**报告编号：2019-XAPG–ZYXX-08**

互联网新技术新业务信息安全评估报告

|  |  |
| --- | --- |
| **委托单位位：** | 中移信息技术有限公司 |
| **业务名称称：** | 移动商城 |

**评估单位：国家计算机网络与信息安全管理中心**

**2019年1月**

目录

[1 业务基本情况介绍 3](#_Toc525288127)

[1.1 业务名称 3](#_Toc525288128)

[1.2 业务功能介绍 3](#_Toc525288129)

[1.3技术实现方式介绍 6](#_Toc525288130)

[1.4用户规模 6](#_Toc525288131)

[1.5 市场发展情况 6](#_Toc525288132)

[2 安全评估情况 6](#_Toc525288133)

[2.1 安全评估情况概述 7](#_Toc525288134)

[2.2 评估人员组成](#_Toc525288135) **[错误!未定义书签。](#_Toc525288135)**

[2.3 评估实施流程](#_Toc525288136) **[错误!未定义书签。](#_Toc525288136)**

[3 业务安全风险分析 7](#_Toc525288137)

[3.1 安全风险分析表 11](#_Toc525288138)

[3.2 风险说明 17](#_Toc525288139)

[4 配套安全管理措施 18](#_Toc525288140)

[4.1 日常安全管理介绍 18](#_Toc525288141)

[4.2 应急管理措施介绍 18](#_Toc525288142)

[4.3 安全保障能力分析表 19](#_Toc525288143)

[4.4 安全保障能力说明 31](#_Toc525288144)

[5 评估结果及整改建议 31](#_Toc525288145)

[5.1 信息安全管理风险评估结果 31](#_Toc525288146)

[5.2 信息内容安全风险评估结果 32](#_Toc525288147)

[5.3 业务平台安全风险评估结果 33](#_Toc525288148)

[5.4 业务运行安全风险评估结果 34](#_Toc525288149)

[6 安全评估结论意见 36](#_Toc525288150)

# 1 业务基本情况介绍

移动商城经过2014年和2015年两年的快速发展，已经成为中国移动面向全国用户的综合电子商务平台。实现商户产品自主上架，实现购机送费、增值业务订购等20余套业务模板，实现所有商品均由省公司根据自身业务发展需要自主上架，总部提供后台支持，业务承载效率得到极大提升。实现了终端、配件、套餐和增值业务等产品的销售需求，为商户提供商品上下架管理、订单管理、库存管理等后台管理功能，为客户提供商品搜索、展示、支付等前台销售功能；建设能力开放平台、支付网关、物流网关等公共基础设施。有效打通两级之间的业务流、信息流和资金流，先后编制了业务和产品、客户体验和服务管理、业务需求和服务保障、资金和结算等10余项管理办法，并顺利实现了两级系统平台对接。

## 1.1 业务名称

移动商城服务

## 1.2 业务功能介绍

本次评估涉及移动商城的销售子系统和服务子系统。

销售子系统由八大功能组成部分：

1、商品中心

商品中心提供对移动商城商品的统一管理，商品发布、上下架审核、商品配置、等商品管理功能，并提供对外的数据支持能力。

2、订单中心

移动商城处理订单的所有功能模块集合。提供对终端（裸机、合约机）、配件等实体商品销售订单的、多渠道的统一管理、订单查询、订单导出、订单流程流转、退货、退款操作及审核等功能，并通过能力开放平台支持对外能力输出。

3、营销中心

营销中心基于移动商城的基础平台，将移动商城商品通过营销工具(秒杀、团购等)，实现商场营销运营能力的提高。通过各类营销工具的使用，吸引网购群体的注意力并产生购买兴趣；同时使得各商户利用营销工具可以快速建立营销活动，提高店铺运营效率。

4、商户中心

移动商城商户管理、用户管理、角色管理、权限管理等功能模块的集合。

实现移动商城对商户的基本信息和状态进行维护和管理、运营后台使用人员的账号、角色、权限等的管理，以及商城帮助中心内容的自助发布等。

5、能力开放平台

能力开放平台建立在移动商城之上，将移动商城自有特色数据资源（如的用户、商品、订单、营销等）封装成一系列数据接口开放出去，时允许外部系统接口插件注册进来，对业务流程进行扩展。

6、支付网关

支付网关是移动商城与外部支付机构之间的接口平台。针对产品销售平台以及自助服务平台发起的支付服务请求（支付、充值缴费等），进行接口协议封装，分发给不同的支付机构进行支付服务，并反馈支付交易结果。

7、运营监控平台

运营监控平台可对系统进行全面的监控，获取系统运行状态、业务运营数据及订单交易数据，全面准确掌握商城整体运行状况，及时发现并解决系统运行和业务运营过程中存在的问题。。

8、物流网关

移动商城物流网关与商户使用的物流商系统对接，实现商户订单配送信息实时同步展示给用户、商户运营人员，并可使商户进行配送状态跟踪。

服务子系统主要功能涉及移动商城个人中心话费充值及业务查询（例如：详单查询、账单查询、业务查询及退订）

## 1.3技术实现方式介绍

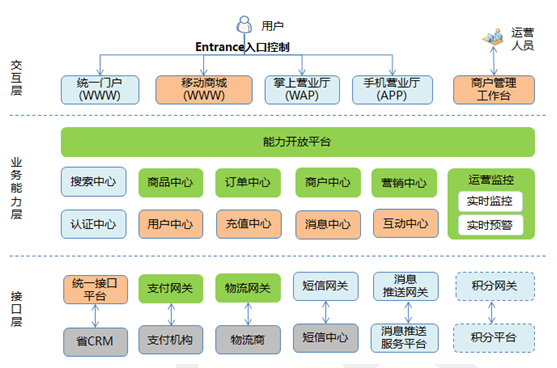


图1 技术实现方式

## 1.4用户规模

2013年7月，移动商城工程启动。2014年6月26日全面完成31省公司和终端公司入驻并对外开放，移动商城一期建设工作基本完成。移动商城服务主要面向中国移动31家省公司及中国移动在网用户。

## 1.5 市场发展情况

中国移动面向用户的统一电商门户在电商的发展浪潮中，从初期的规划建立到目前的规模化运营，历经5年时间。随着移动互联网、物联网广泛的深入到社会生活的各个角落，线上线下组合的电子商务模式层出不穷，为今天的移动电商发展提供了更加广阔的舞台和机遇。截止到目前，移动商城上线功能已基本覆盖了各类自有业务，包括买手机、办套餐、办业务、选号码、挑配件、业务查询、充值缴费、宽带预约等，2017年8月至2018年7月期间，移动商城终端月均销量6234台，号码月均销量3.5万单，套餐月均办理量36.11万笔，增值业务月均办理量164.03万笔，自有业务销量远高于同行业及中国移动外部渠道销量。

# 2 安全评估情况

## 2.1 安全评估情况概述

**1.总体情况**

2018年1月16日至1月18日，国家计算机网络与信息安全管理中心对中移信息技术有限公司（以下简称“中移信息”）的电子渠道交流平台、俱乐部等12个业务开展了新技术新业务信息安全现场评估工作。

评估主要内容包括管理体系评估、业务风险评估和信息安全保障能力评估三个部分。评估方法包括人员访谈、制度文档核实、业务功能验证、内容安全测试、数据安全检测、漏洞扫描、渗透测试等。

本报告主要给出“移动商城”业务的信息安全评估情况。

**2.评估目的**

为进一步提升中移信息技术有限公司新技术新业务的信息安全防护和处置能力，依据新技术新业务信息安全评估相关政策文件，结合通信安全分级保护、风险评估的基本方法和标准，发现并找出新技术新业务相关的管理制度、业务流程、网络系统、服务器以及应用系统等方面存在的安全漏洞和隐患。目的是为企业健全互联网新技术新业务管理制度、完善业务流程、提早启动保障措施、加固系统和网络漏洞提供参考和依据，进而提高业务系统的安全防护水平，为业务的发展创造安全可靠的环境。

**3.评估内容**

新技术新业务安全评估工作主要涉及管理、业务和信息安全保障等方面的安全因素。管理方面，主要采用访谈调研、相关文件查阅的方式，查找管理方面存在的漏洞；业务方面，主要采用人员访谈、功能演示、业务试用、流程梳理等方式，查找业务方面存在的漏洞或隐患；信息安全保障能力方面，主要通过内容测试、漏洞扫描、渗透测试等手段，查验现有信息安全技术保障措施是否满足基本要求。各方面的评估重点如下：

（1）管理体系方面：重点评估新技术新业务的信息安全管理体系和业务安全管理措施是否满足电信管理机构的安全管理要求，具体包括机构设置、管理制度、信息安全相关要求和技术标准以及具体执行情况。

（2）业务风险方面：评估新技术新业务的完整业务流程，结合业务功能属性及技术实现，包括内容发布审核、业务边界安全、权限管理、用户信息保护等，评估系统潜在的信息安全风险。

（3）信息安全保障能力方面：评估现有的安全管理措施、技术手段等信息安全保障能力是否能够有效控制业务信息安全风险。开展内容过滤机制测试；对业务系统、操作系统、网络设备进行安全检测；通过渗透测试查看系统安全防护情况等；

（4）其他：评估新技术新业务相关系统的安全性。

**4.评估依据**

**（1）政策法规依据**

《网络安全法》

《基础电信企业信息安全责任管理办法（试行）》

《互联网新技术新业务信息安全评估管理办法（试行）》

《关于开展基础电信企业网络与信息安全责任考核有关工作指导》

《互联网用户账号名称管理规定》

**（2）安全标准**

《互联网新技术新业务安全评估指南》

《电信网和互联网安全防护管理指南》

《电信网和互联网安全风险评估实施指南》

《电信网和互联网灾难备份及恢复实施指南》

《电信网和互联网物理环境安全等级保护要求》

《电信网和互联网物理环境安全等级保护检测要求》

《电信网和互联网管理安全等级保护要求》

《电信网和互联网管理安全等级保护检测要求》

《2019年省级基础电信企业网络与信息安全工作考核要点与评分标准》

**5.评估方式**

本次信息安全评估的主要方式包括人员访谈、文档材料核查、业务功能验证、内容安全测试和安全测评等。

人员访谈主要是通过对网络与信息安全管理人员、特定业务管理人员、技术维护人员进行访谈获取企业信息安全管理、业务应用及平台安全、安全保障措施等方面的现状。

文档材料核查主要是指对企业信息安全、业务安全等相关制度的制定情况进行核实。

业务功能验证通过检查业务功能和流程，对业务应用和系统平台潜在的安全风险做出研判。

内容安全测试主要用于评估企业内容安全相关的保障能力，包括违法及不良信息样本的识别检测、传播扩散控制等方面。

安全测评主要针对业务平台安全和数据安全，涉及漏洞分析、渗透测试等技术手段。

## 2.2 评估人员组成

|  |  |  |
| --- | --- | --- |
| **姓名** | **职称/职务** | **职责** |
| 段东圣 | 高级工程师 | 评估组长 |
| 姜淦卿 | 工程师 | 评估测试 |
| 刘威 | 工程师 | 评估测试 |
| 裴卓雄 | 工程师 | 评估测试 |
| 孙捷 | 工程师 | 评估测试 |
| 王鑫 | 工程师 | 渗透测试 |

## 2.3 评估实施流程

评估实施流程包括评估准备、现场评估、评估总结三个阶段：

（1）评估准备

成立评估小组，确定小组成员，收集业务相关的管理文档、技术文档、业务市场发展情况、业务自身情况、企业现有的安全管理和保障措施等信息，充分了解业务的使用流程。并根据业务网络访问情况开展前期初步测试和预评估。根据业务情况与被评估方进行深入交流，明确评估重点。

（2）现场评估

现场评估包括管理制度核查、业务安全测试、内容安全测试、系统漏洞检测、设备安全检测五个方面内容。采用人员访谈、内容安全测试、网络安全扫描和渗透测试等方式对企业信息安全管理、业务和技术风险、保障能力进行综合评估。

（3）评估总结

评估总结阶段对评估结果进行综合分析，形成评估结论，撰写评估报告，并提出合理化的整改建议。

# 3 业务安全风险分析

## 3.1 安全风险分析表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **风险类型** | **FX编号** | **业务安全风险评估要点** | **评估**  **意见** | **评估**  **记录** |
| 业务应用安全风险 | 01-FX-01 | 评估人员通过人员访谈的方式，了解被评估业务的用户规模、用户类型、用户之间的相关性（即用户之间是否存在交互关系）。 | 涉及 | 商城服务用户规模超过1000万，用户涵盖移动在网用户，用户之间无相关性 |
| 01-FX-02 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务是否能够确保用户身份信息真实性，如用户注册过程中是否要求提供真实身份信息等。 | 涉及 | 登录移动集团手厅或网厅触屏版的中国移动手机用户可直接进行访问，即用户为手厅或网厅的注册用户，无需再次注册。 |
| 01-FX-03 | 评估人员通过测试验证的方式，检查被评估业务是否具备用户真实身份鉴别功能，是否存在身份仿冒或欺骗的可能。 | 涉及 | 在评估业务中办理业务时，通过对比登录和办理的号码是否一致，同时在办理过程有短信验证码 |
| 01-FX-04 | 评估人员通过人员访谈的方式，检查是否制定了会话失效机制、身份认证失效机制。 | 涉及 | 有身份认证失效机制和会话失效机制。 |
| 01-FX-05 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务的中公共信息的可审核性，承载的信息格式是否包括简单文本，以及文本、图片、语音、视频等审核难度较高的信息格式或文件 | 涉及 | 通过中国移动商城服务子系统工作台，销售子系统工作台移动管理人员可通过账号发布营销信息 |
| 01-FX-06 | 评估人员通过人员访谈、文件审查等方式，了解业务发布的公共信息是否具有多样性属性（即是否包含多类主题信息）。 | 涉及 | 服务子系统主要为资费、优惠券、消息通知等营销推广类信息；销售子系统主要为商品类信息 |
| 01-FX-07 | 评估人员通过人员访谈、文件审查、测试验证等方式，了解业务公共信息内容的相关性（即信息内容是否围绕相近的主题）。 | 涉及 | 无相关性 |
| 01-FX-08 | 评估人员通过人员访谈、演示查验等方式，了解业务语言类型是否包含小语种信息。 | 涉及 | 不包含小语种 |
| 01-FX-09 | 评估人员通过人员访谈、演示查验等方式，了解业务中公共信息产生方式，即确认是否包含第三方或用户发布的信息。 | 涉及 | 按照活动支撑流程发布信息，不包含第三方及用户发布信息 |
| 01-FX-10 | 评估人员通过人员访谈、演示查验等方式，了解业务平台支持的信息传播方式，是否支持点对点、点对多点、多点对多点及裂变式传播。 | 涉及 | 信息传播方式是点对多点 |
| 01-FX-11 | 评估人员通过人员访谈、演示查验等方式，了解业务支持的通信媒介，即业务平台的信息是否可以分享至其他平台，或可跨越网络类型传播。 | 不涉及 | 业务平台信息不可分享至其他平台 |
| 01-FX-12 | 评估人员通过人员访谈、演示查验等方式，了解业务平台信息传递实时性属性，即在向用户推送新消息时是否是直接明示信息内容，是否允许用户修改系统设置实现信息的隐藏。 | 涉及 | 向用户直接明示信息内容 |
| 01-FX-13 | 评估人员通过人员访谈、演示查验等方式，了解业务中信息收取方式，即用户获取信息包含的类型有如下几种：用户主动订阅或申请，系统主动推送等。 | 涉及 | 用户能够主动订阅或申请，同时系统能够主动推送消息。 |
| 业务平台安全风险 | 02-FX-01 | 评估人员通过人员访谈、文件审查等方式，了解业务系统网络拓扑结构中设备位置分布情况。 | 涉及 | 中国移动国际信息港 |
| 02-FX-02 | 评估人员通过人员访谈、文件审查等方式，了解业务平台系统资源调度方式，是否采用云计算技术或云服务方式。 | 涉及 | 移动自有云服务 |
| 02-FX-03 | 评估人员通过人员访谈、文件审查等方式，了解业务平台系统资源调度方式，是否采取了内容分发网络（CDN）技术情况。 | 不涉及 |  |
| 02-FX-04 | 评估人员通过人员访谈、文件审查等方式，了解业务合作模式/服务模式是否满足合规性要求，即核实业务合作模式/服务模式是否满足相关行业管理规定，或合作/用户是否具备开办业务的相关资质。 | 涉及 | 合作模式/服务模式满足相关行业管理规定 |
| 02-FX-05 | 评估人员通过人员访谈、文件审查等方式，了解业务运营在合作（技术合作和服务合作）开展前是否对合作信息安全保障能力（管理制度和技术手段）进行了评估，并形成了相关文档。 | 涉及 | 服务子系统与北京思特奇技术有限公司开展合作，销售子系统与卓望数码技术(深圳)有限公司开展合作，暂未对合作方的信息安全保障能力形成文档性文件。 |
| 02-FX-06 | 评估人员通过人员访谈、文件审查等方式，了解业务系统是否开放API接口。 | 不涉及 | 对外没有提供API，只有调用集团掌厅或手厅的API接口 |
| Web应用安全风险 | 03-FX-01 | 评估人员通过人员访谈的方式，检查该业务应用是否存在多级账号，导致越权的风险及特权账号滥用等问题。 | 涉及 | 商城服务子系统平台存在多级权限，由电渠运营统一用户管理进行开户申请，并分配相应的权限 |
| 03-FX-02 | 评估人员通过人员访谈的方式，查看是否制定有日志记录规范且承诺能够在运营过程中按系统威胁日志留存管理规范进行日志记录与管理工作。 | 涉及 | 商城服务子系统制定有日志管理制度，销售子系统日志记录不规范，未对用户搜索违法信息的行为进行日志留存。 |
| 03-FX-03 | 评估人员通过文件审查和人员访谈的方式，检查是否制定有应用系统与安全设备配置安全规范或软件安全开发规范并且承诺能够对相关系统的Web应用服务及相关协议及时修复已公布的漏洞。 | 涉及 | 参照《中移信息技术有限公司网络安全防护管理办法》 |
| 客户端安全风险 | 04-FX-01 | 评估人员通过人员访谈的方式，查询是否有客户端软件版本管理、版本更新发布机制。 | 不涉及 | 为中国移动集团公司手厅或网厅的一个功能模块，不存在客户端软件版本管理、版本更新发布机制。 |
| 04-FX-02 | 评估人员通过人员访谈的方式，查询是否有相关的软件安装、更新、运行、卸载相关的开发规范与用户告知说明。 | 不涉及 | 为中国移动集团公司手厅或网厅的一个功能模块，不存在客户端软件版本管理、版本更新发布机制。不存在客户端软件安装、更新、运行、卸载 |
| 04-FX-03 | 评估人员通过人员访谈的方式，了解客户端软件是否具备联网功能。 | 不涉及 | 为中国移动集团公司手厅或网厅的一个功能模块，不存在客户端软件版本管理、版本更新发布机制。，不存在客户端软件 |
| 04-FX-04 | 评估人员通过人员、演示查验的方式，了解客户端软件是否存在恶意行为，如系统提权、监听用户操作、窃取用户隐私等。 | 不涉及 | 为中国移动集团公司手厅或网厅的一个功能模块，不存在客户端软件版本管理、版本更新发布机制。不存在客户端软件 |
| 04-FX-05 | 评估人员通过人员访谈的方式，了解是否定期对客户端业务系统进行安全检测并定期修复漏洞。 | 不涉及 | 为中国移动集团公司手厅或网厅的一个功能模块，不存在客户端软件 |
| 他业务逻辑安全风险 | 05-FX-01 | 评估人员通过人员访谈的方式，查询业务是否具有业务订购功能。 | 涉及 | 业务具有业务订购功能，如订购流量包 |
| 05-FX-02 | 评估人员通过人员访谈的方式，查看是否制定了业务认证机制。 | 涉及 | 通过对比登录和办理的号码是否一致，同时在办理过程有短信验证码 |
| 05-FX-03 | 评估人员通过人员访谈的方式，检查是否制定有业务安全使用的开发相关规范并且承诺在应用开发阶段严格遵守该规范。 | 涉及 | 制定有业务安全使用的开发相关规范 |
| 非授权采集风险 | 06-FX-01 | 评估人员通过文件审查的方式，检查与用户签订的用户协议中是否包含收集用户信息的范围、类型及使用目的等内容。 | 涉及 | 参照《中国移动客户端软件服务协议》执行 |
| 06-FX-02 | 评估人员通过人员访谈的方式，检查业务系统采集的数据结果是否包含超出明确告知给用户的信息收集范围、类型及使用目的等内容。 | 涉及 | 业务系统采集的数据结果没有包含超出明确告知给用户的信息收集范围、类型及使用目的等内容。 |
| 数据存储风险 | 07-FX-01 | 评估人员通过人员访谈的方式，了解业务系统是否提供面向外部用户的服务。 | 涉及 | 商城服务子系统提供流量包服务办理、优惠券办理等，面向移动现网用户，销售子系统提供移动现网用户、以及互联网用户注册 |
| 07-FX-02 | 评估人员通过人员访谈的方式，了解业务系统是否存在与公网的访问接口。 | 涉及 | 业务系统存在与公网的访问接口。 |
| 07-FX-03 | 评估人员通过文件审查的方式，检查针对业务系统是否制定了网络设备与安全设备配置安全规范。 | 涉及 | 参照《中移信息技术有限公司网络安全防护管理办法》《移动商城网络与系统安全管理办法》执行 |
| 07-FX-04 | 评估人员通过人员访谈的方式，检查在保持系统运行稳定的前提下，针对业务系统是否承诺能够对相关设备的操作系统和关键服务协议及时安装更新或补丁。 | 涉及 | 有对相关设备的操作系统和关键服务协议安装更新或补丁 |
| 数据管理风险 | 08-FX-01 | 评估人员通过人员访谈的方式，检查是否对数据信息的访问进行权限管理。 | 涉及 | 对数据信息的访问进行权限管理。 |
| 08-FX-02 | 评估人员通过文件审查的方式，检查是否制定了相应的应急处置计划和配套的处置措施。 | 涉及 | 制定应急处置方案 |
| 08-FX-03 | 评估人员通过文件审查、人员访谈的方式，检查是否制定了数据安全监督的相关管理办法。 | 涉及 | 暂未有数据安全监督的相关管理办法 |
| 数据传输风险 | 09-FX-01 | 评估人员通过人员访谈的方式，查看是否对内部数据传输链路采取了技术防护手段。 | 涉及 | 对内部数据传输链路采取技术防护手段。 |
| 数据加工风险 | 10-FX-01 | 评估人员通过人员访谈的方式，询问采取的数据加工方式。 | 不涉及 | 不涉及数据加工 |
| 10-FX-02 | 评估人员通过人员访谈的方式，询问数据加工中使用的用户数据类型，并与明确告知给用户的数据挖掘范围进行对比 | 不涉及 | 不涉及数据挖掘 |
| 10-FX-03 | 评估人员通过人员访谈的方式，询问在进行数据分析和挖掘的过程中，是否进行了数据脱敏。 | 不涉及 | 不涉及数据分析和挖掘 |
| 10-FX-04 | 评估人员需通过人员访谈的方式，询问数据挖掘分析后是否会形成国家关键数据，是否具备相应的保障能力。 | 不涉及 | 不涉及数据挖掘分析 |
| 数据转移风险 | 11-FX-01 | 评估人员通过人员访谈和文件审查的方式，询问接收数据的第三方的安全防护能力情况。 | 不涉及 | 没有接收数据的第三方 |
| 11-FX-02 | 评估人员采用人员访谈和文件审查的方式，询问提供给第三方的数据类型。 | 不涉及 | 没有接收数据的第三方 |
| 11-FX-03 | 评估人员采取人员访谈和文件审查的方式，查看与第三方签订的协议中是否包含数据使用权限的内容，以及第三方对数据使用情况调查。 | 不涉及 | 没有接收数据的第三方 |
| 11-FX-04 | 评估人员采取人员访谈和文件审查的方式，询问是否对第三方进行必要的安全监督管理，并查阅相关记录。 | 不涉及 | 没有接收数据的第三方 |
| 数据删除风险 | 12-FX-01 | 评估人员采取人员访谈和文件审查的方式，询问是否为用户提供删除个人信息的服务。 | 不涉及 | 不为用户提供删除个人信息的服务。 |
| 业务运行安全风险 | 13-FX-01 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务是否采集、存储、管理、传输、加工、转移、删除能够识别自然人个人身份或反应自然人活动的用户个人信息。 | 涉及 | 存储用户交易类信息 |
| 13-FX-02 | 评估人员通过人员访谈的方式，了解被评估业务的业务逻辑，包括业务规则、业务流程等的合规性和合理性。 | 涉及 | 业务规则、业务流程合规、合理。 |
| 13-FX-03 | 评估人员通过人员访谈的方式，了解被评估业务是否包含电信业务涉及的电信网码号资源、电信线路等。 | 不涉及 |  |
| 13-FX-04 | 评估人员通过人员访谈的方式，了解业务是否具有并发语音呼叫、话务转接等功能。 | 不涉及 |  |
| 13-FX-05 | 评估人员通过人员访谈、演示查验等方式，了解业务是否租用语音专线外呼。 | 不涉及 |  |
| 13-FX-06 | 评估人员通过人员访谈的方式，了解被评估业务是否包含码号传送功能。 | 不涉及 |  |

## 3.2 风险说明

综合以上分析，针对业务安全风险，“移动商城”在业务应用安全、业务平台安全、web应用安全等方面建立了较为完备的信息安全保障体系，但存在以下安全风险。

1. 合作方信息安全保障存在风险

业务运营在合作（技术合作和服务合作）开展前未对合作信息安全保障能力（管理制度和技术手段）进行了评估，未能提供相关的文档。

1. 数据安全存在风险

“移动商城”业务暂未制定数据安全监督管理办法，应对业务数据的传输、存储、使用等建立整体性的规范。

1. 追踪溯源风险

“移动商城”制定有日志管理制度，但在销售子系统运营过程中缺少威胁日志留存管理规范，如未对用户搜索违法信息的行为进行日志留存。

# 4 配套安全管理措施

## 4.1 日常安全管理介绍

**1.中移信息技术有限公司信息安全总体管理情况**

在机构设置方面，中移信息技术有限公司于2018年5月成立了专门的信息安全管理部门安全管理中心，目前拥有专职人员23人。此外，综合业务部、财务部、党委办公室、纪检监察部、内审部、人力资源部、规划技术部、运营管理部、工程建设部、大数据平台部、大数据应用部、管理信息系统部、基础平台部、采购中心、研发测试中心、电子渠道运营中心、物联网运营中心、国际业务运营中心、交易业务运营中心、交易业务运营中心、北京业务支撑中心、深圳业务支撑中心、广州业务支撑中心、全网监控与支持中心、企业管理支撑中心、天津中心、黑龙江中心、宁夏中心、河北中心、内蒙古中心、吉林中心、新疆中心、甘肃中心、青海中心、海南中心等34个部门均设有信息安全接口人，分管各部门内部的信息安全事宜。

在制度建设方面，中移信息已制定网络安全责任管理办法、安全事件管理办法、安全应急保障管理办法、互联网新技术新业务信息安全评估管理办法、客户信息安全保护管理办法、网络安全防护管理办法、网络安全三同步管理办法等信息安全相关制度。

在新技术新业务信息安全评估方面，中移信息依据新技术新业务评估管理办法，明确了评估清单报备工作机制，业务定期核查机制以及信息安全评估工作流程。依据上级部门要求建立互联网新技术新业务信息安全评估细则，将“通信能力开放平台”、“基于大数据技术的应用及服务”、“支持业务申请线上受理”等重点业务纳入信息安全评估清单。截止目前，中移信息的信息安全评估工作通过企业自评估的方式开展（含委托第三方开展）。

**2.移动商城业务管理情况**

“移动商城”业务制定了以下安全管理制度，基本满足安全管理要求。如：

《中国移动商城服务子系统应急预案》

《移动商城服务子系统日志管理制度》

《移动商城销售子系统日志留存管理规范》

《移动商城销售内容发布机制》

## 4.2 应急管理措施介绍

中移信息制定了《中移信息技术有限公司安全应急保障管理办法》，根据安全事件级别，确立响应时限要求，安全事件上报要求，三级及以上事件信息及时上报工信部和当地的通管局，四级安全事件不上报；三级安全事件在事件处理完毕后24小时内上报；二级安全事件在4小时内上报；一级安全事件在1小时内上报。重大保障期间必须对网站系统实现7\*24小时网站安全监测，对网站出口流量数据做到7\*24小时的实时监控和回溯能力。重大保障期间应安排专业的安全服务人员现场安全值守，通过合理使用安全管理中心及其他安全设备，对系统的安全状态进行监控，并根据实际环境完善安全管理平台及其他安全设备的告警规则，通过合理的规则配置，及时发现正在发生的安全事件以及现有潜在的安全风险，并及时定位问题，处理问题。

## 4.3 安全保障能力分析表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **保障能力类型** | **BZ编号** | **企业保障能力评估要点** | **评估意见** | **评估记录** |
| 业务应用安全保障 | 01-BZ-01 | 评估人员通过人员访谈、文件审查等方式，了解是否建立了业务上线前、或用户规模发生较大变化时及时开展评估工作的管理制度，并查看历史评估报告。 | 合格 | 建立了业务上线前、或用户规模发生较大变化时及时开展评估工作的管理制度，且是初次评估 |
| 01-BZ-02 | 评估人员通过人员访谈、文件审查等方式，了解是否建立了业务上线前、或用户规模、或业务功能、或基础资源配置、或技术实现方式发生较大变化时及时开展评估工作的管理制度，并查看评估报告。 | 合格 | 建立了业务上线前、或用户规模、或业务功能、或基础资源配置、或技术实现方式发生较大变化时及时开展评估工作的管理制度，且是初次评估 |
| 01-BZ-03 | 评估人员通过使用验证，针对存在信息发布功能的业务，完成一次用户注册操作，确认是否在注册环节要求用户提供真实身份信息，并通过短信等方式进行验证。 | 不合格 | 商城服务子系统工作台账户为电子渠道统一用户管理平台分配的账号，不提供用户注册。商城销售子系统开放了互联网用户注册，使用邮箱验证即可注册成功，无需绑定手机号 |
| 01-BZ-04 | 评估人员通过演示查验方式，模拟普通用户变更身份相关信息（如手机号码等），查看是否进行验证。 | 不涉及 | 不提供普通用户变更身份信息 |
| 01-BZ-05 | 评估人员需查看系统后台记录，是否留存用户身份信息变更日志记录及日志记录内容。 | 不涉及 | 不提供用户身份信息变更 |
| 01-BZ-06 | 评估人员通过测试验证的方式，访问应用的登录界面，查看登录时是否采用人机交互验证策略和机制。 | 合格 | 登录移动集团手厅或网厅的中国移动手机用户可直接进行访问，无需单独在该业务进行登录；登录网页或触屏版的用户通过手机验证码登录。商城互联网用户通过用户名密码图片验证码登录 |
| 01-BZ-07 | 评估人员通过测试验证的方式，使用网络抓包分析工具抓取登录数据包，查看是否在登录操作的通信过程中是否采用SSL/TLS协议或者其他加密协议或方法确保用户密码的传输安全。 | 不合格 | 中国移动手机用户可直接通过短信验证码进行访问，互联网用户登录或输入用户密码，用户登录为加密传输；但商城服务子系统工作台操作员登录过程为明文传输 |
| 01-BZ-08 | 评估人员通过测试验证的方式，使用网页分析工具查看是否在COOKIE中保存用户密码。 | 合格 | 未保存用户密码 |
| 01-BZ-09 | 评估人员通过测试验证的方式，检查是否存在用户弱口令。 | 合格 | 未发现弱口令 |
| 01-BZ-10 | 评估人员通过访谈、日志查验或测试验证的方式，检查业务系统的身份认证失效机制是否能够按照制定的密码更换周期进行有效提示更新。 | 合格 | 登录移动集团手厅或网厅的中国移动手机用户可直接进行访问，无需单独在该业务进行登录或输入用户密码，登录网页版需要短信验证码验证登录 |
| 01-BZ-11 | 评估人员通过访谈或测试验证的方式，检查业务系统的会话失效机制是否能够按照制定的失效时间进行有效执行。 | 不合格 | 业务系统的会话失效机制与电子渠道统一运营管理平台一致，会话失效时间为1天，不满足相关要求。 |
| 01-BZ-12 | 评估人员通过测试验证的方式，使用错误的或禁用的账号密码/其他认证/验证码等登录，尝试访问先前正常登陆账号能访问的页面，检查身份认证失效机制和会话失效机制能否仍能有效执行。 | 合格 | 能够正常执行身份人失效机制和会话失效机制 |
| 01-BZ-13 | 评估人员通过测试验证的方式，查看认证错误提示是否存在泄露信息，当认证失败时，向用户提供的错误信息不应该区分是账号错误还是密码错误，而是通用的提示信息。 | 合格 | 商城服务子系统工作台、销售子系统工作台认证失败时，错误提示为通用提示 |
| 01-BZ-14 | 评估人员通过人员访谈、文件审查等方式，查看是否建立了用户身份信息保护相关管理制度。 | 合格 | 建立了用户身份信息保护相关管理制度。 |
| 01-BZ-15 | 评估人员通过人员访谈、使用验证等方式，查看是否配套了必要的技术手段保障用户身份信息的保密性和完整性。 | 不合格 | 商城服务子系统工作台部分信息采用明文传输，能够泄露用户的账号和密码信息 |
| 01-BZ-16 | 评估人员通过人员访谈等方式，了解是否建立覆盖业务所有内容及信息格式的违法信息监测处置的工作机制和技术手段；如是，询问技术手段实现途径与违法信息监测处置流程。 | 合格 | 服务子系统建立敏感词库，先审后发等手段实现违法信息监测处置 |
| 01-BZ-17 | 评估人员通过演示查验等方式，查看是否留存删除日志记录，查看是否能够调取相关记录。 | 合格 | 留存删除日志记录 |
| 01-BZ-18 | 评估人员查看是否建立违法信息样本库，查看违法信息样本库的更新记录。 | 不合格 | 销售子系统未建立违法信息样本库 |
| 01-BZ-19 | 评估人员注册账号，以用户身份发送含有违法信息的文字、图像、音频、视频等，确认信息能否发送成功。 | 合格 | 用户不可发送信息，评论处仅能够进行评分 |
| 01-BZ-20 | 评估人员通过人员访谈、演示查验等方式，检查是否对图片、语音、视频或小语种等公共信息建立了先审后发机制。 | 合格 | 营销类信息按照活动支撑工作流程建立了先审后发机制。 |
| 01-BZ-21 | 评估人员通过人员访谈、演示查验等方式，检查公共信息的审核是否采用了技术加人工方式。 | 合格 | 公共信息的审核采用技术加人工方式。 |
| 01-BZ-22 | 评估人员通过人员访谈、使用测试等方式，查看在业务使用过程中，是否配备了用户真实身份鉴别管理制度和技术手段。 | 合格 | 配备了用户真实身份鉴别管理制度 |
| 01-BZ-23 | 评估人员通过测试验证方式，针对具备第三方/用户发布信息功能的业务，实际完成一次注册操作，查看在注册环节，是否明确告知用户禁止发布、复制、传播违法信息，是否明确要求用户承诺遵守法律法规(《互联网信息服务管理办法》第十五条)、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等七条底线。 | 不涉及 | 第三方或用户不能发送信息 |
| 01-BZ-24 | 评估人员对用户管理人员进行访谈，针对具备第三方/用户发布信息功能的业务，询问是否根据累计发送违法信息次数等参数对个人账号、公众账号、聊天群组进行安全等级划分；如是，询问等级划分梯度、各等级违法信息处置机制及实现方式等。针对个人账号、公众账号、聊天群组后台数据中是否有安全等级划分及配置相应的处置策略。 | 不涉及 | 第三方或用户不能发送信息 |
| 01-BZ-25 | 评估人员查看人员配备文件，针对具备第三方/用户发布信息功能的业务，查看是否配备专门人员管理公众账号，文件中是否含有人员名单和工作联系方式。 | 不涉及 | 第三方或用户不能发送信息 |
| 01-BZ-26 | 评估人员查看制度文件、工作手册等，针对具备第三方/用户发布信息功能的业务，是否含有针对公众账号发布的公开信息内容作违法信息日常监测巡查的机制和管理要求。 | 不涉及 | 第三方或用户不能发送信息 |
| 01-BZ-27 | 评估人员对公众账号管理人员进行访谈，针对具备第三方/用户发布信息功能的业务，询问违法信息处置方式和流程，是否有相关处置工作的记录。 | 不涉及 | 第三方或用户不能发送信息 |
| 01-BZ-28 | 评估人员实际完成一次群组创建，检查是否明示群组人数上限，是否明确告知：a) 不得复制、发布、传播违法信息； b) 群创建者和群管理者对群组负有管理责任，需承诺本群组不发布、传播违法信息。 | 不涉及 | 不涉及创建群组 |
| 01-BZ-29 | 评估人员查验系统配置，是否对群组人数设置上限，是否对群组违法信息的发布、传播进行监测和处置。 | 不涉及 | 不涉及创建群组 |
| 01-BZ-30 | 评估人员通过人员访谈、文件审查等方式，针对具备第三方/用户发布信息功能的业务，检查是否针对信息发布环节的链接转发、添加评论转发、跨平台分享等功能配套了违法信息监测和处置的管理机制和技术手段。 | 不涉及 | 第三方或用户不能发送信息，评价中心仅能够进行评分，消息中心通过接口调用移动内部服务，服务子系统不控制消息内容 |
| 01-BZ-31 | 针对具备第三方/用户发布信息功能的业务，评估人员分别实际使用一次链接转发、添加评论转发、跨平台分享功能，在有关位置输入违法信息关键字，验证信息是否发送成功。 | 不涉及 | 第三方或用户不能发送信息 |
| 01-BZ-32 | 针对具备第三方/用户发布信息功能的业务，评估人员需使用业务，尝试在具有信息联动发布功能的业务平台上发布违法信息，或将违法有害信息分享至其他业务平台上，查看是否具备迅速切断同步或关联关系，并联动删除各关联平台上的违法信息的能力。 | 不涉及 | 第三方或用户不能发送信息 |
| 01-BZ-33 | 评估人员需查看系统后台记录，查阅是否留存违法信息联动删除操作日志及日志记录内容 | 不涉及 | 不涉及信息联动发布 |
| 01-BZ-34 | 评估人员需使用业务，查看在业务使用前，是否明确告知用户业务推送信息的种类，用户可自主选择是否接收信息，或在业务系统设置是否包含信息推送功能管理的选项 | 不合格 | 用户不能自主选择接收信息，用户是否可退订，未显示在推送短信内容中 |
| 01-BZ-35 | 评估人员使用业务，在不同时间段针对业务平台进行若干次访问，或发布若干条公众信息，随后请导出相关的访问记录；或从日志留存系统页面展示相关记录。评估人员需提供一定查询条件，由相关人员在日志留存系统进行操作演示，验证日志留存系统的查询、检索和审计功能。 | 合格 | 有访问操作相关记录 |
| 01-BZ-36 | 对于已上线的业务，需请提供满足留存时间要求的日志记录；针对未上线的业务，需请提供日志留存系统设计文件，证明其能够满足留存时间要求。 | 合格 | 日志记录满足要求 |
| 业务平台安全保障 | 02-BZ-01 | 评估人员需查看上报给主管部门的业务开办信息，包括业务机房/节点列表、占用机房位置等，并与实际情况进行核对。 | 合格 | 上报给主管部门的业务开办信息与实际情况进行一致 |
| 02-BZ-02 | 评估人员需查看业务系统拓扑图，并访谈相关负责人员，询问针对境内外交互数据的管理制度，以及配套的技术监管手段。 | 合格 | 不存在境内外数据交互 |
| 02-BZ-03 | 评估人员需查看业务后台系统实时运行数据和日志记录，核实是对资源分配使用情况进行实时监控和日志记录。 | 合格 | 能够对资源分配使用情况进行实时监控和日志记录 |
| 02-BZ-04 | 评估人员需查看关于违法信息监测处置制度文件和技术手段配备情况，核验侧是否可执行行业主管部门下发的违法信息监测和处置指令。 | 不合格 | 服务子系统提供敏感词配置管理等技术，对违法信息进行过滤处置，销售子系统暂未配备相关手段 |
| 02-BZ-05 | 评估人员需查看留存业务相关日志记录，核实日志的类型、内容和留存时间是否满足相关法律法规要求。 | 合格 | 存在业务相关日志记录，日志的类型、内容和留存时间满足相关法律法规要求 |
| 02-BZ-06 | 评估人员需向询问，是否对合作/用户的业务经营许可资质进行核实，并留存相关资料； | 合格 | 合作方具有业务经营许可资质 |
| 02-BZ-07 | 评估人员需查看与服务对象签订的协议中，是否包含用户需提供真实身份的内容； | 合格 | 该业务系统提供服务过程中参照《中国移动网站服务协议》执行 |
| 02-BZ-08 | 评估人员需访谈相关负责人，询问是否建立了针对合作信息安全保障能力（管理制度和技术手段）评估机制； | 不合格 | 暂未对合作对象有信息安全保障能力（管理制度和技术手段）建立评估机制 |
| 02-BZ-09 | 评估人员访谈相关负责人，询问是否通过开放接口进行交互的数据建立了安全审核机制和技术保障手段。 | 不涉及 | 未对外开放接口，只有调用移动集团手厅或网厅的接口 |
| Web应用安全保障 | 03-BZ-01 | 评估人员通过测试验证的方式，分别登陆不同级账号，检查不同级账号在分级页面的权限区别，以确认是否存在不同级别账号的管控。 | 合格 | 通过电渠运营统一用户管理模块进行开户申请和权限分配，不同账号权限不同 |
| 03-BZ-02 | 评估人员通过测试验证的方式，登陆超级账户或高权限账户，查看应用是否使用额外的物理验证设备、限制登陆IP或登陆设备手段等对超级账户或高权限账户的使用做出限制。 | 合格 | 移动商城服务子系统平台部分功能模块进行了IP白名单限制 |
| 03-BZ-03 | 评估人员通过人员访谈的方式，查看是否对业务应用运行状况进行日志记录。 | 合格 | 存在业务应用运行状况的日志记录 |
| 03-BZ-04 | 评估人员通过演示查验的方式，查看是否对用户的关键操作、重要行为、业务资源使用情况等重要事件进行日志记录。 | 合格 | 对用户的关键操作、重要行为情况等重要事件进行日志记录。 |
| 03-BZ-05 | 评估人员通过演示查验的方式，查看日志的留存时间长度是否能追溯到最近的6个月内。 | 合格 | 日志的留存时间长度能追溯到最近的6个月内。 |
| 03-BZ-06 | 评估人员通过测试验证的方式，采用Web应用漏洞扫描工具对系统的Web应用服务及相关协议进行漏洞扫描。 | 不涉及 | 本次评估暂未进行漏洞扫描 |
| 03-BZ-07 | 评估人员通过文件审查和测试验证的方式，查看应用系统与安全设备配置安全规范或软件安全开发规范中是否有要求对应用会话并发连接数做出限制，并采用压力测试工具和抓包工具进行测试验证，查看实际并发会话通讯情况是否属实。 | 不合格 | 未对并发连接数进行限制 |
| 客户端安全保障 | 04-BZ-01 | 评估人员通过测试验证的方式，检查客户端软件的应用版本的更新机制是否正常。 | 不涉及 | 为移动集团手厅或网厅的一个功能模块，不存在客户端软件版本管理、版本更新发布机制。 |
| 04-BZ-02 | 评估人员通过验证测试的方式，采用Android分析审计工具，分析移动应用在安装、运行、更新时，是否安装了其他应用。 | 不涉及 | 为移动集团手厅或网厅的一个功能模块，不存在移动应用在安装、运行、更新 |
| 04-BZ-03 | 评估人员通过测试验证的方式，卸载已安装客户端软件，并检查程序文件是否有残留。 | 不涉及 | 为移动集团手厅或网厅的一个功能模块，不存在客户端软件卸载 |
| 04-BZ-04 | 评估人员通过测试验证方式，查看客户端中是否存在插件功能，若存在则应对运行的客户端中提供的插件进行规范性检查，插件应允许用户自主选择是否卸载，并且卸载后无残留。 | 不涉及 | 为移动集团手厅或网厅的一个功能模块，不存在客户端软件 |
| 04-BZ-05 | 评估人员通过测试验证的方式，采用网络抓包分析工具（Burpsuite/Wireshark等），分析网络传输过程中的敏感数据信息是否加密。 | 不涉及 |  |
| 04-BZ-06 | 评估人员通过测试验证的方式，采用网络抓包分析工具（Burpsuite/Wireshark等），分析网络传输过程中客户端软件的网络连接的频次是否进行了合理限制。 | 不涉及 |  |
| 04-BZ-07 | 评估人员通过测试验证的方式，采用Android分析审计工具，检查客户端的敏感权限使用情况，判断在涉及访问本地资源权限时是否正确提示用户授权情况。 | 不涉及 |  |
| 04-BZ-08 | 评估人员通过测试验证的方式，采用漏洞扫描工具，检查客户端业务系统是否存在高中危漏洞。 | 不涉及 |  |
| 业务逻辑安全保障 | 05-BZ-01 | 评估人员通过人员访谈的方式，了解业务订购行为是否需用户认证后才会生效。 | 合格 | 通过对比登录和办理的号码是否一致，同时在办理过程有短信验证码 |
| 05-BZ-02 | 评估人员通过访谈或演示查验的方式，检查出现超出业务阈值是否会给出安全提示。例如，若单日用同一手机号完成超过业务阀值的订购数量，应通过短信或邮件等形式给予用户安全提示。 | 合格 | 出现超出业务阈值，办理失败 |
| 05-BZ-03 | 评估人员通过测试验证的方式，检查在业务认证未通过时触发的保护策略是否正常运行。 | 合格 | 业务认证未通过时触发的保护策略正常运行。 |
| 05-BZ-04 | 评估人员通过测试验证的方式，验证规范的措施是否正常履行，例如检查核心业务的保障措施是否设置阈值，超过阈值时是否给予提示。 | 合格 | 有，超过阈值给予提示。 |
| 非授权采集保障 | 06-BZ-01 | 评估人员通过文件审查的方式，检查是否建立了用户个人信息收集保护及用户授权告知制度。在收集用户个人信息前，获得用户同意，并向用户明确告知授权范畴和风险提示。 | 合格 | 参照《中国移动个人信息保护政策》、《中国移动网站服务协议》执行 |
| 06-BZ-02 | 评估人员通过演示查验的方式，检查业务数据，判定收集用户个人信息的收集范围和使用范围是否遵循以提供服务的最小必要为标准。 | 合格 | 收集用户个人信息的收集范围和使用范围遵循以提供服务的最小必要为标准。 |
| 数据存储保障 | 07-BZ-01 | 评估人员通过人员访谈的方式，检查业务系统是否部署了能够防范网络攻击，检测病毒木马等恶意代码入侵的硬件设备或软件系统。 | 合格 | 部署了能够防范网络攻击的硬件设备。 |
| 07-BZ-02 | 对于业务系统已部署的防范网络攻击和检测病毒木马等恶意代码入侵的硬件设备或软件系统，评估人员通过测试验证的方式，检查是否及时更新了恶意代码软件版本和恶意代码库。 | 合格 | 及时更新了恶意代码软件版本和恶意代码库。 |
| 07-BZ-03 | 评估人员通过文件审查的方式，检查网络设备与安全设备配置安全规范是否设置有效策略，要求根据数据级别采用加密、授权、数字水印、数字签名等技术手段对业务系统存储的数据进行了安全存储保护。 | 合格 | 网络设备与安全设备配置安全规范设置有效策略，根据数据级别采用加密、等技术手段对业务系统存储的数据进行了安全存储保护。 |
| 07-BZ-04 | 评估人员通过测试验证的方式，使用漏洞扫描工具对业务系统进行检测，检查是否已对相关设备的操作系统和关键服务协议及时安装更新或补丁。 | 合格 |  |
| 07-BZ-05 | 评估人员通过人员访谈的方式，检查对于不同安全级别的数据进行权限管理过程中是否采取了相应的隔离措施和安全保护措施。 | 合格 | 采取了相应的保护手段 |
| 07-BZ-06 | 评估人员通过测试验证的方式，检查对业务系统是否采用加密或其他保护措施实现系统管理数据和重要业务数据存储保密性。 | 合格 | 对业务系统采用加密或其他保护措施实现系统管理数据和重要业务数据存储保密性。 |
| 数据管理保障 | 08-BZ-01 | 评估人员通过访谈方式，检查数据操作行为日志记录应至少包括操作时间、操作对象存储地址、操作指示等关键字段 | 合格 | 有对数据操作行为日志记录包括操作时间、操作对象存储地址、操作指示等关键字段 |
| 08-BZ-02 | 评估人员通过访谈的方式，检查本地数据备份与恢复功能。 | 合格 | 本地备份 |
| 08-BZ-03 | 评估人员通过访谈方式，检查异地数据备份功能，如利用通信网络将关键数据定时批量传送至备用场地。 | 不涉及 |  |
| 数据传输保障 | 09-BZ-01 | 评估人员通过人员访谈的方式，检查是否对数据传输方式采取了相应的安全防护措施。 | 不合格 | 登录过程明文传输 |
| 09-BZ-02 | 评估人员通过人员访谈的方式，查看是否对内部不同局域网间数据传输链路采取了技术防护手段。 | 合格 | 采取了防护手段 |
| 09-BZ-03 | 评估人员通过人员访谈的方式，查看数据传输链路是否设置了冗余链路。 | 合格 | 数据传输链路设置了冗余链路。 |
| 数据加工保障 | 10-BZ-01 | 评估人员通过人员访谈的方式，查看是否对拟采用公有云进行加工的数据重要性进行评估，判定其是否适合采取公有云服务进行加工。 | 不涉及 |  |
| 10-BZ-02 | 评估人员通过文件审查的方式，查看与云服务签订的服务合约中，是否明确提出云服务不得违规访问数据。 | 不涉及 |  |
| 10-BZ-03 | 评估人员通过人员访谈和文件审查的方式，询问是否建立了数据加工的管理制度，并且明确提出不得超范围进行数据挖掘。 | 不涉及 |  |
| 10-BZ-04 | 评估人员通过人员访谈和文件审查的方式，询问是否建立了数据加工的管理制度，并且明确提出数据加工前应对涉及用户个人敏感信息的内容应进行匿名化、模糊化、脱敏处理。 | 不涉及 |  |
| 10-BZ-05 | 评估人员通过人员访谈和演示查验的方式，查看据数据挖掘算法中参数变量的设置，是否包含用户个人敏感信息的输入内容。 | 不涉及 |  |
| 10-BZ-06 | 评估人员通过人员访谈的方式，询问对数据挖掘分析后形成的国家关键数据的技术防护措施。 | 不涉及 |  |
| 数据转移保障 | 11-BZ-01 | 评估人员需对人员访谈或文件审查的方式，询问将数据提供给第三方前，是否对第三方的数据安全防护能力进行评估，并查阅相关评估报告。 | 不涉及 | 未对第三方提供数据 |
| 11-BZ-02 | 评估人员采取人员访谈或文件审查的方式，询问将数据提供给第三方前，是否对数据的重要性、敏感性评估进行评估，并查阅相关评估报告。 | 不涉及 | 未对第三方提供数据 |
| 11-BZ-03 | 评估人员采取人员访谈或文件审查的方式，查看是否建立了数据转移管理制度，包含明示用户数据转移情况，并明确规范第三方数据使用权限。 | 不涉及 | 无数据转移 |
| 11-BZ-04 | 评估人员采取人员访谈或文件审查的方式，询问是否建立了针对第三方数据使用安全监督管理机制和技术手段。 | 不涉及 | 不涉及第三方数据使用 |
| 数据删除保障 | 12-BZ-01 | 评估人员采取人员访谈和演示查验的方式，询问是否在用户终止使用电信服务或者互联网信息服务后，业务系统能够停止收集和使用用户个人数据信息。 | 合格 | 在用户终止使用电信服务或者互联网信息服务后，业务系统能够停止收集和使用用户个人数据信息。 |
| 业务运行安全保障 | 13-BZ-01 | 评估人员通过人员访谈、文件审查等方式，了解业务办理过程中是否实施用户二次确认授权机制。 | 合格 | 业务办理过程中有短信验证码 |
| 13-BZ-02 | 评估人员通过人员访谈、文件审查等方式，了解业务办理环节是否单一采用或组合采用短信验证码、图片验证码、语音验证码、智力测试验证码等验证码类型进行用户身份验证。 | 合格 | 业务办理过程中有短信验证码 |
| 13-BZ-03 | 评估人员通过人员访谈、文件审查等方式，对端口类短信下发添加签名，防范不法分子伪造署名假冒企业进行短信下发。 | 合格 | 对端口类短信下发添加签名。 |
| 13-BZ-04 | 评估人员通过人员访谈、演示查验等方式，了解业务是否合理设置登录密码策略，明确密码长度、强度、复杂度等。 | 合格 | 密码长度不少于8位，必须包含英文字母大小写、数字和标点符号中的至少两种 |
| 13-BZ-05 | 评估人员通过人员访谈、演示查验等方式，了解业务是否对频繁试错登录、异地登录等业务异常登录情况进行监测。 | 不合格 | 对频繁试错登录、异地登录等业务异常情况未进行监测 |
| 13-BZ-06 | 评估人员通过人员访谈、演示查验等方式，了解业务是否通过短信提示、下发验证码二次确认等方式，强化业务登录行为的实时告知。 | 不合格 | 移动手机用户登录过程需要短信验证码验证登录，商城服务互联网用户注册登录使用邮箱注册登录，无实时告知 |
| 13-BZ-07 | 评估人员通过人员访谈、演示查验等方式，了解业务使用过程中存在通讯信息诈骗高风险的关键环节，是否采用短信验证码、密保问题、图片验证码、语音验证码、智力测试验证码等方式进行用户身份验证。 | 合格 | 移动现网用户通过短信验证码验证身份、互联网用户使用图片验证码验证身份 |
| 13-BZ-08 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格申请主体资格管控，是否存在违规为个人用户办理语音专线、“400”、“商务总机”业务。 | 不涉及 |  |
| 13-BZ-09 | 评估人员通过人员访谈、文件审查等方式，了解业务是否制定业务管理文件，明确业务在申请主体资格管控、渠道管理、资质核验、码号申请数量管理、台账管理、落地号码管理、外呼管理、合同管理、业务使用复核监测、退出管理、定期检查、考核问责、工作规程管理等关键环节的管理要求。 | 不涉及 |  |
| 13-BZ-10 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严禁代理渠道或网络渠道代为办理。 | 不涉及 |  |
| 13-BZ-11 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格落实用户实名信息核验登记。基础电信企业应建立用户真实有效身份信息核验登记留存机制，加强个人用户身份信息、单位用户证照信息核验，严格落实电信业务用户实名制。 | 合格 | 业务严格落实用户实名信息核验登记。 |
| 13-BZ-12 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格落实申请数量要求，同一用户在同一基础电信企业全国范围内申请“400”、“一号通”、“商务总机”等重点业务号码，每类原则上不得超过5个。 | 不涉及 |  |
| 13-BZ-13 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格落实台账管理，“400”、“一号通”、“商务总机”业务台账信息应包括用户资质、使用用途、真实落地号码等。 | 不涉及 |  |
| 13-BZ-14 | 评估人员通过人员访谈、文件审查等方式，了解“400”、“一号通”、“商务总机”等重点电信业务是否建立业务落地号码核验登记机制。 | 不涉及 |  |
| 13-BZ-15 | 评估人员通过人员访谈、文件审查等方式，了解业务在合同和协议中是否包含登记用户主体责任，细化责任条款。 | 合格 | 按照《中国移动网站服务协议》执行 |
| 13-BZ-16 | 评估人员通过人员访谈、文件审查等方式，了解业务是否利用语音专线进行超频、超时段外呼，利用其他码号等电信资源外呼行为管理是否严格。 | 不涉及 |  |
| 13-BZ-17 | 评估人员通过人员访谈、文件审查等方式，了解业务是否有退出管理。当出现异常情况时，应根据实际情况对相关业务及时予以关停、注销。 | 合格 | 业务有退出管理 |
| 13-BZ-18 | 评估人员通过人员访谈、文件审查等方式，了解基础电信企业应配套建立防范打击通讯信息诈骗相关重点电信业务的信息化管理手段。 | 不涉及 |  |
| 13-BZ-19 | 评估人员通过人员访谈、文件审查等方式，了解基础电信企业应配套建立用户终端侧安全提示服务相关技术手段 | 不涉及 |  |
| 13-BZ-20 | 评估人员通过人员访谈、文件审查等方式，了解语音专线是否实施主叫鉴权。企业应全面落实语音专线主叫鉴权机制，对未按规范进行主叫鉴权的呼叫一律拦截。 | 不涉及 |  |
| 13-BZ-21 | 评估人员通过人员访谈、文件审查等方式，了解语音专线呼叫转移管理是否严格。开通语音专线呼叫转移业务功能，应由基础电信企业集团公司统一审核并建立台账。 | 不涉及 |  |
| 13-BZ-22 | 评估人员通过人员访谈、文件审查等方式，了解是否建立外呼白名单制度，允许外呼的业务号码必须为本网实际开通的、属本企业分配的号码或号段，并统一纳入白名单管理。 | 不涉及 |  |
| 13-BZ-23 | 评估人员通过人员访谈、文件审查等方式，了解企业是否在接入侧设备上禁止违规传送主叫号码为空号或设置主叫号码禁显的呼叫。 | 不涉及 |  |
| 13-BZ-24 | 评估人员通过人员访谈、演示查验等方式，了解企业在网间关口局对不符合号码管理、网间互联规定和标准的违规呼叫、违规号码是否进行拦截。 | 不涉及 |  |
| 13-BZ-25 | 评估人员通过人员访谈、文件审查等方式，了解建立不良呼叫号码监测处置能力。 | 不涉及 |  |

## 4.4安全保障能力说明

1.“移动商城”采用手机号登录和互联网用户登录两种方式进行登录，手机用户登录认证过程采用服务密码和动态密码保护、会话失效机制、短信提示登录等保障措施，确保用户登录安全；但采用互联网登录的用户通过邮箱即可注册登录，未能与手机号码进行绑定，实名认证能力有待加强。

2.测试发现“移动商城”服务子系统工作台在登录过程中，用户名和密码均明文传输，敏感数据传输安全有待加强；且工作台账户未能限制单点登录，会话失效时间过长，身份认证、会话认证安全保障有待加强。

3.“移动商城”销售子系统未建立针对违法有害信息内容的监测处置工作机制和技术手段、违法信息样本库存等，未留存违法操作日志及日志记录内容，日志留存规范有待加强。

4.“移动商城”服务子系统下发的营销类端口短信未能提供业务退订，用户不可自主选择是否接收信息，业务应用安全性有待加强。

# 5评估结果及整改建议

## 5.1 信息安全管理风险评估结果

**1.企业总体信息安全管理风险评估结果**

中移信息建立了一系列网络与信息安全管理制度，包括网络安全责任管理办法、安全事件管理办法、安全应急保障管理办法、客户信息安全保护管理办法、网络安全防护管理办法、业务支撑网数据安全管理办法等相关规定和制度机制，管理制度体系较为完善，基本满足信息安全管理要求。

**2.“移动商城”业务信息安全管理风险评估结果**

“移动商城”业务制定了一系列安全管理制度，基本满足安全管理要求。但仍存在以下风险。

（1）第三方合作安全风险

风险类型：合作方信息安全保障能力不健全风险

风险描述：该业务暂未建立针对合作方信息安全保障能力（管理制度和技术手段）的评估机制，可能存在一定的安全风险。

整改建议：建议在合作开展前对合作方的信息安全保障能力进行评估。

（2）数据安全监督管理不健全风险

风险类型：数据安全监督管理不健全风险

风险描述：该业务缺少独立的数据安全监督管理办法

整改建议：相关办法应涉及业务使用的数据安全传输、存储、调用安全和接口交互数据的安全审计等方面。

## 5.2 信息内容安全风险评估结果

1.业务退订安全风险

风险类型：业务营销短信未提供业务退订

风险描述：向用户下发营销短信，用户不可自主选择是否接收信息，未包含是否接收信息推送功能管理的选项。

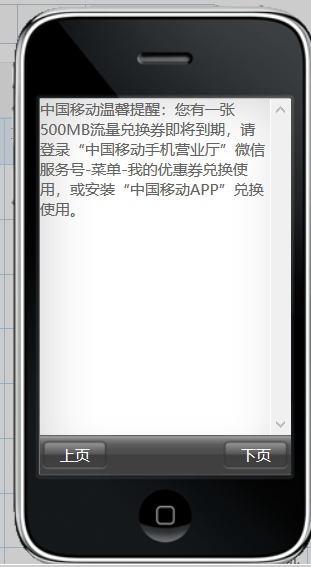
整改建议：建议在营销短信中增加“退订”功能，并在系统中增加是否接收消息推送的选项。

图2营销短信样式

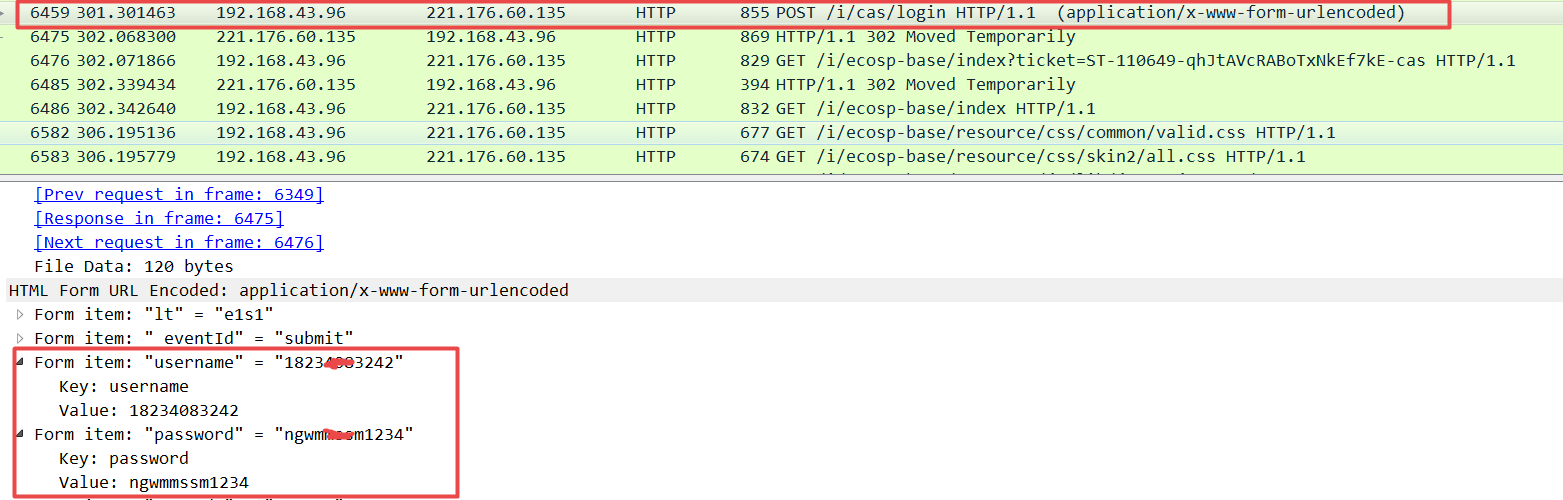
## 5.3 业务平台安全风险评估结果

1.敏感数据传输传输风险

风险类型：敏感信息泄露风险

风险描述：“移动商城”服务子系统工作台操作员、管理员用户信息登录时，在传输过程中未进行加密，直接明文传输，存在敏感信息泄露风险。

整改建议：建议采用SSL或者TLS协议加密传输。

图3 用户名密码明文传输

## 5.4 业务运行安全风险评估结果

1．实名认证身份机制不健全

风险类型：实名认证机制不健全

风险描述：移动商城提供的互联网用户注册方式，用户通过邮箱验证进行注册登录，未能与手机号码进行绑定，难以与用户真实身份信息建立联系。

整改建议：建议通过互联网方式进行注册的用户如进行购买等实际操作时，需绑定用户本人的真实手机号码。

2. 身份认证不健全

风险类型：管理员登陆未进行单点登陆限制

风险描述：管理员可以在多平台上进行登陆，未进行单点控制。若账户被盗用，不能及时发现账户可能面临的安全风险。

整改建议：对于高权限用户，应对管理员单点登陆进行限制，设置同一时间，仅能开启一个会话，并对会话失效时间进行限制，不得超过30分钟。

3.验证码接口安全

风险类型：验证码频繁获取次数未进行限制

风险描述：未对验证码的频繁获取次数进行限制，网站的动态短信发送接口可能被短信轰炸工具收集，造成无法正常使用移动运营商业务。

整改建议：建议添加验证码频繁获取次数限制，防止接口被恶意频繁调用进行轰炸攻击。

4.异地登录等业务异常情况监测

风险类型：未对异地登录等业务异常情况进行监测

风险描述：异地登录等业务异常情况未能够进行提醒，不能及时发现账户可能面临的安全风险。

整改建议：建议添加异地登录等异常情况监测手段，能够对非常用地点的登录进行实时短信提醒。

5.日志留存不完善

风险类型：日志留存系统检索、溯源不健全风险

风险描述：服务子系统日志留存系统未能支持全字段检索、销售子系统未留存违法信息监测日志。

整改建议：建议完善日志留存模块，支持如登陆用户、登陆时间等全字段检索。建议留存违法信息监测处置日志。

图5 日志留存不完善

# 6安全评估结论意见

通过开展信息安全风险评估工作，评估组认为：中移信息技术有限公司在日常网络安全运维、内容安全管控、日常安全拨测、安全事件应急、数据安全保障等方面已建立较为全面的安全管理流程和风险防范机制，但在“移动商城”业务存在如下问题：

评估发现“移动商城”业务存在管理风险2个，内容风险2个，平台风险1个，平台运行风险5个，需进一步完善该业务相关管理制度建设和相关日志留存，在数据传输方式建议采取加密传输，同时加强销售子系统违法违规不良信息的监测处置机制及技术手段，并建立违法违规不良信息库。