【第 1 题】如下为某企业全量数据清单，请据此分析应选取哪些数据开展数据安全风险评估，并简述分析过程。

（本题 200 分，判分规则如下：1.“风险评估的最小范围”为固定答案，全部答对得 50 分，部分答对或者答错得 0 分；2.“选取过程分析”采用人工判分，根据答题情况判 0-150 分）

序号	数据类型	数据项名称	数据级别	数据量	数据日均增量	数据处理目的	对应数据处理活动	数据来源	是否涉及数据出境	数据承载系统
1	网络与数据安全保障类	高危安全漏洞	重要数据	0.041GB	/	运行维护	安全漏洞挖掘	人工填报	否	A 系统
2	网络规划建设类	网络安全产品参数	重要数据	0.1G	/	运行维护	设备参数配置	人工填报	否	B 系统
3	其他	用户数据	重要数据	432TB	/	运行维护	用户注册、登录等服务	设备采集	否	C 系统
4	网络运行维护类	信令监测数据	重要数据	10G	/	运行维护	信令监测	设备采集	否	E 系统
5	网络与数据安全保障	可能引发一般数据安全事件的监测预警	一般数据	0.002GB	/	运行维护	数据安全风险监测	设备采集	否	A 系统

	类	信息								

6	经济运行与业务发展类	商务合作数据	一般数据	50G	/	运行维护	外部商务合作	设备采集	否	D 系统
7	网络规划建设类	规划方案	一般数据	200 条	/	运行维护	系统建设	人工填报	否	B 系统
8	网络运行维护类	网络运行状态监测分析数据	一般数据	5G	/	运行维护	网络运行状态监测	设备采集	否	C 系统
9	其他	用户数据	一般数据	12G	/	运行维护	用户注册、登录等服务	设备采集	否	D 系统
10	物理安全保障类	安保人员清单	一般数据	0.1G	/	运行维护	安保人员部署管理	人工填报	否	F 系统

11	网络运行维护类	运维密码	重要数据	0.1G	/	运行维护	运维人员登录	设备采集	否	E 系统
12	网络运行维护类	运维日志	一般数据	1G	/	运行维护	运维日志记录	设备产生	否	E 系统
13	网络与数据安全保障类	审计记录	一般数据	3G	/	运行维护	日志审计	人工填报	否	G 系统
14	关键技术成果	可行性研究报告	一般数据	7G	/	运行维护	关键技术成果管理	人工填报	否	H 系统

请选手在下述表格中进行作答。

风险评估的最小范围	选取过程分析（简述研判依据、分析过程及选择结果）
☑第 1 项 高危安全漏洞 ☑第 2 项 网络安全产品参数 ☑第 3 项 用户数据 ☑第 4 项 信令监测数据 ☐第 5 项 可能引发一般数据安全事件的监测预警信息 ☑第 6 项 商务合作数据 ☐第 7 项 规划方案 ☐第 8 项 网络运行状态监测分析数据 ☐第 9 项 用户数据 ☑第 10 项 安保人员清单 ☑第 11 项 运维密码 ☐第 12 项 运维日志 ☐第 13 项 审计记录 ☑第 14 项 可行性研究报告	至少应选择第 1、2、3、4、6、10、11、14 项 数据。 【依据】数据安全风险评估范围应覆盖数据处理者 全部重要数据和核心数据，以及一定比例的一般数 据。一般数据以抽样方式选取，抽样应尽量保证评 估数据范围覆盖全部数据类别（ 二级子类），且数据载体避免重复。

【第 2 题】现对该企业商品评分数据处理活动开展正当必要性评估。通过人员访谈及资料查验获得以下信息：

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人

工判分，根据答题情况判 0-150 分）

1.在用户通过电商平台购买商品的过程中，可参考商品评分进行筛选。用户购买完成之后，可自愿通过对商品进行打分影响该商品的评分情况，为其他用户选购商品提供参考。

2.为了满足以上业务开展需求，该电商平台收集、存储、使用数据的情况如下：

商品名称	商品编号	商品评分	商品评分生成时间	店铺名称	店铺编号	用户姓名	用户 ID	用户手机号	用户身份证号码	涉及数据处理活动	数据处理频率
XX 抽纸	S-001-88296	5	2023.7.29	XX 官方旗舰店	D-001-77380	小强	204896826	130XXXX7620	110XXXXXXXXXXX6521	收集、存储、使用加工	每天进行一次大数据分析
XX 洗衣液	S-031-24786	4	2023.9.23	XX 超市	D-087-35469	小明	302857056	182XXXX8201	425XXXXXXXXXXX0946	收集、存储、使用加工	每天进行一次大数据分析
...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...

评估项	评估结果	评估记录

评估分析： 1）该企业的数据处理目的是否合理、正当； 2）所涉及的数据数量、类型、频率是否为实现该目的下的最小范围	☐满足 ☑不满足	1）该数据处理活动为合法开展业务所必须，满足正当性要求。 2）在该数据处理活动中，收集、存储、使用用 户姓名、手机号码、用户身份证号码并非为实 现业务需求的最小范围，不满足最小必要性要求。

【第 3 题】【组织保障】结合附件材料，评估是否满足以下数据安全管理要求。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否明确数据安全基础性管理和数据全 生命周期各环节安全保护要求和操作规 程，覆盖数据分类分级、权限管理、日 志留存、风险监测预警、应急响应、安 全评估、教育培训等方面；是否针对不 同级别数据，明确数据生命周期各环节 具体分级保护要求和操作规程；是否建立数据安全管理制度执行落实	☑满足 ☐部分满足 ☐不满足 ☐不涉及	已在《某企业重要数据和核心数 据安全管理办法》第五章中针对 不同级别数据,明确数据生命周 期各环节具体分级保护要求和 操作规程;《某企业重要数据和 核心数据安全管理办法》第七章 第一节及《某企业数据安全管理 办法》第六章建立数据安全管理 制度执行落实情况监督检查和 考核问责制度，对数据处理活动 进行安全监督管	附件 25-某企业重要数据和核心数据安 全管理办法第五章、第七章第一节 附件 1-某企业数据安全管理办法第六 章、第三章、第五章

情况监督 检查和考核问责制度，对数据处理活动 进行安全监督管理，并协助电信主管部门开展工作。		理，平台支撑部 为数据安全监督检查牵头责任 部门，其他部门开展好本部门数 据安全日常监测巡查工作,并积 极配合开展数据安全监督检查 工作。 已在《某企业数据安全管理办法》第三、五章中明确数据安全 基础性管理和数据全生命周期各环节安全保护要求和操作规程，覆盖数据分类分级、权限管 理、日志留存、风险监测预警、 应急响应、安全评估、教育培训 等方面。	

【第 4 题】【数据分类分级】结合附件材料，评估是否满足以下数据安全管理要求。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
数据分类分级管理制度是否明确数据分类分级管理范围、数据分类分级原则、标准及变更流程	☐满足 ☑部分满足 ☐不满足	已在《某企业数据安全管理办法》第三章第二节、附录 1、附录 2 中明确数据分类分级管理范围、数据分类分	附件 1-某企业数据安全管理办法第三章第二节、附录 1、附录 2 附件 25-某企业重要数据和核心数据

等内容；是否综合考虑业务需求、数据来源和用途等因素，划分本单位数据类别；是否在数据分类的基础上，按照电信主管部门要求以及相关标准规范制定数据分级标准识别重要数据和核心数据，明确各级数据界限，包括具体类别、子类、范围、对应的数据等，是否针对不同级别的数据制定差异化的保护策略。	☐不涉及	级原则、重要数据识别、数据资产梳理等内容。但数据分类分级细则中暂未明确变更流程的相关内容，且未明确重要数据及核心数据识别规则。 已在《某企业重要数据和核心数据安全管理办法》第五章中针对不同级别数据，明确数据生命周期各环节具体分级保护要求和操作规程，制定差异化的保护策略。	安全管理办法第五章

【第 5 题】【数据分类分级】结合附件材料，评估是否满足以下数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否梳理本单位数据，形成数据资产清单。	☐满足 ☑部分满足 ☐不满足 ☐不涉及	已梳理形成数据资产清单，但未对数据进行分类分级。	附件 2-数据资产清单

【第 6 题】【权限管理】结合附件材料，评估是否满足以下数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否建立数据内部登记、审批等工作机制，包括但不限于账号权限分配、开通、使用、变更、注销等审批流程和操作要求，重点关注账号权限变更、沉默账号、离职人员账号回收等情况。	☑满足 ☐部分满足 ☐不满足 ☐不涉及	在《某公司重要数据和核心数据安全管理办法》第三节中明确建立数据内部登记、审批等工作机制，包括但不限于账号权限分配、开通、使用、变更、注销等审批流程和操作要求，重点关注账号权限变更、沉默账号、离职人员账号回收等情况。	附件 4-账号审计 附件 25-重要数据和核心数据安全管理办法

【第 7 题】【权限管理】结合附件材料，评估是否满足以下数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件

查验数据处理活动有关平台系统是否配备账号安全管理措施，避免非授权账号访问处理数据： 1）是否配置口令复杂度策略，如：口令长度不少于8位，使用大写字母、小写字母、数字及特殊字符中至少三种的组合，且与用户名、字符顺序无相关性； 2）是否配置账号锁定策略，对系统账号口令输入尝试次数进行限制； 3）是否对口令遗忘的申请和重置流程实施严格管理。	☐满足 ☑部分满足 ☐不满足 ☐不涉及	系统配置密码长度最少为8位，必须包含小写字母及数字，不满足三种八位要求。系统用户连续错误登录5次后锁定IP。已配置忘记密码策略，系统用户可通过短信验证码重置密码。	附件6-密码策略

【第8题】【日志留存】结合附件材料，评估在以下方面是否满足数据安全管理要求，并有效落实。

（本题200分，判分规则如下：1.“评估结果”为固定答案，答对得50分，答错得0分；2.“评估记录”采用人工判分，根据答题情况判0-100分；3.“对应附件”为固定答案，答对得50分，答错得0分）

评估项	评估结果	评估记录	对应附件

是否明确日志管理要求，包括日志记录范围、留存时间、日志备份要求、日志审计职责划分、人员配备与审计频度等内容。	☐满足 ☑部分满足 ☐不满足 ☐不涉及	已在《某企业数据安全管理办法》第三章第一节、第五节中明确日志管理要求，包括日志记录范围、留存时间、日志审计职责 划分、日志审核策略等内容； 暂未明确日志备份要求、人员配 备与审计频度等。	附件 1-某企业数据安全管理办法第三章第一节、第五节

【第 9 题】【日志留存】结合附件材料，评估是否满足以下数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否定期开展日志审计，形成审计报告。报告是否包含操作时间、操作主体、操作类型、操作对象、操作结果、审计问题、改进方案、异常情况处置记录等内容，是否对审计发现问题进行整改跟踪。	☑满足 ☐部分满足 ☐不满足 ☐不涉及	审计人员每半年对账号权限、操 作日志、4A登录情况进行审计， 并形成审计报告，审计报告操作 时间、审计区间、操作对象、操 作主体、审计方法和审计结论 等，审计未发现问题。	附件8-安全审计报告

【第 10 题】【风险监测预警】结合附件材料，评估是否满足以下数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否明确数据安全风险监测预警工作负责部门；是否明确风险监测预警目的、方式、内容、操作规程、频度等内容；是否定期开展风险监测预警工作。	☐满足 ☑部分满足 ☐不满足 ☐不涉及	1.《某企业数据安全管理办法》 第五章明确风险监测预警要求， 发现数据安全缺陷、漏洞、泄露、 违规传输、访问异常等数据安全 风险时进行预警，及时组织排查 安全隐患，采取必要的措施防范 数据安全风险，但未明确风险监 测预警的操作规程和频度，未明 确数据安全风险监测预警工作 负责部门。 2.未明确风险监测预警目的、方式、内容、操作规程、频度等内 容。 3.企业具备数据防泄漏系统，具 备对网络、邮件、FTP、USB 等多 种数据导入导出渠道进行实时 监控的能力，及时对异常数据操 作行为进行预警拦	附件 1-某企业数据安全管理办法第五章 附件 9-风险监测预警

		截，防范数据 泄露风险。企业已建设数据安全 管控平台，定期对相关平台系统 数据资产进行扫描，能够发现识别个人敏感信息，可以对接口调 用进行必要的自动监控和处理。 企业已建设具有自动化操作审 计能力的平台系统。具备数据操 作权限配置、异常操作告警与处 置等核心功能，数据操作审计内 容和企业平台系统权限分配表 作为系统策略进行配置。	

【第 11 题】【应急处置】结合附件材料，评估是否满足以下数据安全管理要求。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件

数据安全应急预案是否充分考虑数据处理者涉及的各类数据安全事件业务场景，包括但不限于数据泄露（丢失）、数据被篡改、数据被损毁、数据违规使用等；是否根据事件等级明确应急响应责任分工、工作流程、处置措施等。	☑满足 ☐部分满足 ☐不满足 ☐不涉及	已制定数据安全应急预案，明确 应急组织机构及职责、应急流程、应急方案，并明确数据泄露（丢失）、数据被篡改、数据被 损毁、数据违规使用等场景的处 置措施。	附件 10-应急预案

【第 12 题】【应急处置】结合附件材料，评估在以下方面是否满足数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否制定数据安全事件应急演练计划；是否针对数据泄露（丢失）、数据被篡改、数据被损毁、数据违规使用等典型场景，至少每年开展一次演练，并做好演练记录；是否根据演练结果视情况优化本数据处理者数据安全保	☐满足 ☑部分满足 ☐不满足 ☐不涉及	已制定《应急演练计划》并针对 数据丢失、数据被篡改、数据泄 露、数据滥用等典型场景，至少 每年开展一次演练，并做好演练 记录，形成演练报告，但数据安 全事件典型场景不全面。	附件 23-应急演练记录 附件 24-应急演练计划

护措施，形成演练报告。			

【第 13 题】【教育培训】结合附件材料，评估在以下方面是否满足数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
年度培训时长是否不少于 10 学时，培训后是否组织对培训内容进行考核评定，并留存考核评定记录。	☑满足 ☐部分满足 ☐不满足 ☐不涉及	企业已制定数据安全岗位人员教育培训计划，并按照计划执行，年度培训时长不少于 10 学 时，培训后组织对培训内容进行考核评定，并留存考核评定记录。	附件 22-培训考核成绩 附件 11-教育培训计划及记录

【第 14 题】【数据收集】请分析在数据收集环节主要存在哪些风险，应配备哪些技术保障措施（简述依据）。

（本题 200 分，判分规则如下：1.“应配备哪些技术保障措施”为固定答案，答对得 50 分，答错得 0 分；2.“依据”采用人工判分，根据答题情况判 0-150 分）

所处环节	应配备哪些技术保障措施	依据
数据收集环节	☑部署安全防护设备 ☑权限管理 ☑访问控制 ☐校验技术 ☐密码技术 ☐脱敏技术 ☐数据防泄漏技术 ☐日志审计 ☐安全传输通道 ☐安全传输协议 ☐接口安全监测	1、查验数据处理者数据收集相关系统配置策略，是否根据数据安全级别采取相应的安全措施（如防火墙、入侵检测系统、入侵防御系统、白名单接入控制等）防止数据收集设备遭受网络攻击，确保采集过程中数据不被泄露； 2、应对数据收集设备进行安全配置，包括多因子身份鉴别机制、口令复杂度策略、账号锁定策略、口令遗忘和重置流程等。

【第 15 题】【数据存储】请分析在数据存储环节主要存在哪些风险，应配备哪些技术保障措施（简述依据）。

（本题 200 分，判分规则如下：1.“应配备哪些技术保障措施”为固定答案，答对得 50 分，答错得 0 分；2.“依

据”采用人工判分，根据答题情况判 0-150 分）

所处环节	应配备哪些技术保障措施	依据
数据存储环节	☑权限管理 ☑访问控制 ☑校验技术 ☑密码技术 ☐脱敏技术 ☐数据防泄漏技术 ☐日志审计 ☐安全传输通道 ☐安全传输协议 ☐接口安全监测	1、查验数据存储系统核心功能、安全配置策略等，是否落实差异化的安全存储要求，是否配备对用户或业务（应用程序）的访问控制措施，避免非授权访问。 2、查验数据存储系统安全配置策略，是否配备校验技术、密码技术等安全防护措施进行安全存储，是否提供重要数据和核心数据容灾备份的安全防护能力，是否定期开展数据恢复性测试，对备份数据的有效性和可用性进行检查和恢复验证；

【第 16 题】【数据收集】结合附件材料，评估是否满足以下数据安全管理要求。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件

查验数据处理者具体业务用户协议或隐私政策文件，是否明确个人信息收集的目的、用途和范围；是否按照公开透明原则，将收集规则以通俗易懂、简单明了的文字向用户明示并获得授权。	☐满足 ☑部分满足 ☐不满足 ☐不涉及	在用户收集时，通过《用户隐私协议》明确个人信息收集的目的、用途和范围，并且按照公开透明原则，将收集规则以通俗易懂、简单明了的文字向用户明示，但未获得用户主动授权。	附件 12-用户隐私协议

【第 17 题】【数据存储】结合附件材料，评估在以下方面是否满足数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否结合数据分类分级策略和管理要求明确数据存储安全策略和操作规程，包括各类数据存储平台系统差异化的安全存储措施（如加密、访问控制等）、数据存储介质安全策略和管理规定等；是否明确对数据存储系	☑满足 ☐部分满足 ☐不满足 ☐不涉及	1)《某企业数据安全管理办法》 第四章第三节明确数据存储安全要求。各部门应按数据敏感程度做好数据分类管理，对不同安全级别的数据采用差异化安全存储，包括差异化脱敏存储、加密存储、访问控制等。并做好加密算法、脱敏方法的安全性	附件 1-某企业数据安全管理办法：第四章第三节、第三章第四节、第三章第五 节

统账号权限管理、访问控制、日志留存等方面的安全要求。		保　密。各部门应采用访问控制、视频监控、接入鉴权等技术手段，加强对涉及收集、存储数据的重　要物理区域（如机房、维护处室/ 中心）和重点基础设施的安全 防护，定期（至少每季度一次） 开展安全检查，配置安全基线。各部门应采取有效的技术、管理 手段加强对涉及最高级和次高 级数据的系统使用移动存储介 质的管控。 2)《某企业数据安全管理办法》 第三章第四节明确访问权限管　理要求，明确按照权限最小化原　则、依据人员岗位角色进行账号　授权，每个账号应且仅应与唯一　的人员进行关联；应使用系统或　应用权限分配功能对不同级 别的数据设置不同的访问权限，不同岗位角色人员只能访问与 自己职责对应的数据。第三章第 五节明确日志留存要求，明确应 对数据处理相关日志进行留存。日志记录信息应包括操作时间、 操作账号、操作内容、授权情况、 登录信息等，并采用技术手段确 保日志的完整性。日志的保存时 间应满足国家相关法律法规要 求，	

		至少留存六个月。	

【第 18 题】【数据使用加工】结合附件材料，评估是否满足以下数据安全管理要求。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否明确数据导出场景、导出范围，以及相应的审批规则；是否明确要求导出的数据类型及数量为当前处理活动场景所必需的最小数据集。	☑满足 ☐部分满足 ☐不满足 ☐不涉及	因查询用户投诉数据，需将数据导出，导出数据满足最小化要求。导出到本地操作需要进行金库审批，并留存下载记录。	附件 14-数据使用加工

【第 19 题】【数据传输】结合附件材料，评估在以下方面是否满足数据安全管理要求，并有效落实。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否针对不同网络安全域之间的数据传输采取安全防护技术措施。	☑满足 ☐部分满足 ☐不满足 ☐不涉及	传输密码时采用加密算法传输数据。	附件 20-数据传输加密

【第 20 题】【数据提供】结合附件材料，评估是否满足以下数据安全管理要求。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
数据处理者数据提供清单是否包含获取方数据处理者名称、联系人信息，以及提供形式、期限、涉及的业务或系统、数据安全保护措施等内容。是否定期对清单进行更新。	☐满足 ☑部分满足 ☐不满足 ☐不涉及	企业已梳理数据提供清单，明确 获取方数据处理者名称、联系人 信息，以及提供形式、期限、涉 及的业务或系统、数据安全保护 措施等内容，但未并定期对清单进行更新。	附件 15-数据提供

【第 21 题】【数据销毁】结合附件材料，评估是否满足以下数据安全管理要求。

（本题 200 分，判分规则如下：1.“评估结果”为固定答案，答对得 50 分，答错得 0 分；2.“评估记录”采用人工判分，根据答题情况判 0-100 分；3.“对应附件”为固定答案，答对得 50 分，答错得 0 分）

评估项	评估结果	评估记录	对应附件
是否对不同类型的存储介质（闪存、移动硬盘、固态硬盘、硬盘、磁带、光盘等），提供不同的销毁措施。如针对用户注销服务、存储介质维护需要带出机房等场景可采用多遍覆盖、删除密钥、执行固件擦除命令等安全数据删除方式，针对介质报废等场景，可采取高压击穿、消磁、粉碎等物理损毁手段。	☑满足 ☐部分满足 ☐不满足 ☐不涉及	对于报废硬盘，通过物理消磁方 式进行数据删除，留存介质报废 及数据删除申请工单及纸质审 批记录。	附件 16-数据销毁

【第 22 题】【简答题】【计算合规性评估得分】

（本题 200 分，判分规则如下：1.“合规性评估得分”，“是否通过合规性评估”为固定答案，答对各得 50 分，答

错得 0 分；2.“请简述计算和分析过程”采用人工判分，根据答题情况判 0-100 分）

假定针对该数据处理活动的合规性评估结果为：满足项 42 项、部分满足 20 项、不满足 15 项、不涉及 3 项，请问该数据处理活动的合规性评估得分是多少？是否通过合规性评估？请简述计算和分析过程。

基础性安全评估和数据全生命周期安全评估每项评估结果可分为符合、部分符合、不符合、不适用，分别对应 1 分、0.5 分、0 分、不计算得分。因此，该类数据的合规性评估的得分为：

（42*1+20*0.5+15*0）/（80-3）=0.675

加总后平均归一化算数分值小于 0.7，则判定合规性评估不通过；平均归一化算数分值大于等于 0.7，则判定合规性评估通过。

【第 23 题】以下为该企业“安全报警漏洞及事件运营数据”（第 1 题第 4 项数据）的“安全预警数据处理活动”的数据安全风险评估相关结论，请分析其发生数据安全事件的可能性级别。

（本题200分，判分规则如下：1.“可能性级别”为固定答案，答对得50分，答错得0分；2.“判定过程”采用人工判分，根据答题情况判0-150分）

1、合规性评估情况

该数据处理活动正当必要性评估结果为符合。基础性安全评估和数据全生命周期安全评估如下表所示。

序号	合规性评估类别	符合项数量	部分符合项数量	不符合项数量	不适用项数量
1	基础性安全评估	32	2	2	3
2	数据全生命周期安全评估	28	2	1	10
合计		60	4	3	13

2、风险源识别情况

判定因素	结果记录

网络环境和技术措施	数据处理活动系统处于内部网络环境中、但与 2 个内网其他信息系统存在交互，合规性评估中技术措施相关评估项评估结果存在 1 项不符合和 1 项部分符合项。
管理制度和处理流程	1、管理制度可以覆盖数据处理活动全生命周期所有环节、所有场景，但在风险监测报送、应急处置方面要求尚不完善。合规性评估中管理措施相关评估项评估结果存在 2 项不符合和 3 项部分符合。 2、对数据授权访问、批量复制、使用加工、出境、销毁等重点环节进行日志留存。 3、建立数据安全风险报送监测、数据安全事件应急响应机制，按照要求制定应急预案，并定期组织应急演练，可以基本实现对数据安全风险的监测发现和数据安全事件的应急处置，但存在应急演练记录不完整、未明确数据安全风险监测报送要求问题。 4、建立内部审批和登记工作机制，对重要数据处理活动实施严格管理并留存记录。
参与人员和接收方管理	1、建立数据获取方管理制度，明确对数据获取方管理要求，暂不涉及数据获取方。 2、配备数据安全管理人员，明确数据安全管理职责，相关人员能力与岗位职责互相匹配，可以统筹负责数据处理活动的安全监督管理。

	3、重要数据、核心数据处理者设立数据安全管理机构，明确内部数据处理关键岗位、职责、任职要求以及负责履行数据安全管理的义务。 4、重要数据、核心数据处理者对数据处理关键岗位人员进行数据安全相关培训和考核，确保数据处理关键岗位人员相应的数据安全保护专业知识和技能。 5、重要数据、核心数据处理者与数据处理关键岗位人员签订数据安全责任书，但责任书内容未包含处罚措施内容。 6、重要数据、核心数据处理者对数据处理关键岗位人员权限进行区分，通过有效手段限制不同身份数据处理者权限，且权限划分合理、准确。 7、重要数据、核心数据处理者不涉及数据获取方。
安全态势	2 年内未发生过较大及以上数据安全事件，未收到过电信主管部门发出的处罚或风险预警信息。

请选手在下述表格中进行作答。

可能性级别	判定过程（简述合规性评估结论、风险源识别结论，以及综合研判理由和依据）

☐高 ☑中 ☐低	**合规性评估计算得分：（60*1+4*0.5+3*0）/67=0.925** **风险源识别等级为：** 网络环境和技术措施：可能性级别为中，原因：重要数据处于内部网络环境中、与 2 个内网其他信息系统存在交互，合规性评估中技术措施相关评估项评估结果存在 1 项不符合和 1 项部分符合项。 管理制度和处理流程：可能性级别为中，原因：①合规性评估中管理措施相关评估项评估结果存在 2 项不符合和 3 项部分符合②存在应急演练记录不完整、未明确数据安全风险监测报送要求问题。 参与人员和接收方管理：可能性级别为中，原因：重要数据处理者与数据处理关键岗位人员签订数据安全责任书，但存在内容不全面、不充分的问题，未明确约定数据安全处罚措施内容措施内容。 安全态势：可能性级别为低 按照最高原则，可能性等级为中。

【第 24 题】【简答题】【安全影响分析】该数据处理活动分析表如下，请各位选手判定其安全影响程度，并简述判定过程。

（本题200分，判分规则如下：1.“安全影响程度”为固定答案，答对得50分，答错得0分；2.“判定过程”采用人工判分，根据答题情况判0-150分）

序号	数据处理活动	数据项名称	数据类型	数据级别	数据数量	处理目的	数据处理方式	处理频率	是否涉及数据出境	数据载体（涉及信息系统名称）
1	用户评分数据处理活动	用户评分数据	业务经营数据	一般数据	约 10 亿条	为用户购买商品提供参考	数据收集、存储、使用	实时	否	某电商平台系统

判定因素	安全影响程度	判定过程
安全影响分析结论	☐特别严重 ☐严重 ☑一般	该数据处理活动仅涉及一般数据，因一般数据因其数据敏感程度较 低，在发生泄露、损毁、丢失等安全事件后不会对国家安全、公共 利益产生较大影响，因此可直接判定其安全影响程度为一般。

【第 25 题】假定某企业全量数据的风险评估结果如下，请根据附件 28，给出一般数据的风险评估得分、重要数据的风险评估得分、企业数据安全风险评估的总体得分和评估等级，并简述判定过程。

本题 200 分，判分规则如下：1.“一般数据的风险评估得分”“重要数据的风险评估得分”“企业数据安全风险评估总体得分”“企业数据安全风险评估等级”为固定答案，答对各得 40 分，答错各得 0 分；2.“简述分析和计算过程”采用人工判分，根据答题情况判 0-40 分）

- 一般数据
  - 用户风控行为分析数据：1 项数据处理活动为低风险。
  - 业务营收与商业合作分析数据：2 项数据处理活动分别为低风险、中风险。
  - 安保人员信息：1 项数据处理活动为低风险。
  - 产品专利：1 项数据处理活动为低风险。
- 重要数据
  - 全国业务系统工程可行性报告：1 项数据处理活动为低风险。
  - 全国业务系统机房详细基建数据：1 项数据处理活动为低风险。

■ 全国业务系统运行信息、维护策略数据：1 项数据处理活动为高风险。

■ 安全报警漏洞及事件运营数据：2 项数据处理活动分别为中风险、高风险。

■ 全国业务用户注册信息：2 项数据处理活动分别为高风险、极高风险。

■ 全国业务用户行为记录：1 项数据处理活动为中风险。

□ 无核心数据。

请选手在下述表格中进行作答。

一般数据的风险评估得分	重要数据的风险评估得分	企业数据安全风险评估总体得分	企业数据安全风险评估等级	简述分析和计算过程（简述一般数据、重要数据风险评估得分的计算过程；企业数据安全风险评估总体得分的计算过程；企业数据安全风险评估等级的研判过程）
9.125	42.75	51.875	□ 优 □ 良 □ 中 ☑ 差	一般数据 4 项，低风险 3 个，中风险一个： 所以 A=(3*1+1*0.65)/4=0.9125 重要数据 6 项，低风险 2 个，中风险 1 个，高风险 2 个，极高风险 1 个： 所以 B=(2*1+1*0.65+2*0.1=1*0)/6=0.475 因 c=0 企业总体综合得分 S=A*10+B*90=9.125+42.75=51.875