否进行完整性保护。
5. 单项判定

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

* + - * 1. 测评单元（L4-ADS3-08）

1. 测评指标

移动应用软件应采用校验技术或密码技术保证重要数据存储时的完整性，并在检测到完整性错误时采取必要的恢复措施。（本条款引用自GB/T 22239.3-20XX 8.1.4.3）

1. 测评对象

移动应用软件。

1. 测评实施
2. 应检查移动应用软件，查看是否配备检测系统管理数据、鉴别信息和业务数据在存储过程中完整性受到破坏的功能；
3. 应检查移动应用软件采取的恢复措施。
4. 单项判定

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

1. 数据保密性
   * + - 1. 测评单元（L4-ADS3-09）
2. 测评指标

移动应用软件应采用国产密码技术保证重要数据在本地存储时的保密性。（本条款引用自GB/T 22239.3-20XX 8.1.4.4）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看其鉴别信息和主要数据是否采用国产密码技术加密或其他有

效措施实现了存储保密性。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ADS3-10）

1. 测评指标

应确保移动应用软件之间的重要数据不能被互操作。（本条款引用自GB/T 22239.3-20XX 8.1.4.4）

1. 测评对象

移动应用软件。

1. 测评实施

应测试移动应用软件，验证移动应用软件之间的重要数据是否能被互操作。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ADS3-11）

1. 测评指标

应确保移动应用软件数据文件所在的存储空间，被释放或重新分配前可得到完全清除。（本条款引用自GB/T 22239.3-20XX 8.1.4.4）

1. 测评对象

移动应用软件。

1. 测评实施
2. 应检查设计、验收文档或源代码，查看其是否有关于释放或重新分配系统内文件、目录和数据库记录等资源所在存储空间给其他用户前进行完全清除的描述；
3. 应测试移动应用软件，用某用户登录系统并进行操作后，在该用户退出后用另一用户登录，试图操作（读取、修改或删除等）其他用户产生的文件、目录和数据库记录等资源，查看操作是否成功，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）。
4. 单项判定

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

* + - * 1. 测评单元（L4-ADS3-12）

1. 测评指标

移动应用软件应对通信过程中的敏感信息字段或整个报文进行密码加密。（本条款引用自GB/T 22239.3-20XX 8.1.4.4）

1. 测评对象

移动应用软件。

1. 测评实施
2. 应检查移动应用软件，查看其管理数据、鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输保密性；
3. 应测试移动应用软件，可通过用嗅探工具获取通信数据包，查看是否为密文。
4. 单项判定

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

1. 备份和恢复
   * + - 1. 测评单元（L4-ADS3-13）
2. 测评指标

移动应用软件应仅采集和保存业务必需的用户个人信息。（本条款引用自GB/T 22239.3-20XX 8.1.4.5）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件，查看移动应用软件所采集和保存的用户个人信息是否为业务必须

的信息。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ADS3-14）

1. 测评指标

应禁止移动应用软件未授权访问、使用用户个人信息。（本条款引用自GB/T 22239.3-20XX 8.1.4.5）

1. 测评对象

移动应用软件。

1. 测评实施
2. 应测试移动应用软件，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；
3. 应测试移动应用软件，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限；
4. 应渗透测试移动应用软件，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。
5. 单项判定

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

* + - * 1. 测评单元（L4-ADS3-15）

1. 测评指标

移动应用软件应提供移动终端重要数据备份与恢复功能。（本条款引用自GB/T 22239.3-20XX 8.1.4.5）

1. 测评对象

移动应用软件。

1. 测评实施

应检查是否对移动应用软件的重要信息进行了备份，备份方式（如是否为完全数据备份）、

频率和介质存放方式是否达到相关标准的要求，是否定期对备份数据进行恢复测试。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ADS3-16）

1. 测评指标

移动应用软件应将重要数据定时批量传送至备用位置。（本条款引用自GB/T 22239.3-20XX 8.1.4.5）

1. 测评对象

移动应用软件。

1. 测评实施

应检查移动应用软件是否将重要信息定时批量传送至备用位置，以及备份方式（如

是否为完全数据备份）、频率和介质存放方式等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全管理单项测评

安全策略和管理制度

1. 管理制度
   * + - 1. 测评单元（L4-PSS3-01）
2. 测评指标

应建立等级保护对象移动互联安全管理制度，并纳入等级保护对象管理安全制度；（本条款引用自GB/T 22239.3-20XX 8.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括移动互联安全管理规范等相关内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-PSS3-02）

1. 测评指标

应对管理人员或移动终端操作人员执行的日常管理操作建立操作规程；（本条款引用自GB/T 22239.3-20XX 8.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括人员日常管理操作规程。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-PSS3-03）

1. 测评指标

应在等级保护对象管理制度中建立移动终端管理服务端操作使用管理规定。（本条款引用自GB/T 22239.3-20XX 8.2.1.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查安全管理制度，查看是否包括移动终端管理服务端操作使用的相关内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全管理机构和人员

1. 岗位设置
   * + - 1. 测评单元（L4-ORS3-01）
2. 测评指标

应将移动互联管理纳入等级保护对象管理员职责；（本条款引用自GB/T 22239.3-20XX 8.2.2.1）

1. 测评对象

信息安全负责人和管理制度类文档。

1. 测评实施

应访谈信息安全负责人，询问是否设置了移动互联相关管理岗位，岗位职责是否明确。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ORS3-02）

1. 测评指标

应设立移动互联信息安全管理工作的职能部门，并制定各负责人的职责；（本条款引用自GB/T 22239.3-20XX 8.2.2.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查部门和岗位职责文档，查看是否明确了移动互联安全部门、安全岗位的职责。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ORS3-03）

1. 测评指标

应为移动终端管理服务端设置专职管理员、操作员，并纳入职能部门职责。（本条款引用自GB/T 22239.3-20XX 8.2.2.1）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查是否针对移动终端管理服务端设置了专职管理员岗位、操作员岗位，并纳入职能

部门职责。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 人员配备
   * + - 1. 测评单元（L4-ORS3-04）
2. 测评指标

应保证移动终端管理服务端配备专职管理员、操作员和审计员。（本条款引用自GB/T 22239.3-20XX 8.2.2.2）

1. 测评对象

信息安全负责人和记录表单类文档。

1. 测评实施
2. 应访谈信息安全负责人，询问是否设置了移动终端管理端专职管理员、操作员及审计员；
3. 应检查岗位职责文档，查看是否明确了移动终端管理端相关岗位的职责。
4. 单项判定

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

1. 授权和审批
   * + - 1. 测评单元（L4-ORS3-05）
2. 测评指标

应根据各个部门和岗位的职责明确移动互联管理授权审批事项、审批部门和批准人；（本条款引用自GB/T 22239.3-20XX 8.2.2.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查岗位职责文档，查看移动互联网管理授权审批事项、审批部门和审批人是否明确。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ORS3-06）

1. 测评指标

应针对移动互联系统变更、重要操作、物理访问和系统接入等事项执行审批过程；（本条款引用自GB/T 22239.3-20XX 8.2.2.3）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否针对移动应用软件变更、重要操作、物理访问和系统接入等事项执行审批过

程，是否有相关审批记录表单。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ORS3-07）

1. 测评指标

应保证移动终端管理服务端设置专职管理员、操作员权限由审批部门或批准人批准。（本条款引用自GB/T 22239.3-20XX 8.2.2.3）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查岗位职责文档，或会议纪要，查看移动终端管理服务端的专职管理员、操作员权

限的审批过程是否合理，是否由审批部门或审批人批准。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全意识教育和培训
   * + - 1. 测评单元（L4-ORS3-08）
2. 测评指标

应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；（本条款引用自GB/T 22239.3-20XX 8.2.2.4）

1. 测评对象

信息安全负责人。

1. 测评实施

应访谈信息安全负责人，询问是否对各类人员进行移动互联安全教育和岗位技能培训，

告知相关的安全知识、安全责任和惩戒措施等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-ORS3-09）

1. 测评指标

应对移动终端管理服务端设置专职管理员、操作员进行专项安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。（本条款引用自GB/T 22239.3-20XX 8.2.2.4）

1. 测评对象

管理制度类文档。

1. 测评实施

应访谈信息安全负责人，询问是否对移动终端管理服务端的专职管理员、操作员进行移

动互联安全教育和岗位技能培训，告知相关的安全知识、安全责任和惩戒措施等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全建设管理

1. 安全方案设计
   * + - 1. 测评单元（L4-CMS3-01）
2. 测评指标

应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施；（本条款引用自GB/T 22239.3-20XX 8.2.3.1）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否依据风险分析的结果补充和调整过安全措施，具体做过哪些调整。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-02）

1. 测评指标

应根据等级保护对象的安全保护等级进行移动互联安全方案设计，并纳入系统总体方案设计；（本条款引用自GB/T 22239.3-20XX 8.2.3.1）

1. 测评对象

安全规划设计类文档。

1. 测评实施
2. 应检查移动应用系统的安全设计方案，查看方案是否描述系统的安全保护等级，是否描述系统的安全保护策略，是否根据系统的安全级别选择了安全措施；
3. 应检查移动应用软件的安全设计方案，查看是否详细描述安全措施的实现内容，是否有安全产品的功能、性能和部署等描述，是否有安全建设的费用和计划等。
4. 单项判定

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

* + - * 1. 测评单元（L4-CMS3-03）

1. 测评指标

应组织相关部门和安全专家对系统移动互联安全方案设计进行论证和审定，经过批准后才能正式实施。（本条款引用自GB/T 22239.3-20XX 8.2.3.1）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查相关评审记录，查看在系统建设实施前，是否对系统移动互联安全方案进行论证

和审定。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 产品采购和使用
   * + - 1. 测评单元（L4-CMS3-04）
2. 测评指标

应确保移动互联安全产品采购和使用符合国家的有关规定；（本条款引用自GB/T 22239.3-20XX 8.2.3.2）

1. 测评对象

系统建设负责人。

1. 测评实施
2. 应访谈系统建设负责人，询问移动应用软件使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等；
3. 应检查移动应用软件所使用的安全产品的相关证书。
4. 单项判定

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

* + - * 1. 测评单元（L4-CMS3-05）

1. 测评指标

相关密码产品使用应符合国家密码管理相关规定。（本条款引用自GB/T 22239.3-20XX 8.2.3.2）

1. 测评对象

密码产品。

1. 测评实施

应检查移动应用系统所使用的密码产品的相关证书。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 移动应用软件开发
   * + - 1. 测评单元（L4-CMS3-06）
2. 测评指标

应要求对移动业务应用软件开发者进行资格审查；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否对开发者进行资格审查。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-07）

1. 测评指标

应确保开发移动业务应用软件的签名证书合法性；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

软件的签名证书。

1. 测评实施

应检查开发移动业务应用软件的签名证书是否具有合法性。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-08）

1. 测评指标

应要求移动应用软件开发完提供软件设计文档、使用指南及软件源代码；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

软件开发类文档。

1. 测评实施

应检查是否具备软件设计文档，使用指南及软件源代码。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-09）

1. 测评指标

应要求应用软件开发使用的工具来源可靠；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应方访谈系统建设负责人，检查应用软件开发使用的工具来源。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-10）

1. 测评指标

自行开发移动应用软件，应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，检查开发环境与实际运行环境物理是否分开，测试数据和测试结果是否受到控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-11）

1. 测评指标

自行开发移动应用软件，应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查是否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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-12）

1. 测评指标

自行开发移动应用软件，应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查是否包含移动应用软件设计的相关文档并对文档使用进行控制。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-13）

1. 测评指标

自行开发移动应用软件，应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；（本条款引用自GB/T 22239.3-20XX 8.2.3.3）

1. 测评对象

管理制度类文档和记录表单类文档。

1. 测评实施

应检查是否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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 工程实施
   * + - 1. 测评单元（L4-CMS3-14）
2. 测评指标

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。（本条款引用自GB/T 22239.3-20XX 8.2.3.4）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问是否指定专门部门或人员对移动互联工程实施过程进行进度和质量控制，具体由何部门/何人负责。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 测试验收
   * + - 1. 测评单元（L4-CMS3-15）
2. 测评指标

应对系统的移动互联部分进行安全性测试验收。（本条款引用自GB/T 22239.3-20XX 8.2.3.5）

1. 测评对象

系统建设负责人。

1. 测评实施
2. 应访谈系统建设负责人，询问在移动应用软件建设完成后是否对其进行安全性测试验收；
3. 应检查是否具有移动互联工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；
4. 应检查是否具有移动应用软件测试验收报告。
5. 单项判定

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

1. 系统交付
   * + - 1. 测评单元（L4-CMS3-16）
2. 测评指标

应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；（本条款引用自GB/T 22239.3-20XX 8.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否具有移动应用系统交付清单，查看交付清单是否说明系统交付的各类设备、

软件、文档等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-17）

1. 测评指标

应对负责系统移动互联运行维护的技术人员进行相应的技能培训；（本条款引用自GB/T 22239.3-20XX 8.2.3.6）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问移动应用软件正式运行前是否对运行维护人员进行过培训，

针对哪些方面进行过培训。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-18）

1. 测评指标

应确保提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档；（本条款引用自GB/T 22239.3-20XX 8.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-19）

1. 测评指标

应确保提供移动终端管理服务端建设过程中的文档和指导用户进行系统运行维护的文档。（本条款引用自GB/T 22239.3-20XX 8.2.3.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否提供移动终端管理服务端建设过程中的文档和指导用户进行系统运行维护

的文档。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全服务商选择
   * + - 1. 测评单元（L4-CMS3-20）
2. 测评指标

应确保移动互联安全服务商的选择符合国家的有关规定；（本条款引用自GB/T 22239.3-20XX 8.2.3.7）

1. 测评对象

系统建设负责人。

1. 测评实施

应访谈系统建设负责人，询问系统选择的安全服务商有哪些，是否符合国家有关规定。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-21）

1. 测评指标

应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任；（本条款引用自GB/T 22239.3-20XX 8.2.3.7）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查是否具有与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是

否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-22）

1. 测评指标

应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；（本条款引用自GB/T 22239.3-20XX 8.2.3.7）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查与服务商签订的相关协议等文档，查看其内容是否协议的有效期限和责任人的签

字等整个服务供应链各方需履行的信息安全相关义务。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-CMS3-23）

1. 测评指标

应选择安全可靠应用软件分发运营商。（本条款引用自GB/T 22239.3-20XX 8.2.3.7）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人。检查应用软件分发运营商的相关资质与相关证书。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

安全运维管理

1. 资产管理
   * + - 1. 测评单元（L4-MMS3-01）
2. 测评指标

应编制并保存与等级保护对象相关的移动终端资产清单，包括资产责任部门、重要程度和使用人等内容；（本条款引用自GB/T 22239.3-20XX 8.2.4.1）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查资产清单，查看是否针对责任部门、重要程度和使用人等内容编制资产清单。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-02）

1. 测评指标

应根据资产的重要程度对移动终端进行标识管理，根据其价值选择相应的管理措施。（本条款引用自GB/T 22239.3-20XX 8.2.4.1）

1. 测评对象

资产清单、管理制度类文档、记录表单类文档。

1. 测评实施

应检查资产清单及资产管理文档，查看是否根据资产的重要程度对移动终端进行标识管

理，根据其价值选择相应的管理措施。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合或部分符合本单元测评指标要求。

1. 设备维护管理
   * + - 1. 测评单元（L4-MMS3-03）
2. 测评指标

应对各种移动互联设备（包括无线接入设备及移动终端）维护纳入等级保护对象进行管理；（本条款引用自GB/T 22239.3-20XX 8.2.4.2）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查设备管理制度，查看是否将各种移动互联设备（包括无线接入设备）维护纳入管理制度内并进行管理。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-04）

1. 测评指标

应确保移动终端在报废或重用前应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；（本条款引用自GB/T 22239.3-20XX 8.2.4.2）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查设备维护管理文档，查看设备使用管理流程，确认设备在报废、重用前采取必要

的技术措施，确保设备上的敏感信息被彻底消除。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-05）

1. 测评指标

应在移动终端设备丢失后进行远程数据擦除。（本条款引用自GB/T 22239.3-20XX 8.2.4.2）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查管理制度类文档，移动终端设备丢失后应进行远程数据擦除，确保数据不会外泄。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 风险评估和漏洞管理
   * + - 1. 测评单元（L4-MMS3-06）
2. 测评指标

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。（本条款引用自GB/T 22239.3-20XX 8.2.4.3）

1. 测评对象

安全管理员和记录表单类文档。

1. 测评实施
2. 应访谈安全管理员，询问采取哪些措施识别移动互联安全漏洞和隐患，并在评估后对发现的安全漏洞和隐患进行修补；
3. 应检查移动互联安全漏洞管理记录。
4. 单项判定

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

1. 应用软件来源管理
   * + - 1. 测评单元（L4-MMS3-07）
2. 测评指标

应保证移动终端安装、运行的应用软件来自等级保护对象管理者指定证书签名或指定分发渠道；（本条款引用自GB/T 22239.3-20XX 8.2.4.4）

1. 测评对象

安全管理员。

1. 测评实施

应访谈安全管理员，移动终端安装、运行的应用软件是否来自信息系统管理者指定证书

签名或可靠分发渠道。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-08）

1. 测评指标

应保证移动终端安装、运行的移动应用软件由等级保护对象管理者指定的开发者开发。（本条款引用自GB/T 22239.3-20XX 8.2.4.4）

1. 测评对象

安全管理员。

1. 测评实施

应检查移动终端安装、运行的移动应用软件是否由经审核的开发者开发。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 恶意代码防范管理
   * + - 1. 测评单元（L4-MMS3-09）
2. 测评指标

应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；（本条款引用自GB/T 22239.3-20XX 8.2.4.5）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问是否对员工进行移动互联基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查等。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-010）

1. 测评指标

应对截获的恶意代码进行及时分析处理。（本条款引用自GB/T 22239.3-20XX 8.2.4.5）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问移动终端采用何种机制对移动应用软件的使用进行管理。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-011）

1. 测评指标

应保证移动终端管理服务端将移动应用软件运行策略推送给移动终端。（本条款引用自GB/T 22239.3-20XX 8.2.4.5）

1. 测评对象

移动终端管理系统。

1. 测评实施

应查看移动终端管理服务端是否能够将移动应用软件运行策略推送给移动终端。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 配置管理
   * + - 1. 测评单元（L4-MMS3-012）
2. 测评指标

移动终端管理服务端应记录和保存移动终端基本配置信息，包括操作系统、软件组件版本、移动终端各种设备或软件组件的配置参数等；（本条款引用自GB/T 22239.3-20XX 8.2.4.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查配置管理文档，查看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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-013）

1. 测评指标

移动终端管理服务端应将移动终端基本配置信息改变纳入系统变更范畴，实施对配置信息改变控制，并及时更新基本配置信息库；（本条款引用自GB/T 22239.3-20XX 8.2.4.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查配置管理文档，查看移动终端基本配置信息改变是否被纳入系统变更范畴，是否

实施对配置信息改变控制，并及时更新基本配置信息库。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-014）

1. 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。（本条款引用自GB/T 22239.3-20XX 8.2.4.6）

1. 测评对象

记录表单类文档。

1. 测评实施

应检查配置管理文档，查看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。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 监控和审计管理
   * + - 1. 测评单元（L4-MMS3-015）
2. 测评指标

应确保移动终端管理服务端对移动终端状态、资源使用、软件运行等进行监控和审计；（本条款引用自GB/T 22239.3-20XX 8.2.4.7）

1. 测评对象

系统运维负责人。

1. 测评实施
2. 应访谈系统运维负责人，询问移动应用系统采用何种管理机制；
3. 应查看移动终端管理服务端的管理功能，是否能够对移动终端状态、资源使用、软件运行等进行监控和审计。
4. 单项判定

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

* + - * 1. 测评单元（L4-MMS3-016）

1. 测评指标

应对上线后的业务移动应用软件进行监测。（本条款引用自GB/T 22239.3-20XX 8.2.4.7）

1. 测评对象

移动终端管理系统。

1. 测评实施

应查看移动终端管理服务端的管理功能，是否能够对业务移动应用软件进行监测。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 备份与恢复管理
   * + - 1. 测评单元（L4-MMS3-017）
2. 测评指标

应识别需要定期备份的移动终端中的重要业务信息、系统数据及软件系统等；（本条款引用自GB/T 22239.3-20XX 8.2.4.8）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问是否识别出需要定期备份移动应用软件中的业务信息、系统数据和软件系统，主要有哪些。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-018）

1. 测评指标

应规定备份信息的备份方式、备份频度、存储介质、保存期等；（本条款引用自GB/T 22239.3-20XX 8.2.4.8）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查备份管理文档，查看其是否明确了备份方式、备份频度、存储介质和保存期等方

面内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-019）

1. 测评指标

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。（本条款引用自GB/T 22239.3-20XX 8.2.4.8）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查备份管理文档，查看其是否明确了业务数据的重要程度，是否制定了备份、恢复

策略，是否明确了备份恢复措施。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

1. 安全事件处置
   * + - 1. 测评单元（L4-MMS3-020）
2. 测评指标

应报告所发现的移动互联安全弱点和可疑事件；（本条款引用自GB/T 22239.3-20XX 8.2.4.9）

1. 测评对象

系统运维负责人。

1. 测评实施

应访谈系统运维负责人，询问是否有报告所发现的移动互联安全弱点和可疑事件的相关流程与文件。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-021）

1. 测评指标

应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责；（本条款引用自GB/T 22239.3-20XX 8.2.4.9）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查移动互联安全事件的报告和处置流程，查看其是否明确了安全事件的现场处理、

事件报告和后期恢复的管理职责等方面内容。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

* + - * 1. 测评单元（L4-MMS3-022）

1. 测评指标

应针对移动互联系统发生的安全事件制定应急处置预案。（本条款引用自GB/T 22239.3-20XX 8.2.4.9）

1. 测评对象

管理制度类文档。

1. 测评实施

应检查应急预案，查看是否建立了针对移动互联系统安全事件的专项应急处置预案。

1. 单项判定

如果为肯定，则等级保护对象符合本单元测评指标要求，否则，等级保护对象不符合本单元测评指标要求。

第五级测评要求

（略）。

（资料性附录）  
测评力度

* 1. 概述
  + 本标准在第5章到第8章描述了第一级到第四级等级保护对象的单项测评的具体测评实施过程要求。为了便于理解、对比不同测评方法的测评力度以及不同级别等级保护对象单项测评的测评力度增强情况，分别编制表A.1测评方法的测评力度描述和表A.2不同安全保护等级的等级保护对象的测评力度要求表。
  1. 测评力度描述

测评方法是测评人员依据测评内容选取的、实施特定测评操作的具体方法。本标准涉及访谈、检查和测试等三种基本测评方法。访谈、检查和测试等三种基本测评方法的测评力度可以通过其测评的深度和广度来描述，如表A.1。

表A.1 测评方法的测评力度

|  |  |  |
| --- | --- | --- |
| **测评方法** | **深度** | **广度** |
| 访谈 | 访谈的深度体现在访谈过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要访谈只包含通用和高级的问题；充分访谈包含通用和高级的问题以及一些较为详细的问题；较全面访谈包含通用和高级的问题以及一些有难度和探索性的问题；全面访谈包含通用和高级的问题以及较多有难度和探索性的问题。 | 访谈的广度体现在访谈人员的构成和数量上。访谈覆盖不同类型的人员和同一类人的数量多少，体现出访谈的广度不同。 |
| 检查 | 检查的深度体现在检查过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要检查主要是对功能级上的文档、机制和活动，使用简要的评审、观察或检查以及检查列表和其他相似手段的简短测评；充分检查有详细的分析、观察和研究，除了功能级上的文档、机制和活动外，还适当需要一些总体/概要设计信息；较全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和一些详细设计以及实现上的相关信息；全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和详细设计以及实现上的相关信息。 | 检查的广度体现在检查对象的种类（文档、机制等）和数量上。检查覆盖不同类型的对象和同一类对象的数量多少，体现出对象的广度不同。 |
| 测试 | 测试的深度体现在执行的测试类型上：功能/性能测试和渗透测试。功能/性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入等级保护对象。 | 测试的广度体现在被测试的机制种类和数量上。测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出对象的广度不同。 |

## A.3 等级测评力度

测评力度是在测评过程中实施测评工作的力度，反映测评的广度和深度，体现为测评工作的实际投入程度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多；测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的投入。投入越多，测评力度就越强，测评就越有保证。测评的广度和深度落实到访谈、检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、检查和测试的投入程度的不同。

网络安全等级保护要求不同安全保护等级的等级保护对象应具有不同的安全保护能力，满足相应等级的保护要求。为了检验不同安全保护等级的等级保护对象是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。第一级到第四级等级保护对象的测评力度反映在访谈、检查和测试等三种基本测评方法的测评广度和深度上，落实在不同单单项测评中具体的测评实施上。

为了进一步理解不同等级等级保护对象在测评力度上的不同，表A.2在表A.1的基础上，从测评对象数量和种类以及测评深度等方面详细分析了不同测评方法的测评力度在不同等级保护对象安全测评中的具体体现。

表A.2 不同等级保护对象的测评力度要求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测评力度 | | 等级保护对象安全保护等级 | | | |
| 第一级 | 第二级 | 第三级 | 第四级 |
| 访谈 | 广度 | 测评对象在种类和数量上抽样，种类和数量都较少 | 测评对象在种类和数量上抽样，种类和数量都较多 | 测评对象在数量上抽样，在种类上基本覆盖 | 测评对象在数量上抽样，在种类上全部覆盖 |
| 深度 | 简要 | 充分 | 较全面 | 全面 |
| 检查 | 广度 | 测评对象在种类和数量上抽样，种类和数量都较少 | 测评对象在种类和数量上抽样，种类和数量都较多 | 测评对象在数量上抽样，在种类上基本覆盖 | 测评对象在数量上抽样，在种类上全部覆盖 |
| 深度 | 简要 | 充分 | 较全面 | 全面 |
| 测试 | 广度 | 测评对象在种类和数量、范围上抽样，种类和数量都较少，范围小 | 测评对象在种类和数量、范围上抽样，种类和数量都较多，范围大 | 测评对象在数量和范围上抽样，在种类上基本覆盖 | 测评对象在数量、范围上抽样，在种类上基本覆盖 |
| 深度 | 功能测试/性能测试 | 功能测试/性能测试 | 功能测试/性能测试，渗透测试 | 功能测试/性能测试，渗透测试 |

从表A.2可以看到，对不同等级的等级保护对象进行等级测评时，选择的测评对象的种类和数量是不同的，随着等级保护对象安全保护等级的增高，抽查的测评对象的种类和数量也随之增加。

对不同安全保护等级等级保护对象进行等级测评时，实际抽查测评对象的种类和数量，应当达到表A.2的要求，以满足相应等级的测评力度要求。在具体测评对象选择工作过程中，可参照遵循以下原则：

1. 完整性原则，选择的设备、措施等应能满足相应等级的测评力度要求；
2. 重要性原则，应抽查重要的服务器、数据库和网络设备等；
3. 安全性原则，应抽查对外暴露的网络边界；
4. 共享性原则，应抽查共享设备和数据交换平台/设备；
   * 代表性原则，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统的类型。

（资料性附录）  
测评单元编号说明

* 1. 测评指标编码规则

测评单元编号为三组数据，格式为XX-XXXX-XX，各组含义和编码规则如下：

第1组由两位组成，第1位为字母L，第2位为数字，其中数字1为第一级，2为第二级，3为第三级，4为第四级，5为第五级。

第2组由4位组成，前3位为字母，第4位为数字。字母代表层面：PES为物理和环境安全， NCS为网络和通信安全，ECS为设备和计算安全，ADS为应用和数据安全，PSS为安全策略和管理制度，ORS为安全管理机构和人员，CMS为安全建设管理，MMS为安全运维管理。数字代表标准分册：1为第一分册，2为第二分册，3为第三分册，4为第四分册，5为第五分册，6为第六分册。

第3组由2位数字组成，按层面对基本要求中的要求项进行顺序编号。

示例：测评单元编号为L1-PES1-01，代表源自基本要求第一分册的第一级物理安全层面的第一个指标。

* 1. 专用缩略语

物理和环境安全为PES（Physical and Environmental Security ）

网络和通信安全NCS（Network and Communication Security）

设备和计算安全ECS（Equipment and Computing Security）

应用和数据安全ADS（Application and Data Security）

安全策略和管理制度PSS（Policy and System Security）

安全管理机构和人员ORS（Organization and Resource Security）

安全建设管理CMS（Construction Management Security）

安全运维管理MMS（Maintenance Management Security）

参考文献

[1] GB/T 20269-2006 信息安全技术 信息系统安全管理要求

[2] GB/T 20270-2006 信息安全技术 网络基础安全技术要求

[3] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

[4] GB/T 20272-2006 信息安全技术 操作系统安全技术要求

[5] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求

[6] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求

[7] GB/T 18336-2015 信息安全技术 信息技术安全性评估准则

[8] Information technology-Security techniques - Information security management systems requirements（ISO/IEC 27001：2013）

[9] Information technology-Security techniques - Code of practice forinformation security management（ISO/IEC 17799：2005）

参 考 文 献

[1] GB/T 20269-2006 信息安全技术 信息系统安全管理要求

[2] GB/T 20270-2006 信息安全技术 网络基础安全技术要求

[3] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

[4] GB/T 20272-2006 信息安全技术 操作系统安全技术要求

[5] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求

[6] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求

[7] GB/T 18336-2015 信息安全技术 信息技术安全性评估准则

[8] Information technology-Security techniques - Information security management systems requirements（ISO/IEC 27001：2013）

* + [9] Information technology-Security techniques - Code of practice forinformation security management（ISO/IEC 17799：2005）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_