# 六、业务安全风险评估

## **1、业务应用安全风险**

（1）用户

用户主要关注用户规模、用户相关性、用户真实身份鉴别等。如果业务涉及用户规模庞大、用户间关系紧密、用户身份信息无法追溯等，则可能出现安全事件影响范围扩大、用户个人隐私泄露、账户信息被泄露、仿冒、盗取等风险。

（2）业务逻辑

业务逻辑主要关注业务流程及业务逻辑的合理性。如果业务流程复杂，存在认证绕过的可能性，可被诈骗分子利用设计诈骗场景并实施诈骗，造成用户个人隐私泄露、业务滥用等风险。

（3）信息生成

信息发布主要关注信息来源和信息产生方式。如果无法确保业务系统中产生的信息是来自经身份真实认证或鉴别的用户，或业务具有信息发布递送功能，则可能涉及违法有害信息生成发布等风险。

（4）信息传播

信息传播主要关注信息传播方式、传播媒介、传播实时性等。如果业务涉及点对多点、多点对多点、链式网状传播等方式，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）的信息传播能力，或者用户端能够实时读取信息，则可能涉及违法有害信息传播等风险。

## **2、业务数据安全风险**

（1）数据基本属性

数据基本属性主要关注数据级别、数据种类、数据规模等。如果业务包含重要数据、核心数据，或者生物识别信息等个人敏感信息，或数据规模达到一定程度（如包含100万人以上个人信息等），则可能涉及数据被泄露、篡改后影响国家安全、公共利益的风险。

（2）处理方式

处理方式主要关注数据采集、数据存储、数据流转等环节。

数据采集主要关注数据采集方式、数据来源、采集内容等。如果企业通过网络爬取数据，或者采购合作方数据，可能涉及采集方式不合规、数据真实性不足等风险。如果企业向用户采集数据时隐私政策或用户协议不规范，或未取得用户明示同意，则可能涉及超范围采集、非授权采集等风险。

数据存储主要关注存储方式。如果企业存储数据时采用合作方数据中心、分布式数据库等方式进行存储，则可能涉及数据被窃取、篡改、丢失或损毁等风险。

数据使用主要关注使用方式、使用目的等。如果企业超范围使用用户数据且未获取得用户明示同意（如利用数据构建用户画像、进行精准化推送等），则可能涉及个人信息泄露、数据滥用等风险。

数据传输主要关注数据跨境。如果企业在传输数据的过程中出现数据跨境流动或数据转移至境外的情况，则可能涉及数据跨境泄露等风险。

## **3、业务平台安全风险**

（1）软件系统

软件系统主要关注业务系统涉及软件的可靠性和健壮性。如果软件系统存在代码漏洞、代码逻辑错误、系统设计缺陷、兼容性差等，则可能涉及丢失关键数据、遭受外部网络攻击等风险。

（2）智能算法

智能算法主要关注业务涉及的机器学习等人工智能算法，以及算法功能实现方式、应用场景等。如果业务平台采用深度神经网络、自然语言处理(NLP)、大模型等智能算法，提供网络通信、内容分发、数据中心、互联网信息服务等，则可能涉及算法偏见歧视、训练数据泄露、滥用和恶意使用等风险。

（3）网络协议

网络协议主要关注业务系统采用的网络协议加密性、安全性等方面。如果采用HTTP等非加密网络协议，或者网络协议设计存在缺陷、安全漏洞等，则可能涉及数据泄露、易被攻击等风险。

## **4.业务基础设施安全风险**

（1）资源调度

资源调度主要关注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，或者IP地址及域名采取动态分配方式，则可能增加处理违法有害信息的难度。

（2）硬件设备

硬件设备主要关注业务系统的网络设备、服务器等，以及设备的安全管理方式。如果硬件设备存在软硬件漏洞、系统后门等，则可能导致设备被攻击入侵、数据被窃取或破坏等风险。

（3）物理环境

物理环境主要关注业务系统的机房基础设施。如果物理环境遭受自然环境灾害（地震、洪水）或物理设施故障（如断电、温湿度失调等），机房出入人员控制失效等，则可能引发业务中断、服务器宕机、设备损毁或失窃等风险。

## **5、业务合作安全风险**

（1）合作模式

合作模式主要关注合作事项、合作方数量等。如果业务涉及对合作方提供数据、共享数据、委托处理数据，或者委托合作方进行软件开发、数据建模分析、系统运维等情况，可能涉及数据泄露、数据滥用、网络攻击、系统后门等风险。如果业务涉及两个及以上的合作方，则可能加大数据泄露、数据滥用等风险。

（2）合作方资质背景

合作方资质背景主要关注合作方安全违规情况。如果合作方发生过数据泄露（丢失）、数据被篡改、数据被损毁等安全事件，或者合作方因网络安全、数据安全、内容安全等问题被列入电信互联网业务经营不良名单或失信名单，则可能增加业务合作过程中发生类似安全事件的风险。