中国电信互联网新业务安全评估报告

**产品名称：短信营业厅**

**评估单位：国家计算机网络与信息安全管理中心**

**2019年11月**

**目录**

[1 业务基本情况介绍 3](#_Toc513621542)

[1.1 业务名称 3](#_Toc513621543)

[1.2 业务功能介绍 3](#_Toc513621544)

[1.3 技术实现方式介绍 3](#_Toc513621545)

[1.4 （预期）用户规模 5](#_Toc513621546)

[1.5 市场发展情况 5](#_Toc513621547)

[2 安全评估情况 5](#_Toc513621548)

[2.1 安全评估情况概述 5](#_Toc513621549)

[2.2 评估人员组成 6](#_Toc513621550)

[2.3 评估实施流程 7](#_Toc513621551)

[2.4 业务风险识别分析 8](#_Toc513621552)

[2.4.1 整体风险分析矩阵 8](#_Toc513621553)

[2.4.2 高风险识别分析说明 17](#_Toc513621554)

[2.4.3 配套安全管理措施 17](#_Toc513621555)

[3 安全评估结论意见 25](#_Toc513621556)

[3.1 匹配性分析 25](#_Toc513621557)

[3.2 企业整改建议及落实情况 27](#_Toc513621558)

[3.2.1 整改建议 27](#_Toc513621559)

[3.2.2 整改落实情况 27](#_Toc513621560)

[3.3 安全评估结论 27](#_Toc513621561)

[3.4 同类业务的监管建议 27](#_Toc513621562)

[3.5 评估结果签字确认 28](#_Toc513621563)

# 业务基本情况介绍

## 业务名称

河南电信-短信营业厅

## 业务功能介绍

河南电信-短信营业厅是电子渠道的重要组成部分，通过短信方式向客户提供自有及合作产品营销服务，并为其他渠道提供回复、确认、提醒等渠道协同服务，既是重要的服务窗口，也是重要的营销渠道。

## 技术实现方式介绍

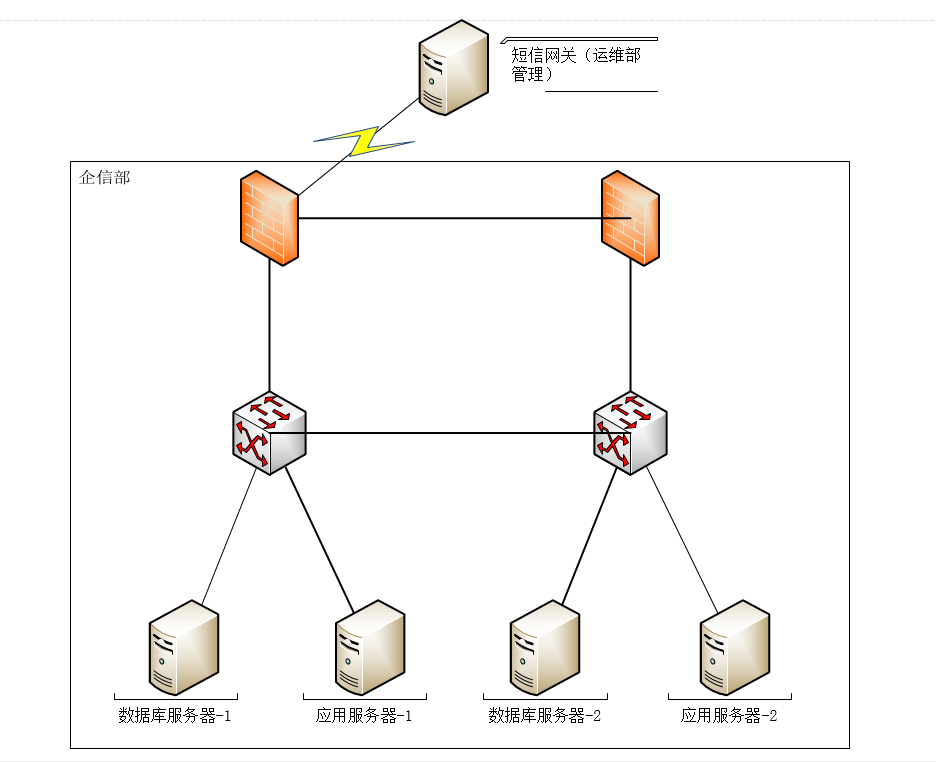
短信作为电子渠道的一部分，其功能主要为渠道管理功能、客户服务功能和营销执行功能，贯穿渠道管理功能域、客户服务功能域、订单和服务请求功能域以及营销管理功能域等。如下图所示，短信营业厅系统主要包含业务功能和系统功能两个部分。

业务功能包括个人业务和渠道业务。个人业务包括订单受理类业务、服务请求类业务、积分服务、密码服务、缴费服务、投诉建议、主动营销和主动服务；渠道业务包括代销商的店员积分服务和空中充值服务。其中，短信综合渠道面向个人客户和销售渠道代销商服务，交互方式有菜单交互方式、编码点播方式。

系统功能包括会话管理、菜单管理、功能指令管理、回复内容管理等基础管理功能和短信处理功能。短信处理功能包括短信收发、内容解析、业务处理引擎、信息封装、解析规则、封装规则等。其中，基础的会话管理、菜单管理、功能指令管理、回复内容管理支撑短信处理功能；短信处理功能支撑业务功能。



短信营业厅平台主要由数据库服务器、应用服务器两个主要部分组成，可以通过防火墙对外访问。用户可以通过发短信到网关，网关在送到短信营业厅。短信营业厅处理完成在发送给短信网关，短信网关在把处理结果短信发送给用户。



## （预期）用户规模

按照集团短信营业厅规划，仅限于河南省内电信用户使用，设计用户规模为千万以上级别。

## 市场发展情况

随河南电信实际用户规模变化。

# 安全评估情况

## 安全评估情况概述

根据《中国电信〔2015〕348号关于印发中国电信新技术新业务信息安全评估管理办法（试行）的通知》的要求，结合“短信营业厅”产品情况，国家计算机网络与信息安全管理中心对河南电信“短信营业厅”业务开展了新技术新业务信息安全现场评估工作。

本次评估使用《互联网新技术新业务安全评估指南》中规定的业务安全风险评估模型，并根据评估业务的具体情况识别业务对应于每个评估模块是否存在相应的信息安全风险。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、数据安全检测等。

## 评估人员组成

|  |  |  |  |
| --- | --- | --- | --- |
| **姓名** | **部门** | **工作岗位** | **联系方式** |
| 马宏远 | 国家计算机网络与信息安全管理中心 | 信息安全评估  组长 | 13910138904 |
| 姜淦卿 | 国家计算机网络与信息安全管理中心河南分中心 | 信息安全评估  工作人员 | 15838060425 |
| 宋乔 | 国家计算机网络与信息安全管理中心辽宁分中心 | 信息安全评估  工作人员 | 18840644109 |
|  |  |  |  |
|  |  |  |  |

## 评估实施流程

本次业务评估依据《互联网新技术新业务安全评估指南》相关要求，评估实施流程包括评估准备阶段、评估实施阶段和评估总结阶段：

**评估准备阶段：**2019年11月16日，成立信息安全评估小组，确定小组成员，向河南电信收集业务相关的管理文档和技术文档等资料，了解业务市场发展情况、业务自身情况以及业务使用流程等信息，根据业务情况与被评估方进行深入交流，明确评估重点。

**评估实施阶段：**2019年11月28日，评估人员对业务相关人员进行了实地调研，通过人员访谈、系统查看、评测验证等多种方式对业务的安全风险以及企业的安全保障能力进行了核实验证。

* 文档查阅：对照评估指标，评估人员提出业务安全保障相关的进一步制度文件需求，企业安排相关人员准备提供，评估人员进行查阅。
* 系统查看，对照评估指标，企业安排相关人员，对业务系统平台的日志记录、内容安全保障技术手段等进行介绍展示，评估人员进行核实确认并保留截图记录。
* 人员访谈：对照评估指标，企业安排网络信息安全部、业务部门以及业务合作方相关人员，对评估人员提出的问题进行回应与讨论。

**评估总结阶段：**针对业务安全风险分析以及安全保障能力评估结果，撰写评估报告，形成评估结论，并提出合理化的企业安全保障能力整改建议。

## 业务风险识别分析

### 整体风险分析矩阵

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **评估事项** | **评估模块** | **评估指标** | **评估内容** | **评估方法** | **评估意见** | 研判依据 |
| 1.业务应用安全 | 1.1用户 | 1.1.1用户规模 | 用户规模主要关注使用业务的用户数量，数量越庞大，发生信息安全事件造成的影响范围越大，信息安全风险越高。 | 人员访谈&文档审查 | 安全风险较高 | 该业务用户规模为大于1000万 |
| 1.1.2用户类型 | 用户类型主要关注使用业务的用户属性特点，包括用户类别（单位用户或个人用户）、年龄分布、地域分布等。 | 人员访谈&测评验证 | 安全风险较低 | 该业务为用户自主注册，未聚焦于特定人群。 低 |
| 1.1.3用户相关性 | 用户相关性反映了特定用户之间联系的紧密程度，若特定用户间紧密关系被用于传播违法信息，则信息的可流通性、可信赖性、被关注程度将提高，信息安全风险将有所增加。 | 人员访谈&测评验证 | 安全风险较低 | 该业务为用户自主注册，用户线下不相识。 |
| 1.1.4用户实名核验 | 用户实名核验关注的是用户使用业务时是否提供了真实身份信息或有助于识别真实身份的相关信息，如果未提供上述信息，将影响企业配合完成事后溯源工作的开展。 | 人员访谈&测评验证 | 不适用 | 该业务使用时不需要用户注册、登录。 |
| 1.1.5用户真实身份鉴别 | 用户真实身份鉴别关注的是用户使用业务或应用过程中业务系统是否能够根据用户提供的必要证明凭证（如账号密码、业务验证信息等），判定其是否具有访问资源或者执行业务相关请求的必要权限，确保用户真实身份与业务应用使用行为的一致性；若业务系统不能对用户真实身份进行鉴别，可能导致用户账户信息被泄露、仿冒、盗取等严重安全事件。 | 人员访谈&测评验证 | 不适用 | 该业务使用时不需要用户注册、登录。 |
| 1.2信息主题 | 1.2.1信息主题多样性 | 信息主题多样性主要指信息内容围绕主题类别多元，如微博客类业务的信息内容主题类别繁杂，数量庞大，从多元信息中识别处置违法信息的难度更大。 | 人员访谈&测评验证 | 不适用 | 该业务的信息主题单一。 |
| 1.2.2信息主题相关性 | 信息主题相关性反映信息内容围绕的主题之间联系是否紧密。若内容大多围绕一个或几个相近主题，且包含违法信息，则违法信息有可能在相关主题中大范围变种并快速传播。 | 人员访谈&测评验证 | 不适用 | 该业务无跟帖、转发功能。 |
| 1.3信息载体 | 1.3.1信息呈现方式 | 信息呈现的方式包括文本、图片、音视频、二维码等文件，考虑到目前图片、音频、视频等文件及流媒体的内容识别技术尚不成熟，此类信息存在传播违法信息的安全风险。 | 人员访谈&测评验证 | 不适用 | 该业务仅包含文本信息。 |
| 1.3.2语言类型 | 语言类型主要包括中文、英文及其他小语种等，考虑到目前小语种语言的内容识别技术尚不成熟，存在传播违法信息的安全风险。 | 人员访谈&测评验证 | 不适用 | 该业务不包含小语种信息。 |
| 1.4信息生成 | 1.4.1信息源 | 如果无法确保业务系统中生成的信息是来自经身份真实认证或鉴别的可信用户，例如信息是由被冒用或盗取的账号或渠道生成、发送，则大幅增加了违法有害信息处置难度。 | 人员访谈&文件审查 | 不适用 | 该业务不包含用户生成信息（UGC）。 |
| 1.4.2信息产生方式 | 如果业务系统中生成的信息不由业务运营企业控制，例如用户生成信息（UGC）、第三方合作者提供信息等，则信息来源不唯一，对违法信息进行处置的工作难度将大幅增长。 | 人员访谈&测评验证 | 不适用 | 该业务不包含第三方合作者提供的信息。 |
| 1.5信息传播 | 1.5.1信息传播方式 | 信息传播方式包括了点对点、点对多点（如公众平台）、多点对多点（如群组聊天）以及链式网状传播（如微博客）等，点对多点、多点对多点、链式网状传播等传播方式扩大了单位时间内信息的传播范围，存在传播违法信息的信息安全风险。 | 人员访谈&测评验证 | 不适用 | 该业务信息传播方式为点对点传播。 |
| 1.5.2通信媒介 | 通信媒介主要考虑网络类型、支持平台类型等，若业务具备跨平台、跨网络（如融合类业务中涉及电信网和互联网之间的传输切换）的信息流动能力，将导致信息传播链条复杂、多维，提高信息传播速度，增加违法信息快速识别和处置的工作难度。 | 人员访谈&测评验证 | 不适用 | 该业务信息内容不可分享至其他平台及跨网络传播。 |
| 1.5.3信息传递实时性 | 信息传递实时性关注信息接收端用户能否实时读取信息，实时通信提高了信息读取概率，提高了信息传播速度，存在传播违法信息的信息安全风险。 | 人员访谈&测评验证 | 不适用 | 该业务不向用户推送信息。 |
| 1.6信息接收 | 1.6.1信息收取方式 | 信息接收环节主要关注信息收取方式等。信息收取方式主要包括信息主动推送、用户主动获取等方式，信息的主动推送提高了信息读取概率，间接提高了信息传播速度，扩大了信息传播范围，存在传播违法信息的信息安全风险。 | 人员访谈&测评验证 | 不适用 | 该业务信息收取方式为用户主动获取。 |
| 1.7信息留存 | 1.7.1公共信息内容留存 | 信息留存关注的是业务系统中传输的公共信息内容和用户使用业务行为的日志记录，如果企业未按相关法律法规要求保留日志信息，将会直接影响企业配合完成事后溯源、取证工作的开展。 | 人员访谈&演示查验 | 不适用 | 该业务不涉及信息发布 |
| 2.业务平台安全 | 2.1设备位置分布 | 2.1.1服务器、机房、节点的地理位置 | 设备位置分布是指承载业务的服务器、机房或节点的地理位置分布。如果业务的服务器、机房或节点在境内外均有分布，且境内外有数据传输，则可能存在因数据跨境流动引发的国家重要数据、个人隐私信息泄露的信息安全风险。 | 人员访谈 | 安全风险较低 | 该业务无境内外数据交互 |
| 2.2资源调度方式 | 2.2.1计算资源/云服务 | 资源调度方式是指业务系统的计算资源、存储资源、带宽资源、IP地址及域名资源的调度方式。如果计算、存储、带宽资源采用了云化或虚拟化，则可能增加企业违法信息处置工作的难度。 | 人员访谈 | 安全风险较低 | 该业务未采用云计算业务或采购第三方云服务。 |
| 2.2.2存储资源/内容分发 | 若业务IP地址及域名采取动态分配方式，则可能增加企业违法信息处置工作的难度。 | 人员访谈 | 安全风险较低 | 该业务未采用内容分发网络技术。 |
| 2.3业务合作 | 2.3.1合作方式的合规性 | 业务合作是指业务运营企业与其他企业开展任意形式的合作。企业需要对任何一种合作方式进行合规性评估（是否符合现行行业管理相关规定）。企业需要评估合作企业的信息安全管理工作及保障措施能否满足相关法律法规要求，能否保障业务的信息安全。 | 人员访谈&文件审查 | 不适用 | 该业务不涉及合作业务。 |
| 2.4开放接口 | 2.4.1是否提供第三方API接口 | 开放接口是指业务系统为第三方提供的标准API接口。第三方调用开放API接口的过程中，如果与业务系统之间产生了数据交互，可能增加业务系统发布、传输、存储违法信息的信息安全风险；如果业务系统开放的API接口未做好违法有害信息监测处置、权限管理、安全审计等，可能带来违法有害信息传播、直接影响业务系统自身安全、非法调用API接口（如实施通讯信息诈骗）等安全风险。 | 人员访谈&文件审查 | 不适用 | 该业务不对第三方提供API接口。 |
| 3.业务运行安全 | 3.1业务逻辑安全 | 3.1.1业务规则、业务流程等存在安全漏洞可能带来的通讯信息诈骗安全风险的大小 | 业务逻辑安全的关注点主要集中在业务规则的合规性、业务流程的合理性及配套的技术保障措施的完善性等。如以一卡多号、短信营业厅、网上营业厅等为代表的电信业务，如果存在未实施二次确认机制、 必要的用户身份验证环节缺失、 短信验证码下发环节用户安全提醒不完善、业务登录提示不足、身份校验技术手段不完备等安全漏洞， 则有可能被诈骗分子利用设计各种诈骗场景，冒充用户实施诈骗。 | 人员访谈&文件审查 | 安全风险较高 | 涉及短信订购业务 |
| 3.2通讯信息管理安全 | 3.2.1从业务功能看，业务涉及的码号资源、电信线路被用于通讯信息诈骗的可能性大小 | ①电信资源主要包括移动电话业务、 一卡多号、“400”、“一号通”、“商务总机”等电信业务涉及的电信网码号资源、电信线路等。如果存在用户实名登记信息不真实不准确、用户资质审核不严格、代理渠道管理薄弱、码号申请数量管理和台账管理未落实、业务落地号码管理不规范、违规为个人用户办理语音专线、“400”、“商务总机”业务、 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不严格、 业务使用复核监测不足、异常行为用户监测管控不力等安全漏洞，则相关码号资源、电信线路有可能被诈骗分子利用实施通讯信息诈骗。 | 人员访谈&文件审查 | 不适用 | 不涉及语音业务 |
| 3.2.2业务被用于违规传送号码的可能性大小 | ②在号码传送过程中，如果存在语音专线未实施主叫鉴权、语音专线呼叫转移管理不严、主叫隐藏功能未关闭、不良呼叫号码监测处置能力不足等安全漏洞，则相关漏洞有可能被诈骗分子利用，以修改主叫号码、设置主叫号码为空号或禁显、违规外呼、私自改变业务使用用途等方式实施通讯信息诈骗。 | 人员访谈&文件审查 | 不适用 | 不涉及语音 |
| 3.2.3从业务功能看，业务被用户传播通讯信息诈骗违法信息的可能性大小 | ③在信息传播方面，如果即时通信、搜索引擎、手机应用软件商城、电商平台、社交平台、网站等互联网业务的违法信息识别处置能力不足，则相关业务有可能成为不法分子贩卖个人信息和诈骗实施软件及工具（如改号软件、非法电话卡、非法银行卡、身份证识别设备破解软件、虚拟交易软件、“伪基站”等）的渠道途径。 | 人员访谈&文件审查 | 不适用 | 不涉及互联网业务 |
| 4.数据安全 | 数据采集 | 从业务角度查看数据采集过程存在被欺诈、诱骗、强迫个人提供信息的可能性大小。 | 数据采集环节指数据获取和创建过程，数据采集环节主要从用户个人利益角度出发，如果企业在收集用户个人信息环节，未告知用户被收集的数据类型、使用目的，未经用户同意收集用户个人信息，或存在欺诈、诱骗、强迫个人提供信息，非法渠道获取个人信息或收集法律法规明令禁止收集的个人信息，超范围收集用户个人信息等，则涉及侵害用户合法权益风险。 | 人员访谈&文件审查 | 不适用 | 不涉及用户个人信息 |
| 数据存储 | 从业务角度查看数据存储过程存在被窃取、篡改或销毁的可能性大小。 | 数据存储环节指将数据持久保存在系统中，数据存储环节主要考虑数据存储环境安全及数据自身安全，如系统安全配置不当，未及时安装更新或补丁，使得操作系统存在漏洞，或移动存储介质管理不善、移动办公设备（包括笔记本电脑、智能手机、平板电脑等）的数据存储保护不善、对数据的访问权限管理不到位，未按照数据的重要性、敏感性等因素进行相应的账号管理和权限分配管理、对于重要或敏感数据未进行加密存储、重要数据未进行备份、企业内部人员管理不善、安全意识淡薄等，可能受到网络攻击、病毒木马等恶意代码攻击、黑客入侵、越权、社会工程、自然灾害等，导致存储数据被窃取、篡改或销毁风险。 | 人员访谈&文件审查 | 不适用 | 不涉及用户个人数据 |
| 数据传输 | 从业务角度查看数据传输过程存在被拦截泄露、窃取或篡改，数据传输中断的可能性大小。 | 数据传输环节指数据在企业内外部流转过程，数据传输环节主要从数据传输链路安全方面出发，如数据通过互联网传输或数据传输链路安全保护不善，未采用加密传输技术活协议，未设置数据传输冗余链路等，则可能导致传输数据被拦截泄露、窃取或篡改，数据传输中断等风险。 | 人员访谈&文件审查 | 安全风险较低 | 电信内部传输数据，符合安全要求。 |
| 数据加工 | 从业务角度看查看数据加工过程存在第三方企业违规访问、处理企业数据的安全隐患、用户个法权益受损或用户隐私泄露、国家重要数据泄露、引发社会恐慌或混乱的安全隐患的可能性大小。 | 数据加工指对采集的原始数据进行计算分析，加工生成新的数据，数据加工环节主要从维护企业、个人、国家利益角度出发进行分析。①如企业采用公有云服务或其他第三方平台存储、处理数据后，第三方企业拥有企业数据的实际控制权，存在第三方企业违规访问、处理企业数据的安全隐患。②如企业未按照数据采集环节对用户的承诺，超范围使用用户数据进行挖掘分析，或在进行数据分析和挖掘的过程中，对个人敏感信息判定不准确、未进行数据脱敏或数据脱敏不彻底，可能导致用户个法权益受损或用户隐私泄露。③如企业进行数据挖掘分析后形成的成果直接或者间接反映了国家军事、政治、经济、社会等现状或重要情报，如果企业未配套相应的安全保护措施，将导致国家重要数据泄露。④企业进行数据挖掘分析后形成的成果数据与公共事务相关，如地理、水文、气象、大气环境等，企业未经相关部门同意，擅自向公众发布这些成果数据，存在引发社会恐慌或混乱的安全隐患。 | 人员访谈&文件审查 | 不适用 | 不涉及数据加工 |
| 数据转移 | 从业务角度查看数据转移过程存在数据转移后被窃取、篡改或销毁，以及转移数据超范围使用处理、违规二次转移，用户隐私及国家重要数据泄露的可能性大小。 | 数据转移指将原始数据、加工过的数据等不同形式的数据分发给外部实体，数据转移环节主要从维护企业、个人和国家利益角度出发。①如企业将数据提供给第三方前，未对第三方的数据安全防护能力进行评估，未明确告知第三方数据使用权限，或未对第三方进行必要的安全监督管理，可能导致数据转移后被窃取、篡改或销毁，以及转移数据超范围使用处理、违规二次转移等安全风险；②如企业将数据提供给第三方前，未对将要转移的数据的重要性、敏感性进行评估，未明确告知第三方数据使用权限，未对第三方进行必要的安全监督管理，可能导致用户隐私及国家重要数据的泄露。 | 人员访谈&文件审查 | 不适用 | 不涉及将数据转给第三方 |
| 数据删除 | 从业务角度查看数据删除过程存在侵害用户合法权益、剩余信息泄露的可能性大小。 | 数据删除指删除组织的数据及其副本。数据删除环节主要从用户个人利益角度出发。①当用户终止使用服务后，符合法律法规留存基础上，如企业未按用户要求删除用户数据的，则涉及侵害用户合法权益风险。②如数据删除手段不当，可能导致剩余信息泄露风险。 | 人员访谈&文件审查 | 不适用 | 不涉及用户个人信息 |
| 个人信息安全 | 从业务角度查看个人信息是否被滥用、泄露、篡改、损毁的可能性大小 | 个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于用户姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。 个人信息安全风险是指，企业由于管理措施、技术手段等安全保障能力的不足或受到自然灾害、基础设施故障等环境危害，在个人信息采集、存储、管理、传输、加工、转移、删除等处理环节，造成个人信息泄露、损毁、篡改等安全事件，对个人隐私以及个人信息主体权益造成安全隐患的风险。个人信息安全风险的具体表现形式包括但不限于：个人信息滥用、个人信息泄露、个人信息篡改、个人信息损毁、个人信息主体权益保护不当、系统故障、网络流量监听、网络攻击、恶意代码、物理攻击、管理不到位、事件应对能力不足、人员安全失控和物理环境安全等。 | 人员访谈&文件审查 | 不适用 | 不涉及用户个人信息 |

### 高风险识别分析说明

综合以上分析，“短信营业厅”业务在以下几个方面存在较高的信息安全风险：

1. 用户规模：目前，河南省内“短信营业厅”用户超过1000万，规模较大，信息安全风险较高。
2. 业务逻辑安全：采用短信实现业务订购，信息安全风险较高。

### 配套安全管理措施

#### 整体保障能力分析矩阵表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **评估事项** | **评估模块** | **评估指标** | **评估方法** | **评估意见** | **研判依据** |
| 业务应用安全保障基线 | 用户管理 | 1.普通账号身份验证 | 人员访谈&测评验证 | 不适用 | 该业务使用时不需要用户注册、登录。 |
| 2.公众账号身份验证 | 人员访谈&测评验证 | 不适用 | 该业务无公众账号功能。 |
| 3.注册信息审核 | 人员访谈&测评验证 | 不适用 | 用户不可线上自主注册。 |
| 4.用户真实身份鉴别 | 人员访谈&测评验证 | 不适用 | 该业务使用时不需要用户注册、登录。 |
| 5.用户账号分级管理 | 人员访谈&测评验证&演示查验 | 不适用 | 该业务不包含用户生成信息（UGC）。 |
| 6.用户投诉管理 | 人员访谈&文件审查&测评验证 | 不适用 | 该业务无信息发布功能。 |
| 信息内容管理 | 7.信息内容管理制度及技术手段 | 人员访谈&演示查验 | 不适用 | 该业务无信息发布功能。 |
| 信息搜索功能管理 | 8.信息搜索功能管理 | 人员访谈&测评验证 | 不适用 | 该业务无信息搜索功能。 |
| 信息发布递送功能管理 | 9.信息发布递送功能管理 | 人员访谈 | 不适用 | 该业务用户不可公开发布信息。 |
| 信息社区平台功能管理 | 10.信息社区平台功能管理 | 人员访谈&文件审查 | 不适用 | 该业务无转发、分享功能。 |
| 信息即时交互功能管理 | 11.群组功能管理 | 人员访谈&测评验证 | 不适用 | 该业务无群组功能。 |
| 12.匿名发布功能管理 | 人员访谈&演示查验 | 不适用 | 该业务无匿名发布功能。 |
| 13.转发功能管理 | 人员访谈 | 不适用 | 该业务无转发、分享功能。 |
| 14.信息销毁功能管理 | 人员访谈&演示查验 | 不适用 | 该业务无信息销毁功能。 |
| 安全规则张贴与主动提示 | 15.安全规则张贴与主动提示 | 人员访谈&测评验证 | 不适用 | 该业务使用时不需要用户注册、登录。 |
| 溯源管理 | 16.用户身份信息变更留存 | 人员访谈&演示查验 | 不适用 | 用户不可变更身份信息。 |
| 17.日志留存管理 | 演示查验 | 满足 | 留存相关日志，符合要求； |
| 信息联动管理 | 18.信息联动管理 | 人员访谈&演示查验 | 不适用 | 该业务无转发、分享功能。 |
| 应急处置 | 19.应急处置管理机制及技术手段 | 人员访谈&文件审查 | 满足 | 满足应急处置管理制度 |
| 业务平台安全保障基线 | 业务平台部署 | 20.平台设施信息备案 | 人员访谈&文件审查 | 满足 | 满足信息备案要求 |
| 21.设施境内外分布 | 人员访谈 | 不适用 | 该业务无境内外数据交互。 |
| 资源调度 | 22.资源实时监控 | 人员访谈&演示查验 | 满足 | 满足资源监控要求 |
| 23.违法信息监测处置 | 人员访谈&演示查验 | 不适用 | 不涉及信息发布功能 |
| 24.系统日志留存 | 人员访谈&演示查验 | 满足 | 满足日志留存要求 |
| 用户接入要求 | 25.合作企业的安全能力 | 人员访谈&文件审查 | 不适用 | 该业务无合作方。 |
| 26.资质审核 | 人员访谈&文件审查 | 不适用 | 该业务无用户接入。 |
| 27.用户信息备案 | 人员访谈&文件审查 | 不适用 | 该业务无用户接入。 |
| 28.应用分发平台功能管理 | 人员访谈&文件审查 | 不适用 | 该业务无应用分发平台功能。 |
| 29.开放接口要求 | 人员访谈&文件审查 | 不适用 | 该业务无第三方API接口。 |
| 业务运行安全保障基线 | 重点电信业务管理 | 30.管理制度建设 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 31.申请主体资格管控 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 32.办理渠道管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 33.用户实名信息核验登记留存 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 34.码号申请数量管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 35.台账管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 36.业务落地号码管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 37.业务外呼管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 38.合同和协议责任约束 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 39.重点电信业务使用复核监测 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 40.移动电话业务使用管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 41.业务退出管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 42.定期检查 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 43.号码核查与企业内部考核问责 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 44.工作规程管理 | 人员访谈&文件审查 | 不适用 | 该业务不涉及语音呼叫、话务转接功能 |
| 45.重点电信业务信息化管理手段 | 人员访谈&文件审查 | 满足 | 存在相关手段 |
| 46.用户安全提醒技术手段 | 人员访谈&文件审查 | 不适用 | 不涉及此类功能 |
| 业务逻辑安全管理 | 47.业务办理管理 | 人员访谈&文件审查 | 不满足 | 短信中未添加签名 |
| 48.业务登录管理 | 人员访谈&文件审查 | 不适用 | 不涉及登陆 |
| 49.业务使用管理 | 人员访谈&文件审查 | 不适用 | 不涉及此类功能 |
| 号码传送规范管理 | 50.语音专线主叫鉴权与呼叫转移管控 | 人员访谈&文件审查 | 不适用 | 不涉及语音呼叫等业务 |
| 51.外呼白名单管理 | 人员访谈&文件审查 | 不适用 | 不涉及外呼业务 |
| 52.号码传送管理 | 人员访谈&文件审查 | 不适用 | 不涉及号码呼叫 |
| 53.不良呼叫号码监测处置系统 | 人员访谈&文件审查 | 不适用 | 不涉及号码呼叫 |
| 数据安全保障基线 | 组织机构和工作机制 | 54.组织机构和工作机制 | 人员访谈&文件审查 | 满足 | 建立相关制度及工作流程 |
| 数据分级分类 | 55.数据分级分类 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 数据采集 | 56.数据采集 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 数据存储 | 57.通用性数据存储保护 | 人员访谈&文件审查 | 不满足 | 配置短信模板时，无相关审计机制，工作人员可直接独立完成短信配置。 |
| 58.数据存储中的国家重要数据保护 | 演示查验&文件审查 | 不适用 | 不涉及重要数据 |
| 数据传输 | 59.通用性数据传输保护 | 演示查验&文件审查 | 满足 | 电信内部传输数据，符合安全要求。 |
| 60.数据传输中的国家重要数据保护 | 演示查验&文件审查 | 不适用 | 不涉及重要数据 |
| 数据加工 | 61.通用性数据加工保护 | 人员访谈&文件审查 | 不适用 | 不涉及数据加工 |
| 62.数据加工中的国家重要数据保护 | 人员访谈&文件审查 | 不适用 | 不涉及数据加工 |
| 数据转移 | 63.通用性数据转移保护 | 人员访谈&文件审查 | 不适用 | 不涉及数据第三方转移 |
| 64.数据转移中的国家重要数据保护 | 人员访谈&文件审查 | 不适用 | 不涉及数据第三方转移 |
| 数据删除 | 65.通用性数据删除保护 | 演示查验&文件审查 | 不适用 | 不涉及个人数据信息 |
| 66.数据删除中的国家重要数据保护 | 演示查验&文件审查 | 不适用 | 不涉及国家重要信息 |
| 个人信息的收集 | 67.收集个人信息的合法性要求 | 人员访谈&文件审查 | 不适用 | 不涉及用户个人信息 |
| 68.收集个人信息的最小化要求 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 69.收集个人信息时的授权同意 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 70.征得授权同意的例外 | 人员访谈&文件审查 | 不适用 | 不涉及国家信息 |
| 71.收集个人敏感信息时的明示同意 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 72.隐私政策的内容和发布 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 个人信息的保存 | 73.个人信息保存时间最小化 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 74.去标识化处理 | 演示查验 | 不适用 | 不涉及个人信息 |
| 75.个人敏感信息的存储 | 演示查验 | 不适用 | 不涉及个人信息 |
| 76.企业停止运营 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 个人信息的使用 | 77.个人信息访问控制措施 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 78.个人信息的展示限制 | 演示查验 | 不适用 | 不涉及个人信息 |
| 79.个人信息的使用限制 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 个人信息的委托处理、共享、转让、公开披露 | 80.委托处理 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 81.个人信息共享、转让 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 82.收购、兼并、重组时的个人信息转让 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 83.个人信息公开披露 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 84.共享、转让、公开披露个人信息时事先征得授权同意的例外 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 用户权益保障要求 | 85.个人信息访问 | 演示查验 | 不适用 | 不涉及个人信息 |
| 86.个人信息更正 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 87.个人信息删除 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 88.用户撤回同意 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 89.用户注销账户 | 演示查验 | 不适用 | 不涉及个人信息 |
| 90.用户获取个人信息副本 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 管理制度保障要求 | 91.组织机构 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 92.安全审计 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 93.人员管理与培训 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息 |
| 94.应急处置 | 人员访谈&文件审查 | 不适用 | 不涉及个人信息数据 |
| 95.申诉管理 | 人员访谈&文件审查 | 不适用 | 不涉及此类功能 |
| 96.请求响应 | 人员访谈&文件审查 | 满足 | 符合相关要求 |
| 97.安全风险评估 | 人员访谈&文件审查 | 满足 | 符合相关要求，开展风险评估 |
| 技术手段保障要求 | 98.技术手段保障要求 | 演示查验 | 不适用 | 不涉及个人信息 |

#### 日常安全管理介绍

1.总体管理情况

河南电信成立信息安全领导小组，负责研究重大事件，落实方针政策和制定总体策略等。职责主要包括：根据国家和行业相关信息安全的政策、法律和法规，批准公司信息安全总体策略规划、管理规范和技术标准。

河南电信成立了专门的信息安全管理部门：“网络与信息安全管理部”，配备专职人员5人。

根据工信部有关规定，将评估过程设置为系统上线前的必要环节，并列入OA系统，同时加强全省范围的信息安全业务培训。

河南电信制定了以下网络与信息安全方面的管理制度：

《中国电信河南公司新技术新业务信息安全评估管理办法（试行）》

《中国电信河南公司用户个人信息安全管理办法（暂行）》

《中国电信河南公司新技术新业务信息安全评估管理办法（试行）》

《河南电信通信项目中网络安全“三同步”的规定（试行）》

《河南省电信公司移动上网日志留存系统查询管理办法》

《河南电信通信网络应急保障预案专项预案-数据专业》

《河南电信增值业务平台安全管理办法》

《中国电信河南公司IDC/ISP信息安全管理系统运行维护管理办法》

《中国电信河南公司BSS工号及权限管理办法》

《中国电信河南公司网络设备及系统平台账号口令管理办法》

《河南电信业务平台应用软件安全技术规范》

《河南电信业务平台分等级安全基线规范》

《信息安全应急演练实施方案》

《中国电信河南公司IDC/ISP信息安全管理系统管理办法（试行）》

《中国电信河南公司移动上网日志留存管理办法（试行）》

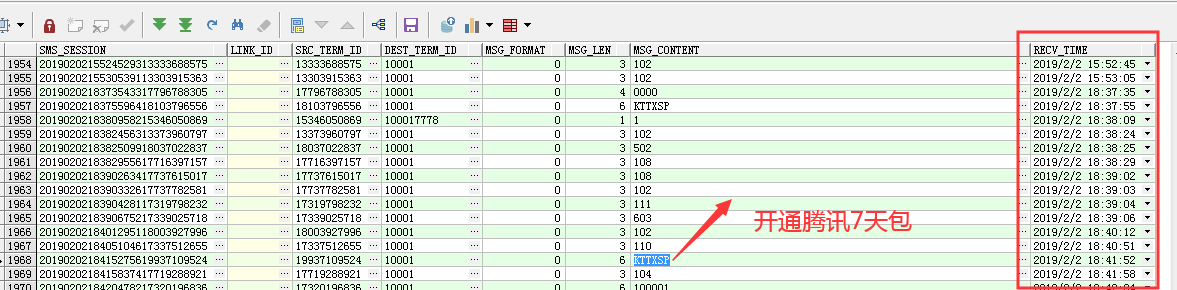
《中国电信河南公司互联网安全事件处理要求》

2.“短信营业厅”业务管理情况

“短信营业厅”业务功能包括相关管理制度，该业务主要由个人业务和渠道业务。个人业务包括订单受理类业务、服务请求类业务、积分服务、密码服务、缴费服务、投诉建议、主动营销和主动服务；渠道业务包括代销商的店员积分服务和空中充值服务。其中，短信综合渠道面向个人客户和销售渠道代销商服务，交互方式有菜单交互方式、编码点播方式。

3.日常管理保障措施

1. 日志管理

 “短信营业厅”后台日志记录规则、时限满足法律法规要求，截图如下所示：

用户行为日志

1. 短信下发

“短信营业厅”短信下发时采用了二次确认等机制，截图如下所示：



#### 应急管理措施介绍

“短信营业厅”所使用的硬件设备都部署于电信机房，机房提供7\*24小时全天监控，保证其正常运转。开发公司安排专人负责应急响应系统出现的问题及故障。

# 安全评估结论意见

## 匹配性分析

“短信营业厅”业务在用户规模、业务逻辑安全存在一定的安全风险，电信公司建立了一系列保障措施和技术手段，具备一定的安全风险管控能力，但还存在以下保障薄弱环节与风险不完全匹配：

1. 业务逻辑安全管理

|  |  |
| --- | --- |
| **保障薄弱环节** | 短信下发未添加签名 |
| **情况说明** | 1. 该业务对在短信下发时，采用了二次确认，但是未添加签名； |
| **可能引发的风险** | 伪造署名假冒企业进行短信下发。 |

1. 数据存储

|  |  |
| --- | --- |
| **保障薄弱环节** | 数据操作无审计 |
| **情况说明** | 在管理员配置短信模板时候，缺少审计环节； |
| **可能引发的风险** | 数据存储存在风险 |

## 企业整改建议及落实情况

### 整改建议

针对“短信营业厅”业务中存在的信息安全风险，建议企业尽快从以下方面加强信息安全保障能力建设：

1. 完善业务逻辑安全管理，添加短信签名；
2. 加强数据存储安全，对短信模板配置前，加入审计；

### 整改落实情况

### 安全评估结论

综上，针对“短信营业厅”业务安全风险，河南电信在业务运行、数据安全等方面总体保障措施较好，但在业务逻辑安全管理、数据存储方面存在薄弱环节，无法很好的匹配业务中的风险，建议企业进行整改完善。

## 同类业务的监管建议

针对“短信营业厅”同类业务，建议在业务逻辑安全管理、数据存储方面加强管理和技术防护，确保相关保障措施与网络信息安全风险匹配，业务整体安全风险可控。

## 评估结果签字确认

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **姓名** | **部门** | **工作岗位** | **联系电话** | **签字** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 审核人：  复核人： | | | | |