(ERP 系统)

数据安全风险评估报告

评估单位（盖章)：

报告时间：2025 年 6 月 10 日

■ 文档说明

文档名称	ERP 系统数据安全风险评估报告		
保密级别	商业秘密	文档版本号	V1.0
制作人	安全评估团队	制作日期	2025-6-10
复审人	信息科技部	复审日期	
扩散范围	限“项目组”内		
分发控制	创建、修改、读取	项目组：读取	

■ 适用范围

本次 ERP 系统数据安全风险评估是由 XX 公司（以下简称“XX”）授权，由数可安团队（以下简称“数可安”）对 ERP 系统进行的数据安全风险评估，并根据评估结果提交技术报告，技术报告用于描述被测试业务系统的风险描述和加固建议，仅限于“项目组”内部人员传阅。

报告结论的有效性建立在被测试单位提供相关信息的真实性基础之上，报告中描述的漏洞详情与修复建议仅适用于测试周期内信息系统的安全状况，当信息系统发生涉及到的系统构成组件（或子系统）变更时本报告不再适用。

■ 版本变更记录

修改日期	版本	说明	修改人
2025-03-25	V1.0	正式版本	姚琦

■ 版权声明

数据安全风险评估报告（样例模板）

一、引言

1.1 评估目的

为落实《数据安全法》《个人信息保护法》等法律法规要求或安全监管需要，对数据处理者的数据安全管理、数据处理活动、数据安全技术和个人信息保护情况等进行安全评估，发现存在的安全问题和风险隐患，督促数据处理者健全安全制度、改进安全措施、堵塞安全漏洞，进一步提高数据安全和个人信息保护能力。

数据安全风险评估的目标，包括但不限于：

a）摸清重要数据种类、规模、分布等基本情况；

b）摸清数据处理活动的情况；

c）发现可能影响国家安全、公共利益或者个人、组织合法权益的数据安全问题和风险；

d）发现共享、交易、委托处理、向境外提供重要数据等处理活动的数据安全问题和风险；

e）促进完善数据安全保护措施，提升数据安全保护能力。

1.2 评估依据

评估依据包括但不限于：

[1] GB/T 20984-2022 信息安全技术 信息安全风险评估办法

[2] GB/T 35273-2020 信息安全技术 个人信息安全规范

[3] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

[4] GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

[5] GB/T 41391-2022 信息安全技术 移动互联网应用程序（APP）手机个人信息基本要求

[6] GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求

[7] JR/T 0223-2021 金融安全技术 数据生命周期安全规范

[8] YD/T 3801-2020 电信网和互联网数据安全风险评估实施方法

[9] 中华人民共和国个人信息保护法（2021 年 8 月 20 日中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议通过）

[10] 中华人民共和国个人信息保护法（2021 年 8 月 20 日中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议通过）

[11] 中华人民共和国网络安全法（2016 年 11 月 7 日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过）

[12] 《互联网信息服务深度合成管理规定》(2022 年 11 月 3 日国家互联网信息办公室、工业和信息化部、公安部联合印发)

[13] 《互联网信息服务算法推荐管理规定》(2022 年 11 月 16 日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合印发)

[14] 《常见类型移动互联网应用程序必要个人信息范围规定》(2021 年 3 月 12 日国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合印发)

[15] 《App 违法违规收集使用个人信息认定方法》(2019 年 11 月 28 日国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合印发)

1.3 评估范围

- **数据范围**：涵盖[系统/项目名称]涉及的业务数据、应用开发数据、用户数据等全量数据资产。
- **生命周期阶段**：包括数据采集、存储、传输、使用、共享、销毁等环节。
- **评估对象**：数据资产、数据处理活动、技术架构、管理制度等。

本次评估工作采取“全面摸排、重点评估”原则，针对“数据安全管理”和“数据安全技术”以宏观视觉全面摸排的方式来评估企业数据安全管理和技术现状；针对“数据处理活动”、“个人信息保护”则聚焦于 ERP 系统，精细、重点的评估该业务处理过程中数据和个人信息安全现状。

评估对象			
编号	评估工作项	目标范围	详情
1	数据安全管理	企业整体	/

2	数据安全技术	企业整体	/	
3	数据处理活动	特定系统	系统名称	ERP
4	个人信息保护	特定系统	系统名称	ERP

1.4 评估人员情况

本次服务，评估方成员信息如下：

序号	姓名	人员资质	角色	联系电话	邮箱
1					
2					
3					

被评估方成员信息如下：

序号	姓名	角色	联系电话	邮箱
1				
2				
3				

1.5 评估时间安排情况

序号	评估项	评估项说明	评估时间
1	信息调研	针对企业的数据处理者情况、业务和信息系统情况、重要数据资产情况、数据处理活动情况以及安全措施情况展开调研。	
2	数据安全管理评估	针对企业的数据安全管理现状进行调研评估，包括：制度流程、组织机构、分类分级、人员管理、合作外包管理、安全威胁和应急管理、开发运维、云数据安全这 8 大维度，最终输出风险等级和风险详情。	
3	数据安全技术评估	针对企业的数据安全技术现状进行调研评估，包括：网络安全防护、身份鉴别与访问控制、监测预警、数据脱	

		敏、数据防泄漏、接口安全、备份恢复、安全审计、安全防护措施这 8 大维度，最终输出风险等级和风险详情。	
4	数据处理活动安全评估	针对某特定系统的数据处理活动现状进行调研评估，包括：数据收集、数据存储、数据传输、数据使用和加工、数据提供、数据公开、数据删除这 7 大维度，最终输出风险等级和风险详情。	
5	个人信息保护评估	针对某特定系统的个人信息保护现状进行调研评估，包括：基本原则、告知同意、保护义务、主体权利、投诉举报、个人信息处理、敏感个人信息保护、大型网络平台这 7 大维度，最终输出风险等级和风险详情。	
6	数据安全风险评估报告输出	通过人员访谈、安全核查和技术测试，输出最终数据安全风险评估报告。	

1.6 数据处理者基本情况

数据处理者基本情况	
单位名称	
组织机构代码	
办公地址	北京市-市辖区-东城区
法人信息	姓名:; 国籍：中国; 职务/职称：; 联系方式：;
人员规模	

经营范围	
单位组织机构架构图	-
数据安全负责人	姓名: 职务: 联系方式:
单位类型	民营企业
是否属于特定类型数据处理者（可多选）	非特定类型
单位所属行业	水利
上级主管部门	网安
业务运营地区，开展数据处理活动所在行政区划	中国
开展数据业务的依据文件、监管文件、指导性文件	
是否境外上市或计划赴境外上市	未有境外上市计划

1.7 业务系统基本情况

业务和信息系统情况	
业务和信息系统名称	ERP 系统
网络规模	
拓扑结构	
系统保护等级	二级
关键信息基础设施	否
业务功能描述	
业务服务对象	个人信息主体
*业务流程	
*业务用户规模	
业务覆盖地域	
业务涉及数据类型	个人信息
业务相关部门信息	
服务入口(移动端)	公众号： 其他：
服务入口 （C/S 端）	
业务系统部署位置	自建机房：北京
外部来源	接入的第三方产品：防火墙

1.8 数据资产情况

重要数据资产情况访谈结果				
序号	重要数据识别维度	是否涉及	被调研人员	备注
1	反映国家战略储备、应急动员能力，如战略物资产能、储备量属于重要数据；	否		
2	支撑关键基础设施运行或重点领域工业生产，如直接支撑关键基础设施所在行业、领域核心业务运行或重点领域工业生产的数据属于重要数据；	否		
3	反映关键信息基础设施网络安全保护情况，可被利用实施对关键信息基础设施的网络攻击，如反映关键信息基础设施网络安全方案、系统配置信息、核心软硬件设计信息、系统拓扑、应急预案等情况的数据属于重要数据；	否		
4	关系出口管制物项，如描述出口管制物项的设计原理、工艺流程、制作方法等的信息以及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告属于重要数据；	否		
5	可能被其他国家或组织利用发起对我国的军事打击，如满足一定精度要求的地理信息属于重要 数据；	否		
6	反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可能被恐怖分子、犯罪分子利用实施破坏，如反映重点安保单位、重要生产企业、国家重要资产（如铁路、输油管道）的施工图、内部结构、安防等情况的数据，以及未公开的专用公路、未公开的机场等的信息属于重要数据；	否		

7	可能被利用实施对关键设备、系统组件供应链的破坏，以发起高级持续性威胁等网络攻击，如重要客户清单、未公开的关键信息基础运营者采购产品和服务情况、未公开的重大漏洞属于重要数据；	否		
8	反映群体健康生理状况、族群特征、遗传信息等的基础数据，如人口普查资料、人类遗传资源信息、基因测序原始数据属于重要数据；	否		
9	国家自然资源、环境基础数据，如未公开的水情信息、水文观测数据、气象观测数据、环保监测数据属于重要数据；	否		
10	关系科技实力、影响国际竞争力，如描述与国防、国家安全相关的知识产权的数据属于重要数据；	否		
11	关系敏感物项生产交易以及重要装备配备、使用，可能被外国政府对我实施制裁，如重点企业金融交易数据、重要装备生产制造信息，以及国家重大工程施工过程中的重要装备配备、使用等生产活动信息属于重要数据；	否		
12	在向政府机关、军工企业及其他敏感重要机构提供服务过程中产生的不宜公开的信息，如军工企业较长一段时间内的用车信息；	否		
13	未公开的政务数据、工作秘密、情报数据和执法司法数据，如未公开的统计数据；	否		
14	其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。	否		
15	百万以上个人信息，十万以上敏感个人信息。	否		

《重要数据目录》

重要数据目录													
基本信息			分类		重要性描述			产生、使用与保护					备注
处理者	系统或应用	地区或部门	类	子类	影响	安全威胁	重要性时效	数量	来源	用途	共享情况	保护情况	

1.9 数据处理活动情况

数据处理活动调研表	
数据处理活动类型	数据处理情况
数据采集	
数据传输	
数据存储	
数据提供	
数据使用和加工	
数据公开	
数据删除	

略...

二、评估方法与过程

2.1 评估方法

- **静态梳理**：通过文档审阅、数据资产盘点，明确数据种类、数量、分布、权限及责任主体。
- **动态分析**：通过数据流梳理、接口测试、现场访谈，识别数据流转中的风险点。
- **风险分级**：参照 L1-L5 级数据分类标准，结合影响范围与程度确定风险等级（高/中/低）。

2.2 评估流程

1. **数据资产发现**：形成数据资产清单（含数据库表、文件、接口等）。
2. **数据分类分级**：制定分类分级清单，明确重要数据保护目录。
3. **风险识别**：从合规、技术、管理维度识别风险点。
4. **风险分析**：评估风险发生可能性及影响程度，确定风险等级。

三、数据资产梳理

3.1 数据资产清单

数据类型	存储方式	数据规模	敏感级别
[示例：用户信息]	关系型数据库	[示例：500 万条]	L3
[示例：项目文档]	文件服务器	[示例：1000 份]	L2

3.2 数据分类分级

- **分类标准**：按数据性质（如个人信息、业务数据、文档数据）划分。
- **分级标准**：

- L1：公开信息（如产品介绍）
- L2：内部信息（如部门报表）
- L3：敏感信息（如用户手机号）
- L4：重要信息（如核心业务数据）
- L5：极重要信息（如密钥、密码）

3.3 重要数据识别

重点保护数据包括：

- [示例：用户身份信息、交易记录、核心业务逻辑文档等]

四、风险识别与评估

4.1 风险分布概况

风险类别	高风险	中风险	低风险	合计
合规风险	[数量]	[数量]	[数量]	[数量]
技术风险	[数量]	[数量]	[数量]	[数量]
管理风险	[数量]	[数量]	[数量]	[数量]

4.2 典型风险点示例

风险 ID	风险描述	风险等级	影响环节
R-T-001	数据传输未采用 HTTPS，存在劫持泄露风险	高	数据传输
R-M-002	生产库存在大量临时表、备份表，管理粗放	高	数据存储
R-C-003	个人信息采集未提供隐私声明	中	数据采集

五、风险应对措施建议

5.1 技术措施

- **数据传输加密**：对所有外部接口启用 HTTPS，敏感字段采用 AES-256 加密。
- **访问控制**：实施最小权限原则，对数据库操作日志进行审计追踪。
- **数据脱敏**：导出/打印时对手机号、身份证号等敏感字段脱敏处理（如显示前 6 后 4 位）。

5.2 管理措施

- **数据生命周期管理**：建立临时表清理机制，定期归档备份数据，明确销毁流程。
- **制度建设**：制定《数据分类分级管理规范》《敏感数据外发审批流程》。
- **人员培训**：每季度开展数据安全意识培训，考核合格后方可接触敏感数据。

5.3 合规措施

- 完善隐私政策，明确告知用户数据收集用途及范围。
- 定期开展数据安全合规自查，形成《合规评估报告》。

六、结论与建议

6.1 总体结论

本次评估发现[系统/项目名称]存在高风险[数量]项、中风险[数量]项，整体风险等级为[高/中/低]，需优先处置高风险项。

6.2 优先级建议

1. 立即整改高风险项（如 HTTPS 部署、临时表清理）。

2.3 个月内完成中风险项整改（如隐私声明补充、外发审批流程建立）。

3.建立常态化风险监控机制，每半年开展一次全面评估。

七、附录

- 附录 1：数据资产清单（详细）
- 附录 2：风险点详细说明及整改计划表
- 附录 3：数据分类分级标准细则

注：本模板中“[ ]”部分为示例内容，实际使用时需根据具体项目补充完整。