ICS 35.240.40
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXX—XXXX

金融数据安全 数据安全评估规范

Financial data security—Data security assessment specification

（征求意见稿）

（本稿完成日期：2021 年 11 月 26 日）

20XX－XX－XX 发布　　20XX－XX－XX 实施

中国人民银行　　发 布

目 次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：。

本文件主要起草人：。

引　言

随着信息技术的发展，众多金融基础业务、核心流程、行业间往来等事务和活动均已运行在信息化支撑载体之上，金融业机构生产运行过程中产生的信息也逐步以不同形式转化为数字资产流转在金融业信息系统之中。随着大数据、人工智能、云计算等新技术在金融业的深入应用，金融数据逐步实现了从信息化资产到生产要素的转变，其重要性日益凸显。数据泄露、滥用、篡改等安全威胁的影响逐步从机构内转移扩大至机构间以及行业间，甚至影响国家安全、社会秩序、公众利益与金融市场稳定。如何在满足金融业务基本需求的基础上，强化数据保护能力，防范数据安全风险，切实保障金融数据价值发挥，已成为当前亟待解决的问题。

金融数据复杂多样，新技术背景下的金融数据应用形态多样、生态各异，并逐步实现与金融产品和服务的深度融合，而当前各金融业机构数据安全管理能力尚处于参差不齐的状态，金融业整体数据安全保护仍有待进一步统筹协调，逐步实现规范化和标准化。开展金融数据安全评估，一方面能够推动金融业机构落实金融业数据安全管理要求，提升金融业数据安全保护工作的规范化和标准化程度；另一方面有助于金融业机构及时全面掌握本机构数据安全管理水平，预测并确认所面临的数据安全威胁和风险，为金融业机构制定防范措施及应对安全事件提供科学依据和指导，可有效防控数据安全事件风险和危害，为金融数据的应用和流动提供有力保障。

为指导金融业机构合理制定和有效落实金融数据安全评估策略，进一步提高金融业数据安全保护水平和数据安全应用能力，服务金融数据价值的最大化发挥，编制本文件。

本文件凡涉及密码技术的相关内容，按国家密码管理部门及行业主管部门有关规定实施；凡涉及采用密码技术解决保密性、完整性、真实性、不可否认性需求的，遵循相关国家标准和行业标准。

金融数据安全　数据安全评估规范

1　范围

本标准规定了金融数据安全评估触发条件、原则、参与方、内容、流程及方法，明确了数据安全管理、数据安全保护、数据安全运维三个主要评估域及其安全评估主要内容和方法。

本标准适用于金融业机构开展金融数据安全评估使用，并为第三方安全评估机构等单位开展金融数据安全检查与评估工作提供参考。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0171—2020　个人金融信息保护技术规范

JR/T 0197—2020　金融数据安全 数据安全分级指南

JR/T 0223—2021　金融数据安全 数据生命周期安全规范

GB 50174—2017　数据中心设计规范

GB/T 39335—2020　信息安全技术 个人信息安全影响评估指南

3　术语和定义

GB/T 35273—2020和GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

金融数据 financial data

金融业机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据。

注：该类数据可用传统数据处理技术或大数据处理技术进行组织、存储、计算、分析和管理。

[来源：JR/T 0197—2020，3.10]

3.2

保密性　confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[来源：GB/T 25069—2010，2.1.1]

3.3

完整性　integrity

保卫资产准确性和完整的特性。

[来源：GB/T 25069—2010，2.1.42]

3.4

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[来源：GB/T 25069—2010，2.1.20]

3.5

真实性 authenticity

确保主体或资源的身份正是所声称的特性。

注：真实性适用于用户、进程、系统和信息之类的实体。

[来源：GB/T 25069—2010，2.1.69]

3.6

删除 delete

在金融产品和服务所涉及的系统中去除信息的行为，使其保持不可被检索、访问的状态。

[来源：GB/T 35273—2020，3.10]

4 缩略语

下列缩略语适用于本文件：

ACL：访问控制列表（Access Control Lists）

API：应用程序接口（Application Programming Interface）

APP：应用程序（Application）

DES-CBC：数据加密标准-密码块链接（Data Encryption Standard-Cipher Block Chaining）

IP：网际互连协议（Internet Protocol）

MAC：媒体访问控制（Media Access Control）

MD5：消息摘要算法（Message-Digest Algorithm 5）

SHA1：安全散列算法（Secure Hash Algorithm 1）

SSID：服务集标识（Service Set Identifier）

WEB：全球广域网（World Wide Web）

WLAN：无线局域网（Wireless Local Area Network）

5 金融数据安全评估概述

5.1 触发条件

金融数据安全评估指金融业机构对其数据处理活动定期或按需开展的风险评估活动，用于评价金融业机构自身和数据处理活动第三方合作机构的数据安全保护能力，为金融业机构建立数据安全保护体系、明确数据安全保护策略和加强第三方合作机构数据安全管理提供参考性资料。金融业机构应定期开展金融数据安全评估工作，评估周期应不超过一年；金融业机构金融数据资产、金融数据安全保障、金融数据应用场景等发生变化时，也应触发金融数据安全评估工作，触发条件及其评估内容应至少包括表5.1.1所示情况。金融业机构在金融产品或服务上线前、业务功能或信息系统发生较大变更以及本机构发生重大数据安全事件等情况时均应开展全面评估，且应重点关注与该产品或服务数据或该变更部分密切相关的评估内容。以上及其他需要进行金融数据安全评估的情况，金融业机构均应及时开展数据

安全评估工作，并留存相关评估过程材料及评估报告等评估结果材料，以备查验、备案或上报等使用。

表5.1.1 数据安全评估触发条件

序号	评估场景	评估侧重点	主要评估内容
1	对 3 级及以上数据进行加工前，应进行数据安全评估。	1.评估数据加工的必要性。 2.评估数据加工的合法合规性。 3.评估所采取数据安全保护措施的充分性和有效性。	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、3、4、7 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的第 5、6、9 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的第 1、7 项。 5.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的全部评估项。 6.章节 7.2.5.3 数据加工 表 7.2.7 数据加工评估内容的第 1、2、3、4 项。 7.章节 7.2.3 数据采集至 7.2.4 数据存储、7.2.6 数据删除及 7.2.7 数据销毁中与当前数据加工相关的全部评估项。
2	使用外部的软件开发包、组件、源码等开展开发测试工作前，应进行数据安全评估。	1.评估外部的软件开发包、组件、源码的安全性。 2.评估测试方法的合规性。 3.评估所采取数据安全保护措施的充分性和有效性。	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、6、7、10、12 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的第 3、9、10、12 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的 1、7、8、9、10 项。 5.章节 6.2.4 合作管理 表 6.2.4 合作管理评估内容的全部评估项。 6.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的全部评估项。 7.章节 7.2.5.5 开发测试 表 7.2.9 开发测试安全评估内容的第 1、2、3、4、5、6、7、9 项。 8.章节 7.2.3 数据采集至 7.2.4 数据存储、7.2.6 数据删除及 7.2.7 数据销毁中与当前开发测试相关的全部评估项。
3	将数据委托给第三方机构进行处理前，应对被委托方的数据安全防护能力进行数据安全评估。	1.评估被委托方组织架构和制度体系方面安全管理的合规性。 2.评估委托方数据安全保护措施的充分性和有效性。 3.评估委托方对数据安全事件所作应急预	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、3、4、7 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的第 5、6、9 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的第 1、7 项。

序号	评估场景	评估侧重点	主要评估内容
		案的充分性和有效性。	5.章节 6.2.4 合作管理 表 6.2.4 合作管理评估内容的全部评估项。 6.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的全部评估项。 7.章节 7.2.5.9 委托处理 表 7.2.13 委托处理安全评估内容的第 2、4、6、7、8、11 项。 8.章节 7.2.3 数据采集至 7.2.4 数据存储、7.2.6 数据删除及 7.2.7 数据销毁中与当前委托处理相关的全部评估项。 9.章节 8 与当前委托处理及相关第三方机构安全管理相关的全部评估项。
4	与外部机构进行数据共享，应定期对数据接收方的数据安全保护能力进行数据安全评估。	1.评估数据接收方组织架构和制度体系安全管理的合规性。 2.评估数据接收方数据安全保护措施的充分性和有效性。 3.评估数据接收方对数据安全事件所作应急预案的充分性和有效性。	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、6、10、12 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的第 3、9、10、12 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的第 4、7、8、9、10 项。 5.章节 6.2.4 合作管理 表 6.2.4 合作管理评估内容的全部评估项。 6.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的第 1、3 项。 7.章节 7.2.5.10 数据共享 表 7.2.14 数据共享安全评估内容的第 9、10、11、12、14 项。 8.章节 7.2.3 数据采集至 7.2.4 数据存储、7.2.6 数据删除及 7.2.7 数据销毁中与当前数据共享相关的全部评估项。 9.章节 8 中与当前数据共享及相关第三方机构安全管理相关的全部评估项。
5	在金融产品或服务上线发布前，数据安全管理委员会应组织开展数据安全评估，避免不当的数据采集、使用、共享等行为。	1.评估金融产品或服务在用户数据采集、传输、存储、使用、删除等数据处理整个流程的合法合规性。 2.评估所采取数据安全保护措施的充分性与有效性。	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、3、6、7、10、11、12 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的 1、2、3、4、7、8、10 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的第 1、2、8、9、10 项。 5.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的全部评估项。 6.章节 6.1 组织架构建设 S1-1 表 6.1.1 组织架构建设情况评估内容的第 3、4、7、11、12、13 项。

序号	评估场景	评估侧重点	主要评估内容
			7.章节 7.2 数据生命周期安全评估中与此产品或服务相关的全部评估项。 8.章节 8 中与此产品或服务相关的全部评估项。
6	若有第三方机构参与到金融业机构数据全生命周期过程，应根据其数据安全保护能力进行数据安全评估。	1.评估第三方机构组织架构和制度体系安全管理的合规性。 2.评估第三方机构所采取数据安全保护措施的充分性与有效性。 3.评估第三方机构对数据安全事件所作应急预案的充分性和有效性。	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、6、10、12、16、17 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的第 2、3、6、9、12 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的第 4、7、8、9、10 项。 5.章节 6.2.4 合作管理 表 6.2.4 合作管理评估内容的全部评估项。 6.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的全部评估项。 7.章节 6.2.4 合作管理 表 6.2.4 合作管理评估内容的第 1、2、3、4、5、6、7、13 项。 8.章节 7.2 数据生命周期安全评估中与当前第三方机构参与过程相关的全部评估项。 9.章节 8 中与当前第三方机构参与过程及第三方机构安全管理相关的全部评估项。
7	在金融业机构业务功能发生重大变化时，应及时进行数据安全评估。	1.评估新的业务功能数据处理整个流程的合法合规性。 2.评估现有数据安全保护技术是否能满足对新业务的数据保护需求。	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、3、6、8、10、12、13、14、15 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的第 1、3、10、11、12 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的第 1、5、6、8、9 项。 5.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的全部评估项。 6.章节 8.5 安全检查 表 8.5.1 安全检查评估内容的第 1、2、5、8 项。 7.章节 7.2 数据生命周期安全评估中与当前业务过程相关的全部评估项。 8.章节 8 中与当前业务数据及业务功能安全监测相关的全部评估项。

序号	评估场景	评估侧重点	主要评估内容
8	在国家及行业主管部门的相关要求发生变化时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，应进行数据安全评估。	1.评估现有数据安全保护措施是否能满足新的保护要求。 2.评估新的数据处理流程的合法合规性。 3.评估引发数据安全事件的薄弱环节及原因。	1.章节 6.1 组织架构建设 表 6.1.1 组织架构建设情况评估内容的第 2、3、6、8、10、12、13、14、15 项。 2.章节 6.2.1 总体规划 表 6.2.1 总体规划情况评估内容的全部评估项。 3.章节 6.2.2 技术管理 表 6.2.2 技术管理情况评估内容的第 1、3、10、11、12 项。 4.章节 6.2.3 人员管理 表 6.2.3 人员管理情况评估内容的第 1、5、6、8、9 项。 5.章节 6.2.5 流程管理 表 6.2.5 流程管理评估表的全部评估项。 6.章节 7.2 数据生命周期安全评估中与当前变更情况相关的全部评估项。 7.章节 8 中与当前变更情况相关的全部评估项。
9	每年至少应开展 1 次全面的数据安全检查评估，评估方式至少包括自评估、外部第三方机构评估等。	1.评估数据安全管理制度的完备性与落实程度。 2.评估数据生命周期各环节的合法合规性。 3.评估数据安全运维保障措施的完备性与有效性。	章节 6 金融数据安全管理评估、7 金融数据安全保护评估、8 金融数据安全运维评估中全部评估项，并以本机构主要数据安全风险、重点改进问题等相关的评估项为主要评估内容。

5.2 评估原则

金融数据安全评估遵守以下原则：

a) 客观公正原则：是指在评估过程中，应当根据被评估方实际情况做出判断和真实的评价，不得夸大或掩盖发现的问题，不得根据个人主观意愿或他人意见做出评价；

b) 可重用原则：是指在适当情况下，相同的评估内容可参考或引用被评估方已有的评估结果；

c) 可再现原则：是指对于相同评估内容和评估要求，在相同评估环境下，采用同样评估方法对同一被评估方的评估实施过程进行重复操作，可得到相同评估结果；

d) 最小影响原则：是指在评估过程中尽量小地影响被评估方现有业务和信息系统正常运行，最大程度地降低对被评估方造成的干扰和风险；

e) 信息保密原则：是指评估参与方对本次评估所涉及的被评估方商业信息、客户信息、技术文件等进行严格保密。

5.3 评估参与方

明确本次金融数据安全评估的牵头部门，作为评估工作的主要参与方，负责牵头开展评估工作，协调各方资源，保证评估工作的开展，并对评估结果的质量负责。牵头部门或人员应具有独立性，不受到被评估方的影响，通常由机构的数据安全管理有关责任部门担任。

根据金融数据安全评估的范围和内容，识别并确认本次评估工作过程涉及的本机构内部各部门，如业务部门、法务部门、合规部门、技术部门等内部组织，作为本次评估工作的其他参与方，负责配合开

展各部分评估工作，及与其相关外部合作方的协调和管理工作，确保评估工作的顺利开展，并对发现的问题进行确认和整改。负责配合开展各部分评估工作，并负责各有关外部合作方的协调和管理工作，确保评估工作的顺利开展，并对发现的问题进行确认和整改。

成立独立评审组，负责对评估过程与结果做真实性与合规性的评审，并确保评审过程的独立性。评审组直接向本机构本次金融数据安全评估工作最高负责人或本机构数据安全管理委员会领导小组负责。

5.4 评估内容

JR/T 0197-2020中的金融数据及其安全分级，以及JR/T 0223-2021中的金融数据生命周期安全要求是金融数据安全评估的主要内容，主要评估域见图1，包括数据安全管理（S1）、数据安全保护（S2）、及数据安全运维（S3）三方面内容。开展金融数据安全评估的过程中，应通过技术手段识别金融业机构的金融数据资产，确定评估的保护对象范围，同时，识别金融业机构数据安全管理相关组织架构建设、制度体系建设、数据资产管理及相应安全防护技术应用等方面需求及实际实施情况，并对数据安全运维机制进行确认，分析金融业机构在金融数据保护过程中存在的缺陷和不足，对金融业机构的数据安全风险、数据保护策略实施情况、数据安全保护能力等进行综合评定，得出最终的评估结论。其中，本文件所述各评估域的各项评估内容表中，凡注明“可选项”的，均为可根据实际情况进行选评的内容，可不计入或仅将已选评项计入最终评估结果；凡未注明“可选项”的，均为必评内容，应计入最终评估结果。此外，实际评估过程中，应结合当前评估需求、评估目标及评估范围等情况，对于不属于当前评估范围内的各项必评内容，视为不纳入本次评估范畴，不应计入最终评估结果，且应在评估相关记录及评估报告中作明确记录和必要说明。

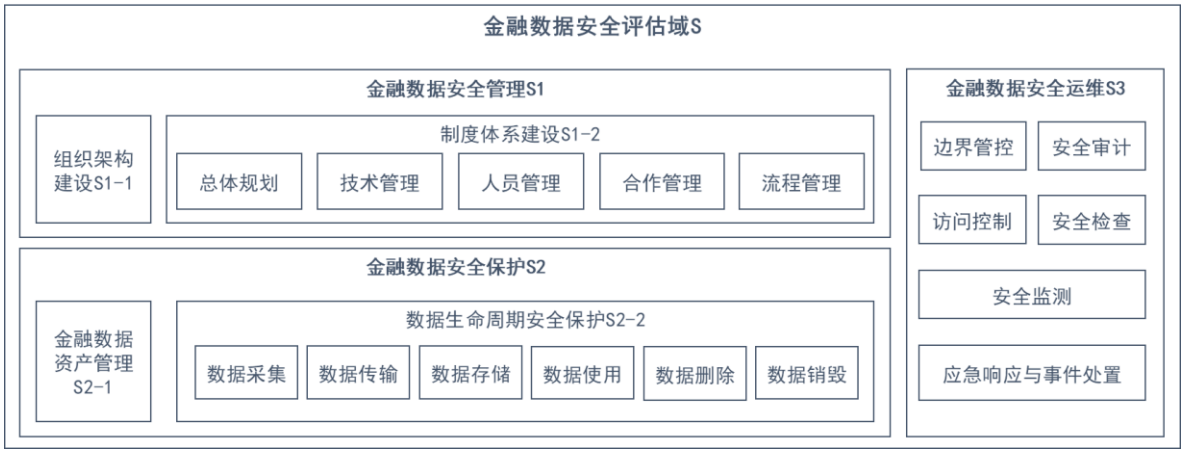

图1 金融数据安全评估域示意图

5.5 评估流程

5.5.1 评估准备

5.5.1.1 明确评估目标

在进行金融数据安全评估前，需首先明确评估目标，包括但不限于：数据安全合规差距分析，提升自身数据安全管理能力，发现并防控自身数据安全风险，核验第三方参与机构数据安全管理能力等。

5.5.1.2 组建评估团队

根据评估目标组建评估团队，评估团队由本机构本次金融数据安全评估的最高负责人、评估参与方以及实施团队等共同组成。其中，本机构本次金融数据安全评估工作的最高负责人，宜由本机构分管数据安全工作的最高负责人担任，负责对本次评估工作进行指导和决策；由最高负责人指定本机构内本次

评估工作的牵头部门，并作为主要参与方承担本次评估工作的总体统筹组织及内部沟通机制的协调建设等工作；由牵头部门识别并报最高负责人审定本机构其他参与方及相关外部合作方。为保障评估工作顺利开展，各参与方主要负责人应为评估团队成员。由牵头部门指定并报最高负责人审定本次评估工作的实施团队及评审组。根据评估及其评审需求及形式的不同，实施团队可由本机构内部具有相关评估能力或资质的人员抽调组成，也可由外部聘请的第三方数据安全评估团队组成；评审组可由本机构内部具有相关评审能力或资质的人员抽调组成，也可由外部聘请的行业专家、权威学者等组成。

5.5.1.3 明确评估范围

根据本机构本次金融数据安全评估实际需求和目标，明确评估范围,确定本次评估所涉及的金融数据、金融产品和服务、信息系统、人员及组织（含内、外部）等。

5.5.1.4 制定评估方案

根据本次评估目标和范围等情况编制并确定本次金融数据安全评估工作的评估方案，明确本次评估工作的主要任务、任务分工、人员安排、时间计划等，至少包括：

a) 评估人员：明确评估人员角色、数量、工作安排等要求，以及各角色的职责、能力及资质要求，并明确具体人员安排清单；
b) 评估要点列表：根据本次评估目标、范围以及本机构业务特点等实际情况，确定本次评估要点，并明确相应评估判定准则；
c) 结果预期：根据本次评估目标、范围以及本机构业务特点等实际情况，明确本次评估工作的主要工作成果预期，并明确各项工作成果的主要交付物及其交付形式、主要结论及预期达到的效果等内容；
d) 方法、技术和工具：根据评估要点及判定准则，确定主要评估方法、技术以及工具，并形成方法、技术和工具清单；
e) 涉及到的配合人员：根据评估要点，识别相关参与方及外部合作方，并明确主要负责人员及主要配合人员；
f) 时间计划：根据评估目标及评估要点，拆分评估任务，明确各项评估任务的主要内容、时间分配等，并形成具体的时间计划清单。

5.5.2 评估实施

依据本次评估工作最高负责人的指导要求，在评估团队牵头部门的组织和其他参与方的共同配合下，金融数据安全评估的实施团队根据已确定的评估方案开展本次评估的实施工作，留存评估实施过程相关记录材料并形成各部分评估结果。为保障评估工作的顺利开展，评估团队确立的内部沟通机制，应能够有助于评估团队定期对评估的进度、难点等进行沟通、确认和协商解决。

5.5.3 安全分析

根据本次金融数据安全评估的评估结果，实施团队对本机构当前数据安全现状、所面临的各类数据安全问题严重程度及主要安全风险情况等进行分析，并提出相应改进建议。本次金融数据安全评估牵头部门就以上评估结果、安全分析及安全建议等情况组织本机构内部审核和确认工作，并会同评估团队各参与方形成最终安全分析结论。

5.5.4 报告编制

本次金融数据安全评估实施团队根据评估结果及安全分析结论编制评估报告，对评估内容、过程、结果、问题等进行总结和分析，并给出总体评估结论。

5.5.5 结果评审

评审团队根据本次金融数据安全评估最终形成的评估报告及总体评估结论，对评估的过程、参与人员、评估结论等进行确认，审核确定各评估事项及参与人员行为等公平公正、真实有效及合法合规。

5.6 评估方法

金融数据安全评估采用的评估方法与风险评估类似，采用的评估手段至少包括：

a) 问卷调查：通过编制并组织填写问卷形式，对被评估方数据安全保护状况等情况进行统计和调查，获取机构情况及评估任务等有关基本信息；
b) 人员访谈：通过与被评估方进行交流、讨论方式，了解有关信息；
c) 文档查验：由被评估方提供与数据安全相关文档材料，评估小组查验相关文档材料是否已涵盖完整数据生命周期要求和控制项；
d) 配置核查：根据被评估方提供技术材料，登录相关信息系统工具平台，检查配置是否与材料保持一致，对文档审核内容进行核实；
e) 工具测试：利用技术工具对信息系统、应用软件等进行实操测试，验证被评估方是否符合相关评估内容所述技术能力、功能等要求；
f) 旁站验证：通过被评估方人员对承载数据的信息系统、设备、网络等进行现场操作和演示，由评估方人员对数据采集界面、数据展示界面、数据存储界面、数据操作日志记录、数据处理流程、防护机制等进行查验，评估数据安全保障措施是否有效，并实地观察人员行为、技术设施和环境状况判断人员的安全意识、业务操作、管理程序等方面的安全情况。

6 金融数据安全管理评估 S1

6.1 组织架构建设 S1-1

组织架构建设情况评估内容见表 6.1.1。

表 6.1.1 组织架构建设情况评估内容

序号	安全要求	评估方法	结果判定
1	应设立由金融业机构高级管理层组成的领导小组，总体负责数据安全工作的统筹组织、指导推进和协调落实，明确数据安全管理部门，协调机构内部数据安全管理资源调配。	1.文档查验	1.查阅数据安全管理委员会领导小组相关制度及工作文件，确认领导小组由金融业机构高级管理层构成。 2.查阅相关制度文件，确认领导小组的工作职责已主要涵盖总体负责数据安全工作的统筹组织、指导推进和协调落实、协调本机构内部数据安全管理资源调配等，并且已明确数据安全管理部门。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	应设立数据安全管理委员会，成员应至少包括主要部门的主要负责人，负责数据安全相关工作的实施、相关政策和制度的制定评审工作，保障数据安全管理工作所需资源，并设立数据安全管	1.文档查验 2.人员访谈	1.查阅数据安全管理委员会相关制度及工作文件，确认委员会成员至少包括数据安全管理、信息科技、业务、法务、合规、风险管理、稽核审计、人事部门等相关部门的主要负责人。 2.查阅相关制度文件，确认委员会的工作职责已主要涵盖负责数据安全相关工作的实施、相关政策和制度的制定评审工作，保障数据安全管理工作所需资源等。

序号	安全要求	评估方法	结果判定
	理专职岗位，负责日常数据安全管理工作。		3.查阅相关制度文件，确认已设立数据安全管理专职岗位，且其职责为日常数据安全管理工作。 4.访谈数据安全管理专职岗位人员，确认日常数据安全管理工作已落实到人、岗位职责明确。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
3	应制定、发布和更新本机构数据安全管理制度、规程与细则，并定期审核和修订。	1.文档查验	1.查阅本机构数据安全管理制度、规程与细则等相关文件，确认其完备性。 2.查阅相关制度、规程与细则的审核及更新记录，确认已定期审核和修订。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	应组织开展本机构数据分级工作，识别并维护数据资产清单。	1.文档查验 2.人员访谈	1.查阅组织开展本机构数据分级工作的相关文件，确认包括数据分级、识别以及维护数据资产清单的内容。确认相关文件中包括负责数据安全分级工作的部门、岗位，负责定义组织整体的数据分级的安全原则，配合推动相关工作要求的执行。 2.访谈相关人员，确认其能够对数据资产清单进行正确识别，并开展定期维护。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	应制定、签发、实施、定期更新隐私政策和相关规程。	1.文档查验 2.旁站验证	1.查阅关于制定、签发、实施、定期更新隐私政策和相关规程的相关文件，确认其完备性。 2.查验APP、网上银行等客户端隐私政策文件获取及查阅方式，确认可正常获取及查阅。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
6	应监督本机构内部，以及本机构与外部合作方数据安全管理情况。	1.文档查验 2.人员访谈	1.查阅关于监督本机构内部以及本机构与外部合作方数据安全管理情况的相关文件和工作材料，确认其已正式发布。 2.查阅相关材料中负责对合作方进行管理的相关岗位和人员情况，确认合作方的数据安全管理情况满足本机构对合作方数据安全要求，并监督合作方遵守相关数据安全管理要求。 3.访谈相关人员，确认本机构内部，以及本机构与外部合作方数据安全管理要求与实际工作开展情况一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。

序号	安全要求	评估方法	结果判定
7	应在金融产品或服务上线发布前组织开展数据安全评估，避免不当的数据采集、使用、共享等行为，如与产品或服务功能及隐私政策不符等情况。	1.文档查验 2.人员访谈	1.查阅关于金融产品或服务上线发布前组织开展数据安全评估的相关文件和工作流程，确认相关文件和工作流程中已设置负责金融产品或服务上线发布前的组织、开展数据安全评估的合规的管理部门、人员，并查阅对数据采集、使用、共享等行为的要求，确认其符合隐私政策规定，并已制定相关解决方案。 2.查阅数据安全评估的相关材料，结合国家及行业主管部门相关规定和技术标准要求、本机构相关制度标准，确认评估过程及结果的合规性。 3.访谈相关人员，确认在数据安全评估过程中，对不当的数据采集、使用、共享等行为的规避情况进行了评估，并确认符合产品或服务功能及隐私政策。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
8	应由业务部门、信息系统建设部门、信息系统运维部门设立数据安全岗位，作为数据安全管理的执行层。	1.文档查验	1.查阅关于设立数据安全岗位作为数据安全管理执行层的相关制度文件，确认其包括业务部门、信息系统建设部门和信息系统运维等数据安全管理与安全应用相关部门。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
9	数据安全岗位人员应根据数据安全相关策略和规程，落实本部门数据安全防护措施。	1.文档查验 2.人员访谈	1.查阅本部门数据安全防护措施落实的相关工作材料，确认其符合数据安全相关策略和规程。 2.访谈相关人员，确认本部门实际落实的数据安全防护措施与数据安全相关政策和规程一致。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
10	数据安全岗位人员应做好经授权审批程序后，为获得授权的各相关方分配数据权限的相关工作。	1.文档查验 2.旁站验证 3.人员访谈	1.查阅关于针对各相关方数据权限分配的授权审批相关文件和工作材料，确认相关文件和工作材料中已建立数据权限使用、申请的评估机制。 2.查验并确认获得授权的各相关方数据权限的分配情况与审批文件相符。 3.访谈相关人员，确认数据权限分配流程合理合规。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
11	数据安全岗位人员应对本部门数据脱敏、对外提供等关键活动的数据安全控制有效性进行确认。	1.文档查验 2.旁站验证	1.查阅本部门数据脱敏、对外提供等关键活动相关文件、审批流程和工作材料，确认数据安全控制的有效性。 2.查阅并确认工作相关材料齐全、合规，至少包括数据使用规范，数据使用范围和权限、合规要求、使用安全防护要求、数据使用限制等。

序号	安全要求	评估方法	结果判定
			结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
12	数据安全岗位人员应配合执行数据相关安全评估及技术检测等工作。	1.文档查验 2.人员访谈	1.查阅关于配合执行数据相关安全评估及技术检测等工作的相关材料，确认能够证明其参与。 2.访谈相关人员，确认其能够配合执行数据相关安全评估及技术检测等工作。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
13	数据安全岗位人员应制定本部门数据安全应急预案，并定期开展数据安全应急演练，依据演练结果，修订数据安全应急预案。	1.文档查验	1.查阅关于制定本部门数据安全应急预案的相关文件，确认已在文件中明确负责数据安全事件应急响应的职责分工和应对流程等。 2.查阅开展数据安全应急演练的相关材料，确认其定期开展。 3.查阅数据安全应急预案修订相关文件，确认其为依据演练结果修订。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
14	数据安全岗位人员应做好处置本部门有关数据安全事件的相关工作。	1.文档查验 2.人员访谈	1.查阅关于数据安全事件处置的相关制度文件和工作流程，确认相关文件及流程中已明确本机构各部门应对不同等级数据安全事件的相关管理要求及应对措施。 2.查阅完成的数据安全事件处置的相关材料，确认材料齐全、合规。 3.访谈相关人员，确认其在处置本部门相关数据安全事件时严格按照相关制度和流程的规定履行职责。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
15	数据安全岗位人员应依据数据安全管理有关制度规范，记录本部门数据活动日志。	1.文档查验	1.查验本部门数据活动的日志记录，确认日志中记录的用户相关数据活动符合数据安全管理相关制度规范。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
16	应明确安全审计、合规稽核、风险管理等相关岗位，作为数据安全管理的监督层。	1.文档查验	1.查阅关于设立数据安全管理监督层的相关制度文件，确认涉及到的岗位包括安全审计、合规稽核、风险管理等相关岗位，并确认存在这些岗位人员对数据生命周期各阶段的数据处理活动所进行安全审计、合规稽核、风险管理等方面的相关记录。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。

序号	安全要求	评估方法	结果判定
17	应根据本机构数据相关业务实际情况，确定相应审计策略及规范，至少包括审计周期、审计方式、审计形式等内容。	1.文档查验	1.查阅审计策略和规范的相关制度文件，确认文件中已明确相关业务的审计策略和规范，并至少包括审计周期、审计方式、审计形式等内容。 2.查阅并确认审计内容与审计策略、规范相匹配。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
18	应监督数据安全政策、方针的执行。	1.文档查验 2.人员访谈	1.查阅数据安全政策、方针的执行情况相关监督工作制度和记录材料，并确认相关政策、方针的执行得到有效监督。 2.访谈相关人员，确认相关监督工作的合规、有效落地情况。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
19	应公布投诉、举报方式等信息，并及时受理数据安全和隐私保护相关投诉和举报。	1.文档查验 2.人员访谈	1.查阅关于受理数据安全和隐私保护相关投诉和举报相关材料，确认相关工作流程明确、规范、合理。 2.查阅并确认所公布的投诉和举报方式合法、合理。 3.访谈相关人员，确认能够及时受理相关投诉和举报，态度和善，处理高效。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
20	应开展数据安全内部审计和分析，发现并反馈问题和风险，并对机构后续相关整改工作进行监督。	1.文档查验	1.查阅关于开展数据安全内部审计和分析的相关文件，确认工作流程合理合规，并根据问题发现和风险反馈的相关材料及其后续整改工作的相关材料，确认对整改工作进行了有效监督。 2.查阅制度文件并确认已建立整改规范，用于指导发现和整改情况的追踪、报告管理、问题管理等。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
21	应配合开展外部审计相关的组织和协调工作。	1.文档查验	1.查阅相关制度文件和工作记录材料，确认具备配合开展外部审计相关的工作组织和工作规定。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。

6.2 制度体系建设 S1-2

6.2.1 总体规划

总体规划情况评估内容见表 6.2.1。

表 6.2.1 总体规划情况评估内容

序号	安全要求	评估方法	结果判定
1	应依据国家与行业主管和监管部门要求，结合机构自身风险管控策略和偏好、安全建设预算等因素，制定本机构数据安全总体安全策略、方针、目标、原则。	1.文档查验	1.查阅本机构数据安全总体规划相关制度文件，确认该文件的制定是在依据国家与行业主管和监管部门要求的同时，结合本机构自身风险管控策略和偏好、安全建设预算等因素所制定，包括本机构数据安全总体安全策略、方针、目标、原则。 2.查阅并确认总体规划整体上明确了数据安全管理的目标、原则、需要执行的活动、所需资源、支持岗位、时间安排和实施步骤等。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	应制定本机构数据分级规程，识别并维护本机构数据资产清单，并标注相应的数据级别。	1.文档查验	1.查阅本机构数据分级规程的相关制度文件，确认相关文件中结合数据类型特点、业务运营需求等对数据安全分级原则、方法、流程等进行了明确。 2.查阅本机构的数据资产清单，确认已对相应的数据安全级别进行了标注。 3.查阅本机构数据资产清单的维护记录，确认数据资产维护事由、频率等合理合规。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
3	应制定数据安全管理制度及实施细则并定期评价更新，确保基于数据分级的数据安全制度体系覆盖机构数据全生命周期，并对有关制度的有效性进行定期评价与更新。	1.文档查验	1.查阅本机构数据安全管理规定和数据安全生命周期保护工作相关制度文件，确认基于数据分级的数据安全制度体系覆盖本机构数据全生命周期。 2.查阅对相关制度规定的有效性进行定期评价和更新的相关材料，确认评价周期、更新频率及事由等合理合规。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	应建立数据安全评估、个人金融信息安全影响评估以及内外部数据安全检查与评估制度。	1.文档查验	1.查阅数据安全评估、个人金融信息安全影响评估以及内外部数据安全检查与评估制度及其工作记录材料，确认具备各项工作的内容、要求、流程等相关规定。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。

6.2.2 技术管理

技术管理情况评估内容见表 6.2.2。

表 6.2.2 技术管理情况评估内容

序号	安全要求	评估方法	结果判定
1	应制定数据安全管理实施细则，并应定期审核和更新金融数据安全管理制度。	1.文档查验	1.查阅相关制度文件，确认具备数据安全管理实施细则。 2.查阅实施细则评价和更新相关记录材料，确认定期对其进行评价更新的情况。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	应针对不同安全级别的数据，制定相应的安全策略和保障措施。	1.文档查验	1.查阅相关制度文件，确认具备数据安全保护策略及保障措施的制定情况和具体要求。 2.查阅相关制度文件和记录材料，确认分别针对不同安全级别的数据制定了相应的安全保护策略及保障措施。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	应建立数据安全日常管理及操作流程，对数据生命周期各阶段的数据保护工作提出具体要求。	1.文档查验 2.旁站验证	1.查阅数据安全日常管理和操作流程的相关文件，确认已对数据生命周期各阶段的数据保护工作制定具体要求。 2.采用旁站验证的方式，确认在数据生命周期各阶段中，各数据级别对应的数据保护策略得以有效落实。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	应建立合理、统一的密码使用和密钥管理技术规范和制度。	1.文档查验 2.人员访谈	1.查阅密码使用和密钥管理技术规范和制度、日志记录等相关材料，确认本机构密码技术应用机制合理、统一规范使用。 2.访谈相关人员，确认密码使用和密钥管理符合相关制度规定。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	应建立数据脱敏技术规范和制度，明确不同安全级别数据脱敏规则、脱敏方法和脱敏数据的使用限制。	1.文档查验 2.配置核查 3.旁站验证	1.查阅数据脱敏技术规范和制度相关文件，确认内容至少包括相关部门的管理职能、数据脱敏的工作流程、不同安全级别数据脱敏规则、脱敏方法和脱敏数据的使用限制等。 2.查验脱敏数据识别和脱敏效果验证服务组件或技术手段的配置相关参数和材料，确认数据脱敏的有效性和合规性。 3.查验数据脱敏操作过程中留存的日志记录等相关材料，确认不存在违规使用脱敏技术的情况。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
6	应建立第三方机构管理制度。	1.文档查验	1.查阅第三方机构管理制度的相关文件，确认第三方机构管理制度有效落地执行。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第1项。 不符合：不满足以上第1项。
7	应建立数据供应方安全管理要求，确定数据来源合法合规，对数据的真实性、有效性进行管理。	1.文档查阅	1.查阅数据供应方安全管理的相关文件，确认其内容至少包括确定数据来源合法合规、对数据的真实性和有效性进行管理等。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
8	应建立数据出境安全控制要求与操作程序。	1.文档查验	1.查阅数据出境安全控制要求与操作程序的相关文件，确认其至少包括检查数据出境审批操作、审批流程等。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
9	应建立数据采集、传输、存储、使用、删除及销毁相关审核规程和数据采集的操作规程，宜采用电子化手段实现审核流程。	1.文档查验 2.旁站验证	1.查阅数据采集、传输、存储、使用、删除及销毁等操作流程和审核规程的相关文件，确认其完整性。 2.查阅数据采集的操作规程，确认内容至少包括规范数据采集的渠道、数据格式、流程和方式。 3.旁站验证数据采集、传输、存储、使用、删除及销毁等操作和审核的日志记录，确认数据相关操作合规。 4.查阅相关设计文档，并结合旁站验证，确认相关规程及操作已采用电子化手段审核流程。（可选项） 结果评价： 符合：满足以上第1至3项或第1至4项。 不符合：不满足以上第1至3项中的一项或多项。
10	应建立数据安全事件管理、处置规程和应急响应等机制，明确重大数据安全事件的处置流程及应对方法。	1.文档查验	1.查阅相关制度文件及记录材料，确认已明确数据安全事件管理、处置规程和应急响应等机制。 2.查阅相关制度文件及记录材料，确认已明确重大数据安全事件的处置流程及应对方法。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
11	在本机构组织架构发生重大调整或数据相关服务发生重大变化时，应及时对金融数据安全策略与规程进行评估，并按需进行修订和更新。	1.文档查验	1.查阅相关记录，确认本机构组织架构重大调整或数据相关服务重大变化情况。 2.查阅以上重大调整及重大变化发生后相关制度评估、修订及更新相关记录，确认及时对金融数据安全策略与规程进行评估，并按需进行修订和更新。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
12	应建立工程环节数据安全管理制度。	1.文档查验	1.查阅并确认具备数据安全工程环节相关管理实施细则。

序号	安全要求	评估方法	结果判定
			2.查阅实施细则评价和更新相关记录材料，确认定期对其进行评价更新的情况。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

6.2.3 人员管理

人员管理情况评估内容见表 6.2.3。

表 6.2.3 人员管理情况评估内容

序号	安全要求	评估方法	结果判定
1	应在录用员工前，对其进行必要的背景调查。	1.文档查验	1.查阅相关管理制度及相关调查记录材料，确认在录用数据安全管理相关人员前已对其开展背景调查。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
2	应对数据安全关键岗位制定统一的保密协议，并与可接触机构3 级及以上数据的员工以及从事数据安全关键岗位的员工签署保密协议。	1.文档查验	1.查阅数据安全关键岗位相关的保密协议范本，对保密要求的统一性进行确认。 2.查阅已签署的保密协议，确认已与可接触机构3级以上数据的员工以及从事数据安全关键岗位的员工签署保密协议。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	应识别机构数据安全关键岗位，并与其签署数据安全岗位责任协议。	1.文档查验	1.查阅并确认数据安全关键岗位的名单，至少包括数据安全管理岗位、审计岗位、业务操作与信息技术操作特权账户所有者、数据各级权限审批岗位、重要数据处理岗位、信息系统主要开发、测试岗位人员、因业务需要需高频或大批量接触3级及以上数据的岗位人员、外部数据采购岗位以及本机构已识别的其他数据安全关键岗位。 2.查阅并确认与数据安全关键岗位人员，均已签署数据安全岗位签署责任协议。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	应在发生人员调离岗位时，立即完成相关人员数据访问、使用等权限的配置调整，并明确有关人员后续的数据保护管理权限和保密责任；若有关人员调整后的岗位不涉及数据的访问与处理的，应明确其继续履行有关信息的保密义务要求。	1.文档查验 2.旁站验证	1.查阅相关材料，确认在发生人员调离岗位时，对相关人员的数据访问、使用等权限配置已进行调整。 2.查阅相关材料，确认相关人员后续的数据保护管理权限配置和保密责任。 3.查阅相关材料，确认调岗人员继续履行相关信息保密义务的情况。 4.旁站验证相关人员的数据访问和使用等权限配置调整参数和日志记录，确认操作与相关制度规定相符。

序号	安全要求	评估方法	结果判定
			结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
5	在与员工终止劳动合同时，应立即终止并收回其对数据的访问权限，明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书。	1.文档查验 2.旁站验证	1.查阅员工终止劳动合同时的相关材料，确认具备保密承诺书等约束其继续履行有关信息保密义务的文件。 2.查阅与员工签订的保密承诺书，确认内容至少包括明确告知其继续履行相关信息的保密义务要求。 3.旁站验证并确认及时终止并收回已终止劳动合同员工的数据访问权限。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
6	应建立外部人员管理制度，对允许被外部人员访问的系统和网络资源建立数据存取控制机制、认证机制，列明所有外部用户名单及其权限，加强对外部人员的数据安全要求和培训，必要时签署保密协议。	1.文档查验 2.旁站验证	1.查阅并确认具备外部人员管理制度的相关文件。 2.查阅相关材料，确认已明确外部人员数据安全要求、开展培训，并在必要时签署保密协议。 3.旁站验证并确认允许外部人员访问的信息系统和网络资源具备相应的数据存取控制机制、认证机制，以及所有外部用户名单及其权限。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
7	应做好数据安全相关岗位人员的安全专项培训相关工作。	1.文档查验 2.人员访谈	1.查阅对数据安全相关岗位人员制定的安全专项培训计划的相关材料，确认培训内容至少包括安全意识、岗位技能、能力拓展等。 2.查阅按照培训计划定期开展数据安全意识教育与培训的相关材料，确认培训内容至少包括国家相关法律法规、行业规章制度、技术标准，以及金融业机构内部数据安全相关制度与管理规程等。 3.查阅对密切接触高安全等级数据的人员定期开展数据安全意识教育和培训的相关材料，确认培训内容至少包括国家相关法律法规、行业规章制度、技术标准，以及金融业机构内部数据安全相关制度与管理规程、岗位数据安全意识及技能培养等。 4.查阅并确认员工对培训结果的评价和记录等相关材料的留存。 5.访谈相关员工，确认开展的教育和培训能够达到预期的效果。 结果评价： 符合：满足以上第1至5项。 不符合：不满足以上第1至5项中的一项或多项。

序号	安全要求	评估方法	结果判定
8	应对数据安全管理专职与关键岗位人员开展培训和考核。	1.文档查验 2.人员访谈	1.查阅相关材料，确认每年至少开展一次对数据安全管理专职与关键岗位人员的数据安全专项培训。 2.查阅相关材料，确认在隐私政策发生重大变化时，对数据安全关键岗位人员开展专业化培训和考核。 3.访谈数据安全关键岗位人员，确认开展的专业化培训和考核能够达到预期的效果。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
9	应对数据库管理员、操作员及安全审计人员等岗位设立专人专岗，并实行职责分离；必要时应对特权账户所有者、关键数据处理岗位等数据安全关键岗位应设立双人双岗。	1.文档查验	1.查阅相关材料，确认对接触高安全等级金融数据的人员及其岗位进行审批和登记。 2.查阅相关材料，确认定期对数据库管理员、操作员及安全审计人员等岗位人员行为进行安全审查。 3.查阅数据库管理员、操作员和安全审计人员等岗位职责的相关材料，确认设立专人专岗，并实行职责分离。 4.查阅特权账户所有者、关键数据处理岗位等数据安全关键岗位的岗位职责相关材料，确认在必要时设立双人双岗。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。

6.2.4 合作管理

与第三方机构（包括外包服务机构与外部合作机构）的合作管理评估内容见表6.2.4。

表6.2.4 合作管理情况评估内容

序号	安全要求	评估方法	结果判定
1	应建立第三方机构审查与评估机制，评估其数据安全保护能力。	1.文档查验	1.查阅第三方机构管理制度，确认具备第三方机构审查与评估相关要求。 2.查阅第三方机构审查与评估报告，确认其数据安全保护能力达到国家、行业主管部门与金融业机构的要求。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	第三方机构应具备一定的资质要求。	1.文档查验	1.查阅并确认具备第三方机构及人员相关数据安全管理资质证明材料及审核记录文件。 2.查阅第三方机构数据安全保护能力合规性评估记录或报告，确认其具备与所开展合作事项相应的数据安全保护机制及运营资质要求。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

序号	安全要求	评估方法	结果判定
3	应通过合同协议等方式，对第三方机构的数据使用行为进行约束，并明确双方在数据安全方面的责任及义务，并明确第三方机构应具备的数据安全保护能力要求。	1.人员访谈 2.文档查验	1.查阅与第三方机构签订的各项合同协议，至少包括： 1）查阅合同协议，确认已明确第三方机构不能留存3级及以上数据。对第三方机构确需留存3级及以上数据的情况，合同协议中应明确标注留存依据，确认已明确第三方机构的保密义务和保密责任。 2）查阅合同协议，确认已明确本机构委托第三方机构加工处理数据行为约束要求。 3）查阅合同协议，确认已明确合同关系解除后，第三方机构不再以任何方式保存从金融业机构获取的数据及相关衍生数据。若涉及向用户直接提供服务的第三方产品或服务，应在与第三方机构解除合作关系时，将金融业机构解除与第三方机构合作关系明确告知用户。 4）查阅与第三方机构及人员签订的保密协议，并确认已明确对该协议履行情况进行监督的相关要求。 5）查阅并确认已在协议中明确双方安全责任及义务分工。 6）查阅并确认已在协议中就第三方机构应具备的数据安全保护能力要求进行明确。 2.对第三方机构确需留存3级及以上数据的情况，查阅并确认具备留存依据、数据安全措施及第三方机构的保密协议。 3.查阅授权材料并进行相关人员访谈，确认第三方机构进行数据存储、使用和共享操作时已得到本机构书面授权。 4.查阅相关资料，确认第三方机构保存的数据到期或解除合作时，第三方机构已签署相关删除协议、履行数据删除责任，并确认金融业机构对相关工作进行检查的相关要求和执行情况。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
4	对可能访问金融业机构数据的第三方机构及人员，金融业机构应要求第三方机构向有关人员传达金融业机构数据安全要求，与其签署保密协议，并对协议履行情况进行监督。	1.人员访谈 2.文档查验	1.查阅涉及数据访问的第三方机构及人员列表清单，查阅对第三方机构人员的安全教育、书面协议等资料，通过与第三方机构人员访谈，了解第三方机构及人员对本机构数据安全要求的掌握情况，确认数据安全教育培训达到预期效果。 2.查验并确认第三方机构与有关人员全部签署保密协议。 3.建立协议落实情况监督制度，查验监督材料，并确认保密协议与监督要求的履行和落实情况。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
5	应对第三方机构进行监督，定期对第三方机构的数据安全保护措施落实情况进行确认。	1.文档查验 2.旁站验证	1.查阅第三方产品或服务合同协议，确认双方已明确在数据安全方面的责任及义务，并明确第三方机构应具备的数据安全保护能力要求。

序号	安全要求	评估方法	结果判定
			2.查阅安全检查和评估资料，确认第三方机构的责任和义务落实到位。 3.查阅第三方机构管理制度，确认已采用书面形式明确对第三方机构的数据安全保护措施落实情况的具体要求，包括确认频率、确认方式等。 4.查阅外部信息安全评估报告、现场检查资料，确认第三方机构数据安全保护措施有效落实，对发现的问题应及时督促整改，并留存监督检查结果及问题整改情况书面记录。 5.查阅设计文档并查验相关信息系统，确认不存在包括3级及以上数据的数据库交由外部合作机构运维的情况。 6.查阅第三方产品或服务合同协议，确认第三方机构在处理数据过程中发生数据安全事件的处置流程和方式。 结果评价： 符合：满足以上第1至6项。 不符合：不满足以上第1至6项中的一项或多项。
6	第三方机构应及时反馈在处理数据过程中发生的数据安全事件。	1.文档查验	1.查阅数据安全事件处置资料，确认第三方机构按照双方约定的处置流程和方式开展数据安全事件处置，并及时向本机构反馈。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
7	应对接入和涉及的第三方产品和服务进行专门的数据安全管理，确保不因第三方的应用接入而危害机构数据安全。	1.文档查验 2.配置核查 3.旁站验证	1.查阅第三方机构管理制度，确认已采用书面形式明确第三方产品或服务接入的基本条件。 2.查阅第三方产品或服务的接入安全评估报告，确认接入的产品或服务采取的风险控制措施能够有效防范接入风险。 3.查验第三方产品和服务接入管理系统，确认在接入端进行严格接入认证，配置安全控制策略，采取安全风险管控措施。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
8	应对第三方接入产品和服务的数据处理活动进行必要的监视。	1.文档查验	1.查阅并确认具备第三方嵌入或接入的自动化工具的功能和安全性检验报告。 2.查阅第三方接入产品和服务的数据处理活动日志记录、审计或检查报告，确认落实安全管理要求和责任，并能对第三方接入产品和服务的数据处理活动进行必要的监视。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
9	第三方产品或服务应具备清晰标识。	1.旁站验证	1.查验向用户直接提供服务的第三方产品或服务接入信息系统，确认界面明确标识产品或服务的提供方。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第1项。 不符合：不满足以上第1项。
10	发生违规行为或安全事件应执行相应的事件处置程序，并报告监管部门。	1.文档查验	1.查阅并确认具备第三方接入产品和服务监视记录和安全事件处置流程，确保违规行为发生时能够及时发现并切断，并执行安全事件处置程序。 2.查阅安全事件书面报告，确认其至少包括事件的发生、分析及处置记录。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
11	对于数据供应方，应通过制度要求、合同协议、技术手段等方式确保数据来源合法合规性、真实性和有效性。	1.文档查验	1.查阅数据安全管理制度，确认已明确数据供应方安全管理要求，要求数据供应方说明数据来源，并明确数据采集过程中个人金融信息和重要数据的知悉范围和安全管控措施。 2.查阅数据供应方资质审核材料、数据采购协议等相关文件，确认具备相关要求并采取措施确保数据来源合法合规、真实有效。 3.查阅数据采集日志，确认数据来源相关记录与事先约定的情况保持一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
12	对于数据供应方，应制定数据供应方约束机制，保证数据合法合规以及保护措施有效性。	1.文档查验	1.查阅数据供应方约束管理制度，确认已明确数据源、数据采集范围和频度，并事前开展数据安全影响评估。 2.查阅数据评估报告等相关证明材料，确认已对数据的真实性、准确性、合法合规情况以及数据保护措施等开展评估。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
13	与第三方机构解除合作关系时，应要求第三方机构不再以任何方式保存从金融业机构获取的数据及相关衍生数据，国家及行业主管部门另有规定的除外；若涉及向用户直接提供服务的第三方产品或服务，应在与第三方机构解除合作关系时，明确告知用户金融业机构已解除与第三方机构合作关系。	1.文档查验	1.查阅合同等相关协议文件，确认与第三方机构解除合作关系相关条款规定内容符合要求。 2.查阅相关合同等协议条款，确认涉及向用户直接提供服务的第三方产品或服务时，履行用户告知义务。 3.查阅第三方解除合作关系相关记录文件，对以上内容的实际执行情况进行确认。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。

6.2.5 流程管理

流程管理情况评估内容见表6.2.5。

表6.2.5 流程管理情况评估内容

序号	安全要求	评估方法	结果判定
1	应建立数据安全管理制度体系，明确相关部门与岗位数据安全工作职责，规范工作流程。	1.文档查验	1.查阅本机构数据安全管理体系建设相关文档，确认相关制度体系已覆盖本机构数据安全管理工作相关技术、人员、制度等各个方面，且相应制度至少包括数据安全管理工作的战略总则、基本方针、管理要求、实施指南、工作流程等内容。 2.查阅数据安全管理实施细则，确认已覆盖数据生命周期各个阶段的数据保护工作具体要求。 3.查阅数据安全日常管理及操作流程相关文件，确认已明确相关部门与岗位职责，并对数据生命周期各阶段的数据保护工作提出具体要求。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
2	应建立数据安全事件管理、处置规程和应急响应等机制，明确处置流程及应对方法。	1.文档查验	1.查阅数据安全事件管理制度，确认已根据数据安全事件严重程度或等级制定相应的处置规程。 2.查阅数据安全事件应急响应制度，确认已明确数据安全事件应急响应牵头部门及相关执行部门的工作职责、数据安全事件发现及报告机制等要求。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	应建立数据采集、传输、存储、使用、删除及销毁相关审核规程。	1.文档查验 2.旁站验证	1.查阅并确认具备数据采集、传输、存储、使用、删除及销毁相关审核制度。 2.如有审核规程电子化系统，应上机查验并确认系统流程覆盖数据生命周期的各个阶段，并对其与相应制度规定的一致性进行确认。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

7 金融数据安全保护评估 S2

7.1 数据资产分级管理评估 S2-1

数据资产分级管理情况评估见表7.1.1。数据资产清单相关示例参见附录A。

表 7.1.1 数据资产分级管理情况评估内容

序号	安全要求	评估方法	结果判定
1	应建立数据安全分级相关制度，明确数据分级中的具体工作内容。	1.文档查验	1.查阅数据安全管理制度，确认具备数据安全分级相关制度。 2.查阅数据安全分级实施相关制度文件，确认包括数据安全分级实施工作具体工作内容相关材料。 3.查阅数据安全分级工作的相关材料，确认至少包括数据分级目标和原则、涉及的角色、部门及职责、分级方法和具体要求、

序号	安全要求	评估方法	结果判定
			日常管理流程和操作规程、相关绩效考核和评价机制、分级结果的发布、备案和管理规定以及数据分级结果审核与修订的原则和周期等内容。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
2	数据安全分级结果应由数据安全管理最高决策组织进行审议批准。	1.文档查验	1.查阅数据安全级别评定过程及结果的审核资料，确认符合法律法规及内部制度相关要求。 2.查阅并确认具备数据安全管理最高决策组织对数据安全分级进行审议批准的相关材料。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	应对数据进行盘点、梳理与分类，形成统一的数据资产清单。	1.文档查验 2.旁站验证	1.查阅数据资产盘点相关工作材料，确认包括数据资产梳理工作相关内容。 2.查阅数据资产清单，确认清单内容至少包括数据类型、数据级别等相关内容。 3.查阅数据资产清单及相关材料，确认材料内容完备、及时，且至少包括数据类型、功能、数据级别、数据承载介质等，数据资产清单示例参见附录A。 4.查阅数据资产清单和数据资产梳理相关资料，确认数据资产梳理和资产清单已覆盖当前评估范围，如提供金融产品或服务过程中直接（或间接）采集的电子数据；本机构信息系统内生成和存储的数据；本机构内部办公网络与办公设备（终端）中产生、交换、归档的电子数据；本机构原纸质文件经过扫描或其他电子化手段形成的电子数据；其他应纳入数据资产管理的电子数据等。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	应定期梳理数据资产并及时更新数据资产清单。	1.文档查验	1.查阅数据安全管理制度，确认已明确数据资产定期梳理和更新要求，并已明确数据梳理更新的条件和频率。 2.查阅数据资产清单更新记录，确认已对数据资产使用、留存及报废等状态进行登记，并能做到定期更新。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	应将数据安全性遭到破坏后可能造成的影响作为确定数据安	1.文档查验	1.查阅数据安全相关制度文件，确认数据安全级别确定重要依据包括数据安全性遭到破坏后可能造成的影响相关内容。

序号	安全要求	评估方法	结果判定
	全级别的重要依据，将数据从高到低进行级别划分。		2.查阅数据安全分级相关制度文件，确认已对数据级别划分要求及数据从高到低进行划分做出具体规定。 3.查阅数据安全相关制度文件，确认包括数据安全分级的规则，且定级过程充分考虑数据类型、数据内容、数据规模、数据来源、本机构职能和业务特点等因素，并在此基础上结合数据安全性（保密性、完整性、可用性）遭受破坏后所造成的影响评估情况，来进行数据安全级别划分。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
6	应制定明确的定级规则，根据规则完成对数据资产的定级。	1.文档查验	1.查阅数据安全定级规则相关规定，参照JR/T 0197—2020，对数据安全分级规则合理性进行确认。 2.查阅数据资产清单及数据安全分级相关记录材料，确认数据定级结果与本机构数据安全定级规则的一致性。 3.查阅数据资产清单，确认对于数据体量大，涉及的客户（包括个人客户和单位客户）多、涉及客户（包括个人客户和单位客户）资金量大、涉及多行业及多机构客户的情况，其影响程度、安全级别等已从高确定。 4.查阅数据安全定级规则，及数据安全分级结果，确认重要数据的安全等级不可低于5级。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
7	应制定数据安全定级流程和具体操作步骤，以制度规程形式发布。	1.文档查验	1.查阅数据安全管理制度，确认已包括数据安全定级规程，且至少包括数据安全定级流程和具体操作步骤。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
8	应根据规范流程实施数据安全定级工作。	1.文档查验	1.查阅数据定级过程相关记录文档，确认定级流程至少包括“数据资产梳理-数据安全定级准备-数据安全级别判定-数据安全级别审核-数据安全级别批准”等基本步骤。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
9	应对符合变更条件的数据按照定级流程实施级别变更。	1.文档查验 2.旁站验证	1.查阅数据级别变更记录，确认已对原有数据安全级别不再适用现有数据做到及时、规范地实施定级变更，且变更事由至少包括法律法规所要求的、数据应用场景发生较大变化的、数据处理方式发生较大变化的、本机构信息系统架构等发生重大调整的、本机构发生重大数据安全事件的等情况。

序号	安全要求	评估方法	结果判定
			2.查阅数据定级文档及变更记录，确认数据变更按照数据安全定级流程要求执行。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

7.2 数据生命周期安全评估 S2-2

7.2.1 概述

依据JR/T 0197-2020、JR/T 0223-2021，梳理数据流，并结合数据资产清单及数据分级情况，对业务必须最小数据集、生命周期各环节的数据活动安全合规情况进行分析和判断，对数据生命周期各环节数据安全保护措施的落地情况及其有效性进行验证，形成数据生命周期安全防护分析表，见附录B。

7.2.2 数据采集

7.2.2.1 从外部机构采集数据

从外部机构采集数据安全评估内容见表7.2.1。

表7.2.1 从外部机构采集数据安全评估内容

序号	安全要求	评估办法	结果判定
1	应通过合同协议等方式，明确双方在数据安全方面的责任及义务，明确数据采集的范围、频度、类型、用途等，确保外部机构数据的合法合规性和真实性，必要时提供相关个人金融信息主体的授权。	1.人员访谈 2.文档查验 3.旁站验证	1.查阅合同协议等约定条款，确认已书面明确双方数据保护责权划分，并确认外部机构已提供具有法律效力的数据来源合法合规性承诺证明。 2.查阅合同协议等约定条款，确认已书面明确数据采集的范围、频度、类型、用途、数据保护措施、数据使用期限及到期后数据处理方式。 3.访谈相关人员，确认本机构已明确在何种情况下，会要求外部机构提供个人金融信息主体授权。 4.查验并确认外部机构提供的个人金融信息主体授权方式、授权内容与实际数据采集实现情况完全一致。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1、2、4项。 不符合：不满足以上第1、2、4项中的一项或多项。
2	从外部数据供应方处采集数据，应制定数据供应方约束机制，并明确数据源、数据采集范围和频度，并事前开展数据安全影响评估。	1.人员访谈 2.文档查验	1.查阅数据安全相关制度，确认已明确数据供应方约束要求，并对数据源、数据采集范围和频度以及开展事前数据安全评估提出具体要求。 2.查阅并确认已制定数据安全影响评估的规范，并在规范中明确开展数据安全影响评估的启动条件、流程、内容、风险等级划分、风险级别与结论、改进建议、报告编制等。其中，评估内容包括外部数据及其数据源的真实性、合法性与正当性，采集的范围、频度、类型和用途合理性和必要性，安全保护措施

序号	安全要求	评估办法	结果判定
			有效性，一旦发生数据安全事件可能给相关方合法权益造成的损害及该损害发生的可能性等。 3.查阅数据安全影响评估报告，访谈相关人员，确认事前开展相关评估，且评估过程符合数据安全影响评估规范。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
3	采集的企业客户数据应与提供的金融产品或服务直接相关，并与合同协议条款、隐私政策中约定采集的内容保持一致，不应超范围采集数据。	1.文档查验 2.旁站验证	1.查阅合同协议，确认已明确向企业客户提供的金融产品或服务具体内容。 2.查验并确认采集的企业客户数据均与所提供金融产品或服务直接相关。 3.查验并确认采集的企业客户数据与合同协议条款、隐私政策中约定采集的内容完全一致，未超范围采集数据。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
4	应明确数据采集过程中个人金融信息和重要数据的知悉范围和安全管控措施，确保采集数据的合规性、完整性和真实性。	1.人员访谈 2.文档查验 3.旁站验证	1.查阅数据安全相关制度，确认已明确采集过程中个人金融信息和重要数据的知悉范围和安全管控措施。 2.访谈相关人员并查阅相关记录文档，确认采集的个人金融信息和重要数据的知悉范围与制度要求一致，不存在超知悉范围采集数据。 3.查验并确认数据采集过程中个人金融信息和重要数据的安全管控措施及其实际有效性。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
5	通过系统批量采集的数据应采用摘要、消息认证码、数字签名等密码技术确保采集过程数据的完整性。	1.文档查验 2.配置核查 3.工具测试 4.旁站验证	1.查阅批量采集数据相关信息系统的设计和实施相关文档，确认已采取摘要、消息认证码、数字签名等密码技术保障采集过程数据的完整性。 2.查验并确认采集数据相关信息系统已采用摘要、消息认证码、数字签名等密码技术保障采集过程数据的完整性。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
6	应对人工批量采集数据的环境进行安全管控，并通过人员权限管控、信息碎片化等方式，防止采集过程出现数据泄露。	1.人员访谈 2.文档查验 3.配置核查 4.旁站验证	1.查阅数据安全相关制度，确认已对人工批量采集数据环境的数据防泄漏等安全管控做出相关规定。 2.查验并确认数据采集过程中已采用数据防泄露技术手段及对人工批量采集数据的环境已采用安全管控措施，并确认其与相关安全制度规定内容一致。 3.查验并确认人工批量采集数据环境安全管控措施的有效性。 4.查验人工批量采集数据的相关信息系统，确认已采用人员权

序号	安全要求	评估办法	结果判定
			限设置、信息碎片化等方式，防止采集过程出现数据泄漏。 结果评价： 符合：满足以上第 1 至 4 项。 不符合：不满足以上第 1 至 4 项中的一项或多项。
7	采集数据时，应对数据采集设备或系统的真实性进行验证。	1.文档查验 2.工具测试 3.旁站验证	1.查阅数据采集设备或信息系统的相关建设文档，确认该设备或信息系统具有身份识别、数字证书等鉴别技术，以确保设备或信息系统的真实性。 2.查验并确认采集设备或信息系统具有鉴别真实性的功能或技术。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
8	应对数据采集过程进行日志记录，并采取技术措施确保信息来源的可追溯性。	1.文档查验 2.工具测试 3.旁站验证	1.查验并确认数据采集设备或信息系统已具有日志记录的功能。 2.抽样查验数据采集过程的日志记录，确认已记录所采集数据的提供方、采集时间、采集方式等，确保采集数据的可追溯性。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
9	采集 3 级及以上数据时，还应结合口令密码、设备指纹、设备物理位置、网络接入方式、设备风险情况等多种因素对数据采集设备或系统的真实性进行增强验证。	1.文档查验 2.工具测试 3.旁站验证	1.查阅采集3级及以上数据的设备或信息系统的设计和实施相关文档，确认该设备或信息系统具有增强验证功能。 2.查验采集3级及以上数据的设备或信息系统，确认可进行增强验证。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
10	采集 4 级数据时，还应满足： 1)对采集全过程进行持续动态认证，确保数据采集设备或系统的真实性，必要时可实施阻断、二次认证等操作。 2)对采集的数据进行数据加密。 3)不应通过人工方式采集。	1.人员访谈 2.文档查验 3.工具测试 4.旁站验证	1.查阅采集4级数据的设备或信息系统的相关建设文档，确认具备在采集全过程进行持续动态认证的相关要求(防范因认证过期未及时断连、单次认证有效期限过长等验证机制自身脆弱性问题带来的数据安全风险)，并已明确采集4级数据的加密方式。 2.查验并确认已明确采集4级数据时使用实时阻断和二次认证等操作的必要情形，并确认其操作有效性。 3.查验并确认采集4级数据的设备或信息系统对采集全过程可进行持续动态认证。 4.查验并确认数据采集设备或信息系统对采集的4级数据进行加密。 5.访谈相关人员，了解4级数据采集方式，确认未通过人工方式采集。 结果评价： 符合：满足以上第1至5项。

序号	安全要求	评估办法	结果判定
			不符合：不满足以上第1至5项中的一项或多项。

7.2.2.2 从个人金融信息主体采集数据

从个人金融信息主体采集数据安全评估内容见表7.2.2。

表7.2.2 从个人金融信息主体采集数据安全评估内容

序号	安全要求	评估办法	结果判定
1	APP、WEB 等客户端相关业务完成后不应留存 3 级及以上数据，并及时对缓存进行清理。	1.文档查验 2.工具测试 3.旁站验证	1.查阅处理个人金融信息的APP、WEB等客户端相关建设文档，确认已明确不留存3级及以上数据的方案和及时清理缓存的方案。 2.查验并确认APP、WEB客户端在完成相关业务后未留存3级及以上数据，且在业务完成后能及时对缓存进行清理。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	采集的个人金融信息应与提供的金融产品或服务直接相关，并与合同协议条款、隐私政策中约定采集的内容保持一致，不应超范围采集数据。	1.人员访谈 2.文档查验 3.旁站验证	1.查阅合同协议，确认已明确向个人金融信息主体提供的金融产品或服务具体内容。 2.查验并确认采集的个人金融信息与提供的金融产品或服务直接相关，未采集无关信息。 3.查验并确认采集的个人金融信息与合同协议条款、隐私政策中约定采集的内容完全一致，未超范围、过量采集数据。 4.查验提供的金融产品清单，识别涉及个人金融信息采集的产品，选择不低于十分之一的产品，对近180天内的个人金融信息采集做抽样查验，确认不存在超范围、过量采集数据。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
3	通过纸质表单采集数据并转换为电子数据时，满足以下要求： 1)对表单的保存、查阅、复制等操作进行严格审批授权，涉及 3 级及以上数据的操作，应进行专项审批，并对表单流转的全过程进行监控与审计。 2)在纸质表单电子化的过程中，应采取技术措施对电子化过程中的数据完整性、保密性进行控制。	1.人员访谈 2.文档查验 3.旁站验证	1.查阅数据安全相关制度，确认已明确纸质表单管理机制，且机制设计合规。 2.查验并确认对纸质表单的保存、查阅、复制等操作均有审批记录，确认涉及3级及以上表单操作经由专人审批，且流转记录完整、审计记录合规。 3.查阅纸质表单电子化相关文档，确认存在保障数据完整性和保密性的技术措施和权限控制措施设计。 4.查验纸质表单电子化的权限控制情况，确认仅授权人员有电子化操作权限。 5.抽样查验并确认电子化后的数据类型、数据量、数据内容等与纸质表单数据完全一致。 结果评价： 符合：满足以上第1至5项。 不符合：不满足以上第1至5项中的一项或多项。

序号	安全要求	评估办法	结果判定
4	数据采集过程应符合表 7.2.1 第 4 至 10 项安全要求。	同表7.2.1第4至10项	同表7.2.1第4至10项
5	金融业机构在停止其提供的金融产品或服务时，应立即停止数据收集活动及数据分析应用活动，相关国家及行业主管部门另有规定的按照相关规定执行。	1.文档查验 2.旁站验证	1.查阅数据安全相关制度，确认已明确本机构在停止提供金融产品或服务时，立即停止数据收集活动及数据分析应用活动定的相关规定。 2.查阅本机构停止其提供的金融产品或服务相关资料，确认其数据活动与相关数据安全制度规定的内容完全一致。 3.查阅合同协议条款，确认关于本机构在停止提供金融产品或服务时应立即停止数据收集活动及数据分析应用活动的约定内容。 4.抽样查验相关系统日志，确认在停止对个人提供金融产品或服务后，立即采取措施停止数据收集活动及数据分析应用活动，且此后未进行此产品和服务相关的任何数据活动。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。

7.2.3 数据传输

数据传输安全评估内容见表7.2.3。

表7.2.3 数据传输安全评估内容

序号	安全要求	评估办法	结果判定
1	应加强软件开发安全管理，保障数据传输工具的安全性，工具上线前应开展必要的渗透测试、支持库漏洞查找等工作，以防止工具使用过程中遭受恶意破坏、功能篡改、信息窃取等攻击。	1.文档查验 2.工具测试	1.查阅数据安全相关制度，确认至少包括软件开发安全管理、数据传输工具安全管理，以及传输工具或信息系统上线前需开展渗透测试、漏洞扫描等安全检测等要求。 2.查阅数据传输工具或信息系统上线前开展的渗透测试、漏洞扫描等安全检查报告，确认报告的真实性，查验并确认相关安全漏洞与隐患已整改消除。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
2	应采用防火墙、入侵检测等安全技术或设备，确保数据传输网络的安全性。不同网络区域或安全域之间应进行安全隔离和访问控制。	1.配置核查 2.旁站验证	1.查验并确认已配备防火墙、入侵检测等网络安全设备或相关技术，且防火墙重点在网络边界部署，入侵检测的镜像流量涵盖网络内部和外部的所有流量。 2.查验并确认防火墙已配置合理有效的控制策略，入侵检测设备可检测异常攻击行为。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

序号	安全要求	评估办法	结果判定
3	终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入内部网络。	1.文档查验 2.配置核查 3.旁站验证	1.查阅并确认已部署终端安全管控系统设计文档，且具备准入控制、终端鉴别等功能。 2.查验并确认终端安全管控系统已配置相关安全策略。 3.查验并确认终端安全管控系统配置相关安全策略的有效性。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
4	应对通信双方进行身份认证，确保数据传输双方是可信任的。	1.配置核查 2.工具测试	1.查验并确认通信前均对双方进行身份认证。 2.进行通信方身份篡改等攻击试验，查验操作返回结果，确认数据传输采用身份认证技术且能够确保通信双方身份可信。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
5	应采用数字签名、时间戳等方式，确保数据传输的抗抵赖性。应采用密码技术或非密码技术等方式，确保数据的完整性。	1.文档查验 2.工具测试 3.旁站验证	1.查阅并确认设计文档中具备数据传输抗抵赖性、完整性保障措施及密码算法设计。 2.查验并确认已采用密码技术或非密码技术，以确保所传输数据的正确、完整性。 3.查验并确认数据传输时已采用数字签名和时间戳等抗抵赖技术。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
6	应选用安全的密码算法，禁用如MD5、DES-CBC、SHA1 等不安全的算法。	1.文档查验 2.工具测试 3.旁站验证	1.查阅数据安全相关制度，确认已明确禁用如 MD5、DES-CBC、SHA1等不安全的算法。 2.查验并确认数据传输已使用安全的密码算法，无上述不安全算法应用。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
7	2 级及以上数据的内部传输，应事先经过审批授权明确当前授权的范围、频次、有效期等，避免出现一次性授权、打包授权等情况。2 级及以上数据的对外传输，应事先经过审批授权并采取数据加密、安全传输通道或安全传输协议进行数据传输。	1.文档查验 2.工具测试 3.人员访谈	1.查阅数据安全相关制度，确认已明确2级及以上数据内部传输和对外传输的审批授权机制，且审批授权机制符合规定，已明确数据对外传输应采用的安全防护技术措施。 2.查验并确认2级及以上数据的对外传输已采取安全防护技术措施。 3.访谈相关人员，询问相关部门2级及以上数据对内传输和对外传输情况，抽样查验相关事项审批授权记录，确认授权范围、频次、有效期等内容正当合理，无一次性授权、打包授权等情况。 结果评价： 符合：满足以上第1至3项。

序号	安全要求	评估办法	结果判定
			不符合：不满足以上第1至3项中的一项或多项。
8	3 级及以上的数据内部传输，应采取数据加密、安全传输通道或安全传输协议进行数据传输。3 级及以上数据原则上不应对外传输，若因业务需要确需传输的，应经过事先审批授权，并采取技术措施确保数据保密性。	1. 文档查验 2. 工具测试 3. 旁站验证	1. 查阅数据安全相关制度，确认已明确3级及以上数据内部传输应采用的安全防护技术措施，并明确3级及以上数据原则上不应对外传输，确需对外传输的已明确审批授权机制，且明确相应安全防护技术措施。 2. 使用工具统计近180天内3级及以上数据对外传输记录，抽样查验相关事项审批授权记录，确认完全一致。 3. 查验并确认3级及以上数据的内部传输（跨物理区域、跨安全域等存在安全风险的场景）已采取安全防护技术措施，如数据加密、安全传输通道或安全传输协议等。 4. 查验并确认已采取技术措施监测并防止非授权的3级及以上数据对外传输。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
9	4 级及以上数据传输，应对数据进行字段级加密，并采用安全的传输协议进行传输。4 级数据中的个人金融信息原则上不应对外传输，国家及行业主管部门另有规定的除外。	1. 文档查验 2. 旁站验证 3. 人员访谈	1. 查阅数据安全相关制度，确认已明确4级及以上数据传输需对数据进行字段级加密，且使用安全的传输协议进行传输，并明确除国家及行业主管另有规定外，4级个人金融信息原则上不应对外传输。 2. 查验并确认4级及以上数据传输对数据字段进行加密，且使用安全的传输协议。 3. 查验并确认已采取技术措施监测并防止4级个人金融信息对外传输。 4. 查验并确认4级数据中没有对外传输个人金融信息的情况（国家及行业主管部门另有规定的除外）。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
10	应在数据传输不完整时清除传输缓存数据。应在数据传输完成后立即清除传输历史缓存数据。	1. 文档查验 2. 工具测试 3. 旁站验证	1. 查阅相关设计文档，确认已明确在数据传输不完整时以及数据传输完成后及时清除缓存数据的技术方案。 2. 使用工具测试并确认数据传输中断时的返回结果符合设计预期。 3. 至少选取三类业务系统，抽样查验并确认近1周内数据传输后的缓存数据未留存。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
11	应定期检查或评估数据传输的安全性和可靠性。	1. 文档查验	1. 查阅数据安全相关制度，确认已明确开展数据传输安全性和可靠性检查或评估的周期。

序号	安全要求	评估办法	结果判定
			2.查阅并确认已制定数据传输安全评估规范，明确开展评估的启动条件、流程、内容、风险等级划分、风险级别与结论、改进建议、报告编制等。 3.查阅数据安全评估报告，确认已明确评估形式、评估内容和范围、评估结果及评估真实性，同时针对评估中发现的问题制定了整改计划。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
12	向国家机关、行业主管和监管单位传输数据，应按照国家及行业相关管理要求进行传输。	1.文档查验 2.旁站验证	1.查阅数据安全相关制度，确认已明确向国家机关、行业主管和监管单位传输数据时需要遵照的国家及行业相关管理要求。 2.查验并确认在向国家机关、行业主管和监管单位传输数据时，按照国家及行业相关管理要求做好相关保护措施。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
13	通过内部无线网络传输数据，在满足以上基本要求的基础上，还应采用绑定设备序列号或硬件地址（MAC 地址）等管控措施对无线接入点进行准入控制，合理设置传输功率，控制无线信号的覆盖范围。	1.配置核查 2.旁站验证	1.查验无线接入点的配置，确认对传输功率、信号覆盖范围已进行合理设置。 2.查验并确认相关网络设备通过设备序列号或硬件地址绑定措施已实现无线接入点的准入控制。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
14	通过内部无线网络传输数据，在满足以上基本要求的基础上，还应对 SSID 采用规范的命名规则，不泄露机构名称、网络特性、物理位置等信息，禁止使用缺省的 SSID，生产环境应禁用 SSID 广播，避免攻击者通过扫描直接获取无线网络信息。	1.配置核查	1.查验无线网络设备的SSID命名，确认不存在泄漏机构名称、网络特性、物理位置等情况的不规范名称。 2.查验无线网络设备的配置，确认不存在使用缺省的SSID。同时，确认生产环境的无线网络设备已配置了禁用SSID广播的设置。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
15	通过内部无线网络传输数据，在满足以上基本要求的基础上，还应采用安全、可靠的加密协议，对无线通信信道进行安全加密。	1.文档查验 2.配置核查	1.查阅相关材料，确认已具备无线通信信道安全加密设计文档或产品说明。 2.查验无线网络设备的配置，确认无线通信信道使用了安全可靠的加密协议。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
16	通过内部无线网络传输数据，在满足以上基本要求的基础上，还	1.文档查验 2.配置核查	1.查阅建立的安全管理基线相关文件，确认已明确无线网络设备安全加固相关策略。

序号	安全要求	评估办法	结果判定
	应确保无线网络设备的物理安全，禁用不必要的服务，强化无线网络设备的管理账号和口令安全，禁止使用弱口令，建立安全管理基线。	3.工具测试	2.查验并确认无线网络设备安全基线满足要求。 3.使用弱口令检测工具，查验并确认无线网络设备的管理账号和口令安全，确认不存在弱口令。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
17	通过内部无线网络传输数据，在满足以上基本要求的基础上，还应加强无线网络用户管理，禁止多人使用同一账号，采用双因素认证方式对接入用户进行身份校验，停用长时间未登录使用无线网络的账号。	1.文档查验 2.配置核查 3.旁站验证	1.查阅无线网络管理制度，确认已明确禁止多人使用同一账号、采用双因素认证方式对接入用户进行身份校验、停用长时间未登录使用的账号。 2.查验无线网络相关配置与认证方式，确认对接入用户已使用了双因素认证方式、无多人使用同一账号的情况，且长时间未使用的账号已停用。 结果评价： 符合：满足以上第1至2项. 不符合：不满足以上第1至2项中的一项或多项。
18	通过内部无线网络传输数据，在满足以上基本要求的基础上，还应采取措施控制移动智能终端在内网和互联网交叉使用的风险，加强应用安全和数据泄露防护，防范恶意代码传播。	1.文档查验 2.旁站验证	1.查阅数据安全管理相关制度，确认已明确移动智能终端在内网和互联网交叉使用的各项安全防护要求和技术防护措施，以及加强应用安全和数据泄漏、防范恶意代码的安全管理要求和技术防护措施。 2.查验并确认移动智能终端在内网和互联网交叉使用时已采取包括防范数据泄漏和恶意代码等技术的安全防护措施。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
19	通过内部无线网络传输数据，在满足以上基本要求的基础上，还应明确短期使用及临时搭建的无线网络使用期限，期满后应及时拆除或关闭。	1.文档查验 2.工具测试 3.人员访谈	1.查阅无线网络管理制度，确认已明确临时搭建无线网络的相关要求。 2.查验临时无线网络搭建使用记录，确认使用合规，且经测试不存在不关闭的临时无线网络。 3.查验并询问短期使用及临时搭建的无线网络使用期限要求，查验临时无线网络使用情况，确认期满后已经及时拆除或关闭无线网络。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
20	通过运营商网络传输数据，在满足基本要求的基础上，2 级及以上数据还应采用专线或 VPN 等技术确保传输通道的安全，确保数据传输的安全性。	1.文档查验 2.配置核查	1.查阅运营商网络传输管理制度，确认已明确2级及以上数据传输采用专线或VPN等技术要求。 2.查验网络设备相关配置，确认通过运营商网络传输2级以上数据时已采用专线或VPN等安全的传输通道。 结果评价： 符合：满足以上第1至2项。

序号	安全要求	评估办法	结果判定
			不符合：不满足以上第1至2项中的一项或多项。
21	通过物理介质批量传递 3 级及以上数据时应对数据进行加密或脱敏，并由专人负责收发、登记、编号、传递、保管和销毁等，传递过程中可采用密封、双人押送、视频监控等确保物理介质安全到位，传递过程中物理介质不应离开相关责任人、监控设备等的监视及控制范围，且不应在无人监管情况下通过第三方进行传递，国家及行业主管部门另有规定的除外。	1.文档查验 2.人员访谈 3.旁站验证	1.查阅数据安全管理相关制度，确认已明确了物理介质批量传递3级及以上数据的管理要求。 2.访谈相关人员明确3级及以上数据的外部应用场景，确认3级及以上数据通过物理介质传递的场景和使用情况。 3.查验并确认物理介质批量传递3级及以上数据的登记记录符合要求。 4.查验物理介质批量传递3级及以上数据的加密或脱敏方式，确认加密或脱敏有效。 5.查验押送、视频监控等记录材料，确认物理介质批量传递3级及以上数据的过程中符合要求。 结果评价： 符合：满足以上第1至5项。 不符合：不满足以上第1至5项中的一项或多项。

7.2.4 数据存储

数据存储安全评估内容见表7.2.4。

表7.2.4 数据存储安全评估内容

序号	安全要求	评估办法	结果判定
1	数据存储不应因存储形式或存储时效的改变而降低安全保护强度。	1.文档查验 2.人员访谈 3.旁站验证	1.查阅数据安全相关制度，确认已明确“不应存储形式或存储时效的改变而降低数据安全保护强度”的要求。 2.访谈相关人员，了解并确认本机构当前采用的数据存储形式及不同存储形式所采用的安全防护措施。 3.随机查验生产环境存储的各级别数据与其他存储介质存储的相应数据，确认同级别数据具有相同安全防护措施。 4.随机查验各级别历史数据的安全防护措施，确认符合相应级别的安全防护要求。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
2	应根据安全级别、重要性、量级、使用频率等因素，将数据分域分级存储。	1.文档查验 2.旁站验证	1.查阅数据安全相关制度，确认已明确“根据安全级别、重要性、量级、使用频率等因素，将数据分域分级存储”的要求。 2.查阅数据分域分级存储的实施方案，确认已对各类数据的存储按照级别、重要性等进行了合理的界定与划分，能够体现纵深防御、差异化防护的基本思路。如按照处理数据的最高级别，对不同的业务系统进行安全区域划分，基于不同安全区域实施差异化保护策略。 3.查验并确认各区域各级别存储的数据与实施方案完全一致，确认数据分域分级存储技术隔离有效。 结果评价： 符合：满足以上第1至3项。

序号	安全要求	评估办法	结果判定
			不符合：不满足以上第1至3项中的一项或多项。
3	应依据最小够用原则存储数据，不应以任何形式存储非业务必需的金融数据，存储时间应为业务必需的最短时间，国家及行业主管部门另有规定的除外。	1.人员访谈 2.文档查验 3.旁站验证	1.查阅数据安全相关制度，确认已明确根据最小够用的数据存储原则，且不能以任何形式存储非业务必须的金融数据。 2.查验并确认以清单等形式明确的各类业务使用金融数据的期限要求。 3.应随机选取三个业务系统，查验各类数据的存储时间，确认均小于规定的业务必需使用时间。 4.应随机选取三个信息系统（至少涵盖生产、测试系统），查验各类已存储数据，访谈相关人员数据的实际业务用途，确认满足最小够用原则。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
4	应定期对数据存储过程中可能产生的影响进行风险评估，并采取相应安全防护措施。	1.文档查验 2.工具测试	1.查阅数据安全相关制度，确认已明确开展数据存储风险评估的机制（启动条件、流程、内容、风险等级划分、风险级别与结论、改进建议等）、已明确评估周期。 2.查阅数据存储安全评估报告，确认包括评估方式、评估内容及范围、评估结果、问题整改计划等。查验整改计划执行结果，确认已按计划执行、结果真实性。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	脱敏后的数据应与用于还原数据的恢复文件隔离存储，使用恢复原始数据的技术应经过严格审批，并留存相关审批及操作记录。	1.文档查验 2.旁站验证	1.查阅数据安全相关制度，确认已明确恢复原始数据的审批机制。 2.查阅数据分域分级存储的实施方案，确认脱敏后的数据与用于还原数据的恢复文件不属于同一区域，符合隔离存储的要求。 3.查阅并确认恢复原始数据的使用审批记录与操作记录合理、规范、详实。 4.查验并确认脱敏后的数据与用于还原数据的恢复文件存储区域与实施方案完全一致。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
6	应采取一定措施确保数据存储的完整性，存储 3 级及以上数据时，应采用密码技术、权限控制等技术措施保证数据完整性。	1.文档查验 2.工具测试 3.旁站验证	1.查阅数据安全相关制度，确认已明确3级及以上数据的完整性保护要求。 2.查验数据存储相关系统实施方案，确认存储3级及以上数据的信息系统或数据库已采用完整性安全保护技术措施，如基于密码技术的完整性保护、合理的权限控制、勒索病毒防护技术等。

序号	安全要求	评估办法	结果判定
			3.查验并确认对存储3级及以上数据的信息系统或数据库采取的安全防护技术措施与实施方案完全一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
7	2 级及以上数据应采取技术措施保证存储数据的保密性，必要时可采取多因素认证、固定处理终端、固定处理程序或工具、双人双岗控制等安全策略。	1.人员访谈 2.文档查验 3.旁站验证	1.查阅数据安全相关制度，确认已明确2级及以上数据的保密性保护要求。 2.查验数据存储相关系统实施方案，确认存储2级及以上数据的信息系统和数据库采用的保密性安全防护技术措施，如身份认证、权限控制、安全隔离等。 3.访谈相关人员，确认关于必要性情况的约定。 4.查验并确认存储2级及以上数据的信息系统或数据库在必要时已采取相关安全防护措施，如多因素认证、固定处理终端、固定处理程序或工具、双人双岗控制等。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
8	3 级数据的存储应采取加密等技术措施保证数据存储的保密性。	1.文档查验 2.工具测试 3.旁站验证	1.查阅数据安全相关制度，确认已明确3级数据的保密性保护要求。 2.查阅3级数据存储相关系统实施方案，确认存储3级数据已采用加密技术等措施。 3.查验并确认对存储3级数据的信息系统已采取了加密技术等措施。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
9	保存 3 级及以上数据的信息系统，其网络安全建设及监督管理宜满足网络安全等级保护 3 级要求。	1.文档查验	1.查阅保存3级及以上数据信息系统的建设文档，确认相关安全设计方案符合网络安全等级保护3级要求。（可选项） 2.查阅保存3级及以上数据信息系统等保测评报告和备案证明，确认该系统已通过3级等保测评。（可选项） 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
10	文件系统中存放含有 3 级及以上数据的文件，宜采用整个文件加密存储方式进行保护。	1.文档查验 2.工具测试 3.旁站验证	1.查阅文件系统实施方案，确认存储3级及以上数据的文件已采用整体加密技术措施。（可选项） 2.查验并确认存放含有3级及以上数据的文件已进行整体加密存储。（可选项） 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

序号	安全要求	评估办法	结果判定
11	4 级及以上数据应使用密码算法加密存储。	1.文档查验 2.工具测试 3.旁站验证	1.查阅数据安全相关制度，确认已明确4级及以上数据的保密性保护要求。 2.查阅4级及以上数据存储相关系统实施方案，确认存储4级及以上数据已采用具有密码算法的加密技术措施。 3.查验并确认对存储4级及以上数据的信息系统已采取了具有密码算法的加密方式。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
12	在我国境内产生的金融数据原则上应在我国境内存储，国家及行业主管部门另有规定的除外。	1.文档查验 2.工具测试	1.查阅数据安全管理相关制度，确认已明确我国境内产生的金融数据原则上应在我国境内存储，以及境外存储时需履行国家及行业主管部门相关规定等要求。 2.查验存储金融数据的信息系统的部署位置，确认均为国内地址。若存在境外存储金融数据情况，应确认符合国家及行业主管部门相关要求和规定。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
13	在我国境内产生的 5 级数据应仅在我国境内存储。	1.文档查验 2.工具测试	1.查阅数据安全相关制度，确认已明确境内产生的5级数据仅在我国境内存储等要求。 2.查验存储5级数据信息系统的部署位置，确认均为国内地址。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
14	应对数据存储区域进行规划，并对不同区域之间的数据流动进行安全管控。	1.文档查验 2.配置核查	1.查阅并确认已制定数据存储区域划分方案，并明确不同区域之间数据流动的安全管控措施。 2.查验相关安全管控设备的安全策略配置，确认已配置相关安全管控策略。 3.抽样查验近180天内数据在不同区域之间流动的安全管控记录，确认存储区域之间数据流动记录与方案一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
15	根据数据的安全级别和数据对系统运行的影响，制定数据备份策略和恢复策略，备份策略应至少指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法、备份周期或频率、备份范围等。	1.文档查验 2.配置核查	1.查阅数据安全相关制度，确认已明确数据备份和恢复相关机制。 2.查验并确认已根据数据的安全级别和对信息系统运行的影响制定合理的数据备份和恢复策略，且备份策略要素合规。 3.查验相关备份系统的配置，确认与已制定的策略一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。

序号	安全要求	评估办法	结果判定
16	生产数据应采取实时备份与异步备份、增量备份与完全备份的方式，提供本地数据备份与恢复功能。	1.文档查验 2.配置核查 3.旁站验证	1.查阅数据安全相关制度，确认已明确生产数据备份相关要求。 2.查阅相关备份系统的设计文档，确认配置了实时备份、异步备份、增量备份、完全备份等备份方式。 3.查验数据备份与恢复记录，确认备份与恢复实现与设计一致。 4.查验并确认生产数据本地备份与恢复功能有效。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
17	应建立同城与异地数据备份中心的远程数据备份与恢复功能，利用通信网络将关键数据定时批量传送至备用场地。	1.文档查验 2.旁站验证	1.查阅数据安全相关制度，确认已明确同城与异地数据备份中心的相关要求。 2.查验同城与异地备份中心建设实施方案，确认已明确远程数据备份与恢复，以及通过通信网络将关键数据定时批量传送至备用场地的设计内容。 3.旁站验证远程数据备份与恢复功能，确认结果符合预期。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
18	数据备份应基于多冗余策略，可采用磁带、磁盘镜像、磁盘冷备、热备、双活等技术实现，备份频度及保存期限不低于相关监管和业务使用要求。	1.人员访谈 2.文档查验 3.配置核查 4.旁站验证	1.查阅数据备份实施方案，确认数据备份采取多冗余策略与方式。 2.访谈业务相关人员，确认业务数据备份频度和数据最低保存期限要求。 3.查验数据备份的多冗余策略，确认与实施方案一致。 4.查验备份频度与保存期限的执行情况，确认符合监管与业务使用要求。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
19	应定期开展灾难恢复演练，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。	1.文档查验	1.查阅数据安全相关制度，确认已明确开展灾难恢复应急演练的相关机制，并明确开展演练的周期以及验证关键技术应用可行性的要求。 2.查阅灾难恢复演练方案、演练记录与总结报告，确认记录规范详实，其中关键技术应用已进行可行性验证测试。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
20	应定期对备份数据的有效性和可用性进行检查，定期对主要备份业务数据进行恢复验证，根据	1.文档查验 2.旁站验证	1.查阅数据安全相关制度，确认已明确检查备份数据有效性和可用性的周期、备份业务数据恢复验证的周期以及存储介质的使用期限。 2.查阅数据备份有效性和可用性检查记录，确认其规范详实。

序号	安全要求	评估办法	结果判定
	介质使用期限及时转储数据，确保数据可用性。		3.应检查备份业务数据恢复验证记录，确认记录规范详实。 4.对备份数据有效性和可用性进行查验，确认备份业务数据可正常恢复。 5.实地查验备份介质的使用时间，确认无超期使用的情况。 6.查验并确认介质使用期限到期后及时转储数据，且相关记录真实有效。 结果评价： 符合：满足以上第1至6项。 不符合：不满足以上第1至6项中的一项或多项。
21	生产数据备份存放环境及其物理设施的安全保护等级应按照GB/T 50174—2017的要求执行。	1.文档查验	1.查阅数据安全相关制度，确认已明确生产数据备份存放环境及物理设施的安全保护等级应按照GB/T 50174—2017的要求执行。 2.查阅验收报告、检查报告等相关资料，确认生产数据备份存放环境及物理设施符合GB/T 50174—2017。 结果评价： 符合：满足以上第1至2项要求。 不符合：不满足以上第1至2项中的一项或多项。
22	大数据平台应提供数据整体迁移功能，并具备迁移数据的完整性检测能力。	1.文档查验 2.工具测试	1.查阅大数据平台相关建设方案或迁移方案，确认具有数据整体迁移的功能，并具备迁移数据的完整性检测能力。 2.查阅大数据平台相关建设方案或迁移方案，并确认大数据平台具备平台整体迁移可行性，但不具备数据整体迁移的功能。 3.查验并确认数据整体迁移、数据完整性检测相关制度要求及技术方案。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第2至3项。 不符合：不满足以上第2至3项中的一项或多项。

7.2.5 数据使用

7.2.5.1 数据访问

数据访问安全评估内容见表7.2.5。

表7.2.5 数据访问安全评估内容

序号	安全要求	评估方法	结果判定
1	应综合考虑主体角色、信用等级、业务需要、时效性等因素，按最小化原则确定 2 级及以上数据的访问权限规则。	1.文档查验 2.人员访谈 3.旁站验证	1.查阅信息系统设计文档，确认对2级及以上数据访问权限规则、配置方式的详细说明。 2.访谈相关人员，确认根据人员角色和业务职能，且按最小化原则分配2级及以上数据的访问权限。 3.查验信息系统，确认人员访问权限配置规则，包括主体角色、信用等级、业务需要、时效性等因素。 4.尝试与规则不符操作（如使用已超时效的主体角色），查验操作返回结果，确认符合预期。

序号	安全要求	评估方法	结果判定
			结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	3 级及以上数据访问应建立访问权限申请和审核批准机制，保证实际操作与申请并审批的操作是一致的。	1.文档查验 2.旁站验证	1.查阅数据访问管理规程，确认已对3级及以上数据访问权限申请和审核批准规则做出书面规定。 2.查验数据访问申请和审核批准记录，确认实际操作与申请并审批的操作是一致的。 3.查验并确认数据访问已通过访问控制组件或访问控制代理技术对访问的终端设备、信息系统进行控制。（可选项） 结果评价： 符合：满足以上第1至2项或第1至3项。 不符合：不满足以上第1至2项中的一项或多项。
3	2 级及以上的数据访问应进行身份认证，对访问者实名认证，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档，确认对2级及以上的数据访问已设计身份认证功能，并对访问者进行实名认证，建立数据访问权限与访问者实际身份的关联关系，如账号、行号和身份证或手机号实现关联。 2.查验访问者身份验证和实名认证相关功能，确认功能正常。 3.尝试使用不同身份或角色的访问者发起2级及以上数据访问申请，查验返回结果，确认数据访问权限与实际访问者的身份或角色完全一致。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	2 级及以上的数据访问过程应留存相关操作日志，操作日志应至少包括明确的主体、客体、操作时间、具体操作类型、操作结果等。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档，确认已对数据访问过程的日志记录内容、保存期限进行说明。 2.查验日志系统，确认数据访问操作行为日志各要素已被记录，要素中应至少包括明确的主体、客体、操作时间、具体操作类型、操作结果等。确认相关日志记录要素完整详尽，并与实际情况完全一致。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	3 级及以上的数据访问应实现多因素认证或二次授权，并应结合业务需要对数据采取脱敏和控制访问数据行数的技术措施，以满足最小化原则要求。	1.文档查验 2.旁站验证	1.查阅相关设计文档，确认对3级及以上数据的访问采用多因素认证或二次授权措施，确认已结合业务需要对数据采取脱敏和控制访问数据行数的技术措施，以满足最小化原则要求。 2.现场查验3级及以上数据的访问多因素认证或二次授权相关功能，确认功能正常。

序号	安全要求	评估方法	结果判定
			3.现场查验访问3级及以上数据脱敏和控制访问数据行数相关功能，查验返回结果，确认脱敏和控制访问数据行数等技术措施符合要求。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
6	应对数据的访问权限和实际访问控制情况进行定期审计，至少每半年 1 次对访问权限规则和已授权清单进行复核，及时清理已失效的账号和授权。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档或相关文档，确认已明确数据的访问权限的审计策略、审计周期和审计内容，审计周期设置不应低于半年1次。 2.查阅评估范围内相关审计报告，确认已对数据访问权限和实际访问控制情况进行审计。 3.查验评估范围内相关审计报告，确认审计中发现的失效的账号和授权整改情况。确认已失效的账号和授权已被及时清理，与整改报告一致。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
7	应通过访问控制等措施限制频繁查询数据人员的数据访问频率，如柜员、客户经理、客服人员等确需批量查询的应通过相应审批并留存相关记录，并宜提供访问控制组件与审批结果的自动联动能力。	1.文档查验 2.配置核查 3.工具测试 4.旁站验证	1.查阅相关制度文档、基线要求，确认已明确通过访问控制等措施限制频繁查询数据人员的数据访问频率。 2.查阅并确认系统配置文件中访问控制等措施的相关配置参数与制度文档或基线要求完全一致。 3.使用工具等手段测试尝试频繁发起数据查询申请，查验返回结果，确认相关限制措施符合要求。 4.使用工具等手段查验评估范围内批量查询的访问记录，并与审批记录做逐一核对，确认完全一致。 5.查验新增申请审批请求功能，确认访问控制组件与系统审批请求结果实现自动联动的能力。（可选项） 结果评价： 符合：满足以上第1至4项或第1至5项。 基本符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
8	特权账号应明确安全责任人，严格限定特权账号的使用地点，并配套多因素认证措施对使用者进行实名认证。	1.文档查验 2.旁站验证 3.配置核查	1.查阅并确认具备特权账号（信息系统管理员、有权限进行批量明文数据查询系统用户等）管理规程，且管理规程中已明确特权账号可使用场景、可使用地点和相关安全责任人。 2.查阅信息系统设计文档，确认特权账号登陆已设计多因素认证措施，且认证措施具备实名认证能力。 3.查验特权账号实名认证相关功能和使用地点限制，并确认功能正常。 结果评价： 符合：满足以上第1至3项。

序号	安全要求	评估方法	结果判定
			不符合：不满足以上第1至3项中的一项或多项。
9	应预先明确特权账号的使用场景和使用规则，并配套建立审批授权机制。	1.文档查验 2.旁站验证 3.配置核查	1.查阅并确认信息系统需求文档与设计文档，已就特权账户使用场景进行明确，并已设计电子化的授权审批机制。 2.若无电子化授权审批机制，查阅并确认具备相关业务流程管理规范，并已分场景（或业务操作）就特权账户使用与授权审批进行书面规定，相关授权审批记录规范详实。 3.对设计电子化的授权审批机制的信息系统，查验相应系统功能，确认功能正常。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1、2或第1、3项。 不符合：不满足以上第1、2项中的一项或多项或第1、3项中的一项或多项。
10	可访问 3 级及以上数据的特权账号，在每次使用前应进行审批授权，并宜采取措施确保实际操作与所获授权的操作是一致的，防止误执行高危操作或越权使用等违规操作。	1.文档查验 2.旁站验证 3.工具测试	1.查验审批记录，选取可访问3级及以上数据特权账号使用记录，并与审批授权记录做逐一核对，确认完全一致。 2.查验特权账号数据访问操作，并确认审批授权流程、双人复核等措施。 3.查阅相关设计文档，并进行旁站验证，对实际操作与所获授权操作的一致性技术保障措施进行确认。（可选项） 结果评价： 符合：满足以上第1至2项或第1至3项。 不符合：不满足以上第1至2项中的一项或多项。
11	应详细记录特权账号的访问过程和操作记录，配备事后审计机制，并确保特权账号无法对操作日志进行修改和删除。	1.旁站验证	1.查验相关信息系统，确认已对特权账号的访问过程和操作记录进行收集保存，并已配备相关事后审计机制。 2.实用工具抽样查验近180天内特权账号的访问过程操作记录，确认相关记录要素完整详尽。 3.使用特权账号尝试对存有操作日志进行修改或删除，查验执行结果，确认符合要求。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

7.2.5.2 数据导出

数据导出安全评估内容见表7.2.6。

表7.2.6 数据导出安全评估内容

序号	安全要求	评估方法	结果判定
1	应根据最小够用原则，确定数据导出场景、导出数据范围和相应的权限规则。	1.文档查验 2.旁站验证	1.查阅数据安全管理相关制度，确认已明确数据的导出需求、具体场景、导出范围和相应的权限规则，且明确要求导出的数据类型及数量均应为当前应用场景所必需的最小数据集。

序号	安全要求	评估方法	结果判定
			2.查验信息系统导出功能，确认相应应用场景的实际数据导出情况与相关制度要求及该应用场景设计预期完全一致。 3.查阅信息系统数据库配置文档，确认数据库管理员不存在未经授权审批即可从后台直接导出数据的可能性，并确认留存相关授权审批记录及数据导出相关日志记录，且两者记录的操作时间、操作类型、操作内容等信息保持一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
2	2 级及以上的数据导出操作应明确安全责任人，配备安全、完善的身份验证措施对导出操作人进行实名认证。	1.文档查验 2.旁站验证	1.查阅数据导出规程，确认已明确数据导出操作的安全责任人及安全职责。 2.查阅信息系统设计文档，确认对导出操作已设计身份验证措施，且验证措施具备实名认证能力（如通过账号、工号、身份证号或手机号等实现实人关联）。 3.查验数据导出操作，确认操作人需要进行账号和身份认证相关功能后方可导出。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
3	2 级及以上的数据导出应有详细操作记录，包括操作人、操作时间、操作结果、数据类型及安全级别等，留存时间不少于 6 个月。	1.文档查验 2.工具测试	1.查阅信息系统设计文档，确认已对2级及以上数据的导出记录进行收集保存，操作记录包括操作人、操作时间、操作结果、数据类型及安全级别等。 2.使用工具或人工查验评估范围内2级及以上的数据导出记录，确认操作记录详实和留存时间不少于6个月。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	3 级及以上数据的导出操作还应有明确的权限申请和审核批准机制。	1.文档查验 2.工具测试	1.查阅信息系统设计文档，确认包括对3级及以上数据的导出操作权限申请和审核批准机制的相关内容。 2.使用工具或人工抽样查验近180天内3级及以上数据的导出记录，并与权限申请和审核批准记录进行逐一核对，确认完全一致。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	3 级及以上数据的导出操作前应使用多因素认证或二次授权机制，并将操作执行的网络地址限制在有限的范围内。	1.文档查验 2.旁站验证 2.工具测试	1.查阅信息系统设计文档，确认已对3级以上数据的导出操作设计包括多因素认证或二次授权以及操作执行的网络地址限制功能。 2.查验3级以上数据的导出操作前多因素认证或二次授权相关功能，并确认功能正常。

序号	安全要求	评估方法	结果判定
			3.查验并确认已设置网络地址限制，尝试在未授权的网络地址将数据导出，确认操作会被拒绝。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
6	3 级及以上的数据导出应使用加密、脱敏等技术手段防止数据泄露，国家及行业主管部门另有规定的除外。	1.文档查验 2.工具测试	1.查阅信息系统设计文档，确认已对3级及以上数据导出设计加密、脱敏等技术手段。 2.查验信息系统导出的3级以上数据，确认所使用的加密、脱敏等技术手段符合预期。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
7	4 级数据原则上不应导出，确需导出的，除上述要求外，还应经金融业机构高级管理层批准，并配套数据跟踪溯源机制。	1.文档查验 2.配置核查	1.查阅信息系统设计文档，确认数据导出功能中不存在4级数据，如包括4级数据已设计数据跟踪溯源机制。 2.查验数据导出管理规程，确认已做出对4级数据的导出须经本机构高级管理层批准的书面规定。 3.使用工具或人工统计评估范围内4级数据的导出记录，并与权限申请和审核批准记录做逐一核对，确认完全一致，需重点核对本机构高级管理层批准记录。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。

7.2.5.3 数据加工

数据加工安全评估内容见表7.2.7。

表 7.2.7 数据加工安全评估内容

序号	安全要求	评估方法	结果判定
1	应明确原始数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容。	1.文档查验	1.查阅信息系统设计开发等过程记录文档，确认已对原始数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容进行详细说明。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。
2	3 级及以上数据加工之前应进行数据安全评估，并采用加密、脱敏等技术措施，保证数据加工过程的数据安全性。	1.文档查验 2.工具测试	1.查阅信息系统设计文档，确认已对3级及以上数据加工的安全性、合规性进行评估，内容至少包括数据加工需求合理性、所用数据的必要性、数据来源及数据加工操作的合法合规性、数据安全技术措施的有效性、主要安全风险及其发生的可能性等，并留存相关评估报告等记录文件。 2.查阅信息系统设计文档，确认后台管理系统已对3级及以上数据加工过程所采用加密、脱敏等技术措施进行详细说明。

序号	安全要求	评估方法	结果判定
			3.使用工具查验或人工检查3级及以上数据加工过程数据，查验返回结果，确认使用的加密、脱敏等技术手段符合预期。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1、2项或第1、3项。 不符合：不满足以上第1、2项中的一项或多项或第1、3项中的一项或多项。
3	除业务必须外，不应对 4 级数据进行加工。	1.文档查验	1.查阅数据加工管理过程文档或相关数据安全管理要求，确认已明确非业务必须外不对4级数据进行加工，或就4级数据加工的场景清单、具体场景需求、授权审批机制作出书面规定。 2.抽样查验评估范围内4级数据加工操作记录，并与授权审批记录逐一核对，确认进行4级数据加工真实必要。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	应对数据加工过程进行必要的监督和检查，确保加工过程的数据安全性。	1.文档查验	1.查阅存在的数据加工管理规程，确认已就数据加工过程进行监督和检查或行为审计做出书面规定。 2.查验评估范围内数据加工过程的监督和检查或行为审计记录，确认符合要求。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	应完整记录数据加工过程的操作日志。	1.文档查验 2.工具测试	1.查阅信息系统设计文档，确认已对数据加工过程操作的日志记录内容、保存期限进行说明。日志应至少包括数据获取方式、访问接口、数据级别、处理结果等内容。 2.使用工具查验评估范围内数据加工的操作日志，与数据加工授权审批记录或数据安全评估报告逐一核对，确认完全一致。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

7.2.5.4 数据展示

数据展示安全评估内容见表 7.2.8。

表7.2.8 数据展示安全评估内容

序号	安全要求	评估方法	结果判定
1	数据展示前，应事前评估展示需求，包括展示的条件、环境、权限、内容等，确定展示的必要性和安全性。	1.文档查验	1.查阅并确认具备信息系统设计文档、评估过程记录、评估结论等展示需求评估文档，并已明确展示功能需求及安全要求。 2.查阅相关文档，确认包括展示界面、展示条件、环境限制、查询权限、展示内容、数据安全级别、安全措施等内容。 3.查阅评估结果，确认评估结论并与实际执行和情况一致。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
2	对应用系统桌面、移动运维终端、柜面受理设备等界面展示增加水印，水印内容应最少包括访问主体、访问时间。	1.旁站验证	1.查验相关界面的数据展示页面，确认页面展示使用水印技术。 2.查验并确认水印内容至少包括访问主体唯一标识、访问时间等。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
3	禁用展示界面复制、打印等可将展示数据导出的功能。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档，确认系统不具备或禁用展示界面复制、打印等可将展示数据导出的功能。 2.查验相关功能的数据展示操作，确认数据的用户无法执行复制、打印等可将展示数据导出的操作。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	业务系统对 2 级及以上数据明文查询实现逐条授权、逐条查询，或具备对查询相关授权、次数、频率、总量等指标的实时监测预警功能，并留存相关查询日志。	1.文档查验 2.旁站验证 3.工具测试	1.使用逐条授权、逐条查询的（如由任务、事件触发的查询）业务系统，查阅信息系统设计文档，确认逐条查询功能中明确说明逐条授权的功能流程、方式。 2.使用逐条授权、逐条查询的业务系统，查验相应信息系统功能，并确认功能与信息系统设计文档一致。 3.使用逐条授权、逐条查询的业务系统，使用抽检或工具统计等方式对2级及以上明文数据的查询日志进行检查，并与审批授权记录做逐一核对，确认完全一致。 4.具备监测预警功能的业务系统，查阅相关信息系统设计文档，确认监测指标涵盖相关授权、次数、频率、总量等，以及超过相关阈值的安全保护措施。 5.具备监测预警功能的业务系统，查验触发监测指标预警时的系统响应或查阅相关审计日志记录，确认相关安全保护措施符合预期。 6.具备监测预警功能的业务系统，查阅并确认留存2级及以上明文数据的相关查询日志。 结果评价： 符合：逐条授权、逐条查询的业务系统满足以上第1至3项，具备监测预警功能的满足以上第4至6项。 基本符合：逐条授权、逐条查询的业务系统满足以上第1、2项，具备监测预警功能的满足以上4、5项。 不符合：不满足以上第1、2中的一项或多项或第4、5项中的一项或多项。

序号	安全要求	评估方法	结果判定
5	数据展示后，应及时将展示数据从本地缓存中清除。	1.文档查验 2.问卷调查 3.旁站验证	1.查阅信息系统设计文档，确认展示数据的清除方式及相应的实现方式。 2.使用手动清除方式的，查验并确认数据清除工具、步骤和清除周期，并确认与展示数据相关的本地缓存及时清除。 3.使用自动清除方式的，查验展示页面关闭后，本地缓存不存在相关数据，并确认功能正常。 结果评价： 符合：满足以上第1、2项或第1、3项。 基本符合：手动清除方式满足以上第1项，自清除方式必须满足第1、3项。 不符合：手动清除方式不满足以上第1项，自清除方式第1、3项中的一项或多项。
6	2 级数据的展示应事先通过审批授权后方可展示。	1.文档查验 2.旁站验证	1.查阅相关管理制度，确认已建立授权审批机制，明确审批人员及流程，查阅信息系统设计文档，已就2级以上数据的展示场景进行明确。 2.若无电子化授权审批机制，查阅并确认过往2级以上数据相关授权审批记录。 3.对设计电子化的授权审批机制的信息系统，查验相应系统功能，并确认功能正常。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
7	3 级数据的展示应在审批的基础上采用屏蔽等技术措施防止信息泄露。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档，确认所采取的数据屏蔽技术策略、手段及详细说明。 2.查验相应信息系统的数据展示屏蔽功能，确认功能正常。 3.查阅相关制度文档，确认已制定统一的屏蔽策略。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1、2项。 不符合：不满足以上第1至2项中的一项或多项。
8	4 级及以上数据不应明文展示，国家及行业主管部门另有规定的除外。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档，确认不存在4级及以上数据或4级以上数据未进行明文展示。 2.查验并确认展示功能中未涉及4级以上明文数据。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

7.2.5.5 开发测试

开发测试安全评估内容见表 7.2.9。

表7.2.9 开发测试安全评估内容

序号	安全要求	评估方法	结果判定
1	应采取技术措施，实现开发测试环境数据与生产环境数据的有效隔离。	1.文档查验 2.配置核查 3.工具测试	1.查阅相关制度或文档，确认已规定开发测试环境数据与生产环境数据的有效隔离以及数据存储的相关要求。 2.查阅信息系统规划部署相关文档，确认开发测试环境与生产环境的隔离措施及详细说明。 3.采用网络物理隔离的，查验并确认网络拓扑与实际情况完全一致；采取其他隔离措施的，查验网络拓扑及相关权限设置，确认开发测试环境与生产环境之间具有严格的访问控制策略配置。 4.采取其他隔离措施的，查验网络拓扑及相关权限设置，确认开发测试环境与生产环境之间具有严格的访问控制策略配置。 5.使用工具查验并确认开发测试环境无法生产环境网络互通。 结果评价： 符合：满足以上第1至5项。 基本符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
2	应通过安全运维管理平台或数据提取专用终端获取数据，专用终端应事先经过审批授权后方可开通，原则上不应涉及4级数据。	1.文档查验 2.旁站验证	1.查阅相关设计文档，确认除安全运维管理平台和数据提取专用终端外，无其他数据获取渠道。 2.使用安全运维管理平台获取数据，确认能够数据获取成功，并查验管理平台日志信息或审计信息，确认所获取的数据安全级别不高于4级及以上。 3.使用数据提取专用终端获取数据，查验审批授权记录，统计评估范围内数据获取记录，并逐一核对确认完全一致，查验审计日志确保获取记录一致，且所获取的数据安全级别不高于4级及以上。 4.查验网络、主机、数据库等审计日志，确认获取数据只包括安全运维管理平台和专用终端。 结果评价： 符合：满足以上第1至4项。 基本符合：使用安全运维管理平台获取数据满足以上第1至2项；使用数据提取专用终端获取数据满足以上第1、3项。 不符合：不满足以上第1至3项中的一项或多项。
3	通过管理平台或专用终端获取3级及以上数据时，应通过技术手段控制数据的获取范围，包括对象、数据量等，并能对获取的数据按照策略进行脱敏处理，保证生产数据经过脱敏处理后才能被提取。	1.文档查验 2.旁站验证 3.工具测试	1.查阅相关设计文档，确认已对获取3级及以上数据的控制措施、技术手段、脱敏策略进行详细说明。 2.查验并确认通过管理平台或专用终端获取3级及以上数据的控制措施（安全设备）已按照设计进行部署，相应策略已配置生效。 3.查验3级及以上数据获取过程，确认对获取对象、数据量的控制措施正常有效，并确认获取的数据已脱敏处理。 4.使用工具测试已脱敏处理的数据，确认脱敏处理措施有效。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
4	开发测试等过程的数据，应事先进行脱敏处理，防止数据处理过程中的数据泄露，国家及行业主管部门另有规定的除外。	1.文档查验 2.工具测试	1.查阅相关设计文档，确认已明确开发测试过程中的脱敏策略。 2.使用工具测试现场抓取开发测试等过程中的数据，确认脱敏处理措施有效。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	使用外部的软件开发包、组件、源码等开展开发测试工作前应进行数据安全评估。	1.文档查验	1.查阅数据安全评估报告，确认已对外部的软件开发包、组件、源码的安全性进行审查。 2.调阅软件开发包、组件的清单，确认其版本已及时更新，且不存在明显的安全漏洞。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
6	接入开发测试环境的内外部终端设备应进行统一安全管理，宜安装统一的终端安全管理软件。	1.文档查验 2.配置核查	1.查阅相关设计文档，确认内外部终端设备所采取的安全策略至少包括：网络准入、防病毒、操作系统补丁、文件输入输出审计等管控措施。 2.抽样查验部分接入开发测试环境的内外部终端设备，确认所采取的安全策略能正常运行。 3.查验并确认内外部终端设备接入开发测试环境申请、准入操作及变更记录，确保与实际终端数量和策略一致 4.如安装统一的终端安全管理软件，查验并确认设计文档和管理系统（服务器）所配置的安全策略与实际管控终端数量、安全接入安全要求一致。（可选） 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
7	应制定开发测试安全审核流程，对数据源、需求进行审核，以确保数据分析目的、分析操作等方面的正当性与合法性。	1.文档查验	1.查阅相关文档，确认已明确开发测试安全审核流程 2.查阅过往对数据源、需求的审核记录，确认与审核流程要求相符。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
8	应对开发测试过程进行日志记录，并定期进行安全审计。	1.文档查验 2.旁站验证	1.查阅相关文档，确认已明确开发测试过程所需记录内容，以及相应的审计策略和审计周期。

序号	安全要求	评估方法	结果判定
			2.查阅审计记录，确认审计内容与实际情况一致，且符合审计周期要求。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项。
9	非本机构设备接入开发测试环境应经过开发部门以及设备使用部门审批，存储有开发测试数据的设备、介质带离金融业机构前应经过开发部门以及设备使用部门审批。	1.文档查验 2.现场核查	1.查阅管理制度、信息系统需求文档与设计文档，确认已就非本机构设备接入开发测试环境场景进行明确，并已设计电子化的授权审批机制。 2.若无电子化授权审批机制，查验并确认存在相关业务流程管理规范，并就非本机构设备接入的审批进行书面规定，相关授权审批记录规范详实。 3.对设计电子化的授权审批机制的信息系统，查验相应系统功能，并确认功能正常。 4.查验已接入测试开发环境的非本机构设备，与审批记录逐一核对，确认完全一致。 5.查验存储有开发测试数据的设备、介质带离本机构的审批记录，确认开发部门以及设备使用部门审批通过。 结果评价： 符合：满足以上第1至5项。 不符合：不满足以上第1至5项中的一项或多项。

7.2.5.6 汇聚融合

汇聚融合安全评估内容见表7.2.10。

表7.2.10 汇聚融合安全评估内容

序号	安全要求	评估方法	结果判定
1	汇聚融合的数据不应超出采集时所声明的使用范围，因业务需要确需超范围使用个人金融信息的，应事先再次征得个人金融信息主体明示同意。	1.文档查验 2.旁站验证	1.查阅相关设计文档和隐私政策或其他数据采集声明，确认已明确数据汇聚融合的业务场景，并已就所使用的数据类型、安全级别、数据来源、使用目的进行详细说明。 2.查阅征求个人金融信息主体明示同意相关功能和内容，确认其已涵盖汇聚融合数据的使用目的和范围。 3.抽样查验汇聚融合的数据，确认均未超出事先声明的数据使用范围。 4.抽样查验存在使用范围、目的等变更的汇聚融合场景，确认变更后的数据使用范围、目的等均于事先再次征得个人金融信息主体明示同意。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
2	汇聚融合前应根据汇聚融合后可能产生的数据内容、所用于的目的、范围等开展数据安全影响	1.文档查验 2.旁站验证	1.查阅数据安全影响评估报告，确认已对汇聚融合后可能产生的数据内容、所用目的、范围的影响，合规性和安全性进行评估。

序号	安全要求	评估方法	结果判定
	评估，并采取适当的技术保护措施。		2.查阅信息系统设计文档和安全文档，确认已结合数据安全影响评估结果采取相应技术防护措施，并现场核验，确认实际情况与文档描述完全一致。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	涉及第三方机构合作的，应以合同协议等方式明确用于汇聚融合的数据内容和范围、结果用途和知悉范围、各合作方数据保护责任和义务，以及数据保护要求等，并采用技术手段如多方安全计算、联邦学习、数据加密等技术降低数据泄露、窃取等风险。	1.文档查验 2.旁站验证	1.查阅合同协议等约定条款，确认已书面明确双方数据保护责权划分，并确认第三方机构已提供具有法律效力的数据来源合法合规性承诺证明。 2.查阅合同协议等约定条款，确认已书面明确用于汇聚融合的数据内容和范围、结果用途和知悉范围、各合作方数据保护责任和义务，以及数据保护要求。 3.查验相关设计文档和安全文档，确认已采用技术手段降低数据泄露、窃取等风险。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	4 级数据原则上不应用于汇聚融合，因业务需要确需汇聚融合的，应建立审批授权机制并具备数据跟踪溯源能力后方可汇聚融合。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈并确认数据汇聚融合的业务场景所以使用的数据安全级别不高于4级。 2.所使用的数据安全级别为4级及以上的，查阅相关制度文档，确认已建立审批授权机制，且相关审批授权记录规范完整。 3.所使用的数据安全级别为4级及以上的，查阅相关信息系统设计文档及安全文档，确认已具备数据跟踪溯源能力，并查验数据跟踪溯源功能，确认功能正常有效。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1项或第2、3项。 不符合：不满足以上第1项或第2、3项中的一项或多项。
5	应对脱敏后的数据集或其他数据集汇聚后重新识别出个人金融信息主体的风险进行识别和评价，并对数据集采取相应的保护措施。	1.文档查验	1.查阅个人金融信息主体的风险识别和评价文档，确认对脱敏后的数据集或其他数据集汇聚后重新识别出的个人金融信息进行有效的风险识别和评价。 2.查阅相关设计文档，确认已采取相应技术保护措施，可有效防范脱敏后的数据集或其他数据集汇聚后个人金融信息主体的风险。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

序号	安全要求	评估方法	结果判定
6	汇聚融合后产生的数据以及原始数据的衍生数据，应重新明确数据所属单位和安全保护责任部门，并确定相应数据的安全级别。	1.文档查验 2.现场核查	1.查阅相关管理规程，确认已对汇聚融合数据和衍生数据重新明确所属单位、安全保护责任部门、安全级别做出书面规定。 2.抽样查验并确认汇聚融合后产生的数据以及原始数据的衍生数据已明确所属单位、安全保护责任部门、安全级别。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

7.2.5.7 公开披露

公开披露安全评估内容见表 7.2.11。

表 7.2.11 公开披露安全评估内容

序号	安全要求	评估方法	结果判定
1	应依据国家有关规定与行业主管部门规章，在金融业机构官方渠道披露数据。	1.文档查验	1.查阅关于披露的相关制度和文档，确认已明确了数据披露的官方渠道。 2.查阅评估范围内数据披露记录清单，确认清单要素至少包括：披露日期、披露时间（指永久或固定时间段）、披露渠道、数据规模、披露目的、披露范围、数据内容简要、数据安全级别等。 3.查阅本机构官方网站、客户端软件等官方渠道发布的历史数据信息，确认披露记录清单与实际情况完全一致。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	数据安全管理部门应会同有关业务部门，对拟披露数据的合规性、业务需求、数据脱敏方案进行审核。	1.文档查验	1.查阅关于信息披露的相关制度和文档，确认对数据披露建立了管理机制和流程，包括审批流程、审批参与部门、审批要点等。 2.查阅业务部门披露需求，确认已包括了必要的要素，并进行了论证，要素至少包括：对拟披露数据的合规性、业务需求、数据脱敏方案，且记录规范详实，合规性应说明披露依据的国家或行业主管部门规定，业务需求应说明业务必要性并按最小必要的原则确定披露数据的范围，数据脱敏方案应说明脱敏方式及脱敏后达到的效果。 3.查阅数据脱敏方案，并查验数据脱敏执行情况，确认所涉及的数据已按照方案要求进行脱敏处理。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。

序号	安全要求	评估方法	结果判定
3	业务部门应对披露渠道、披露时间、拟公开数据的真实性，以及数据脱敏效果进行确认。	1.文档查验 2.旁站验证	1.查阅业务部门对数据披露的确认记录，确认其要素至少包括：披露渠道、披露时间、拟公开数据的真实性，且记录规范详实。 2.旁站验证业务部门的数据实际脱敏过程，确认脱敏效果真实、有效。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
4	应留档数据公开披露的审批过程和记录。	1.文档查验	1.查阅相关制度及文档，确认已明确数据公开披露的审批过程和记录的要求。 2.查阅数据披露的审核记录及确认记录，确认两份记录能一一对应。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
5	通过金融业机构官方网站披露数据时，采取包括网页防篡改等技术措施，防范披露数据篡改风险。	1.文档查验 2.旁站验证 3.工具测试	1.查阅官方网站安全设计文档，确认已对网页防篡改策略、技术措施进行了详细说明。 2.查验官方网站的安全措施，确认已采用网页防篡改等技术措施来防范披露数据被篡改风险。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
6	通过金融业机构客户端应用软件披露数据时，按照 JR/T 0092—2019 相关要求执行。	1.文档查验 2.配置核查 3.旁站验证	1.查阅客户端的安全设计文档，确认客户端应用软件具备相关防篡改策略与手段。 2.查验客户端应用软件，确认相关配置能够满足披露数据的防篡改与防泄露需求。 3.查验相关应用、设备的数据披露实际情况，确认数据防篡改、防泄漏等策略被实际执行。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
7	不应公开披露 3 级及以上数据。	1.文档查验 2.旁站验证	1.查阅数据披露记录，并与JR/T 0179-2020比对，确认数据安全级别划分准确无误。 2.查验数据披露信息，确认不存在3级及以上数据披露信息。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。

序号	安全要求	评估方法	结果判定
			不符合：不满足以上第1项。
8	应准确记录和保存数据的公开披露情况。	1.文档查验	1.查阅官方数据披露渠道的数据公开披露记录，确认数据公开披露行为真实存在。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。

7.2.5.8 数据转让

数据转让安全评估内容见表 7.2.12。

表 7.2.12 数据转让安全评估内容

序号	安全要求	评估方法	结果判定
1	不应违规进行数据转让。	1.文档查验 2.旁站验证	1.查阅与外部机构进行数据转让的记录及相关合同协议，确认与外部机构已约定获得数据转让的相关授权。 2.抽样查验转让数据的场景，确认所转让数据的内容、范围、处理方式等符合JR/T 0223-2021等对于数据转让的相关规定。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
2	因机构收购、兼并、重组等情况，将金融产品服务移交至其他金融业机构时，应通过逐一传达或公告的方式向个人金融信息主体等履行告知义务。	1.文档查验	1.查阅收购、兼并、重组的相关证明文件，确认证明文件真实、有效。 2.查阅相关传达或公告记录，确认具有明确的传达对象、传达内容、传达日期记录。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
3	因机构收购、兼并、重组等情况，承接其他金融业机构的金融产品或服务时，若变更转让数据的使用目的，应重新获得个人金融信息主体的明示同意或授权。	1.文档查验	1.查阅收购、兼并、重组的相关证明文件，确认证明文件真实、有效。 2.查阅个人金融信息主体的明示同意或授权记录，确认已说明变更后的数据使用目的，且与实际情况完全一致。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
4	若发生机构破产且无承接方的情况，应将情况及时报送行业主管部门，将数据移交至行业主管部门指定的机构进行继续保存，或依据行业主管部门的要求，对数据进行销毁处理，并将将数据	1.文档查验	1.查阅破产相关证明文件，确认证明文件真实、有效。 2.若将数据移交至行业主管部门指定的机构的，查阅向行业主管部门的数据移交申请记录和反馈文件，确认数据移交行为的真实性。

序号	安全要求	评估方法	结果判定
	处理结果通过逐一传达或公告的方式向个人金融信息主体等履行告知义务。		3.若对数据进行销毁处理的，查阅相关销毁记录，确认已登记销毁时间、销毁方式，以及销毁数据的总量、类型、条数，并有负责销毁机构或人员的确认记录。 4.若对数据进行销毁处理的，查阅相关公告内容，确认已通过逐一传达或公告的方式履行告知义务。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。

7.2.5.9 委托处理

委托处理安全评估内容见表 7.2.13。

表 7.2.13 委托处理安全评估内容

序号	安全要求	评估方法	结果判定
1	落实委托处理活动中的第三方开展数据安全管理工作要求。	1.文档查验 2.人员访谈	1.查阅管理制度和相关文档，确认已明确本机构第三方机构安全管理制度，且其中已明确委托处理活动中第三方的相关管理要求。 2.查阅委托处理相关第三方管理工作实际开展过程中的相关记录材料，确认符合本文件6.2.4合作管理相关评估内容。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
2	受委托的第三方机构应满足国家及行业主管部门的相关要求，金融业机构应对第三方机构开展事前尽职调查。	1.文档查验	1.查阅管理制度和相关文档，确认已明确对第三方机构开展事前尽职调查的具体内容，至少包括：经营情况、技术能力、内控管理、合规守法等方面。 2.查阅尽职调查记录，确认已对第三方机构满足国家及行业主管部门的相关要求进行验证，至少包括国家及行业主管部门相关要求，第三方机构的符合情况。 3.对国家及行业主管部门采取清单制管理或颁发资质证书的，查阅第三方机构提供的证明材料，其具备确认从事相关业务的资质。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	委托行为不应超出事前已获得授权及合同协议约定的数据使用范围。应根据委托处理的数据内容、范围、目的等，对数据委托处理行为进行数据安全影响	1.文档查验 2.旁站验证 3.工具测试	1.查阅相关数据的授权和合同协议等约定文件，确认本机构的委托行为在已获得的授权范围内，且已明确数据使用范围，且在与被委托方的合同协议中对此进行了说明和约定，其中数据使用不应超出数据采集时所声明的目的和范围。

序号	安全要求	评估方法	结果判定
	评估，涉及个人金融信息的，应进行个人金融信息安全影响评估，并采取相应的有效保护措施。		2.查阅信息系统设计文档、合同协议等文件，确认双方均已明确需数据委托处理的业务场景，以及所委托处理的数据类型、数据范围、处理目的、安全级别等，数据范围符合“最小够用”的原则。 3.查阅相关评估报告，确认已开展数据安全影响评估，对范围、影响层级进行评估且未超出事前已获得授权及合同协议约定的数据使用范围。 4.涉及个人金融信息的，查阅评估报告，确认已按照GB/T 39335-2020及JR/T 0171-2020开展了个人金融信息安全影响评估。 5.涉及个人金融信息的，查阅信息系统设计文档，确认已对安全防护措施进行详细描述，并通过使用工具或信息系统演示等手段，确认所采用的安全防护措施与设计文档完全一致。 结果评价： 符合：满足以上第1至5项。 基本符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
4	应对被委托方数据安全防护能力进行数据安全评估，并确保被委托方具备足够的数据安全防护能力，提供了足够的安全保护措施。	1.文档查验 2.工具测试	1.查阅管理制度和相关文档，确认已明确对委托方开展数据安全评估的方式、周期、内容。 2.查阅评估记录、评估报告或证明材料，确认被委托方已具备足够的数据安全防护能力，必要时可使用工具、现场查验对评估结果进行复核。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
5	不应对4级数据进行委托处理。	1.文档查验 2.旁站验证 3.工具测试	1.查阅信息系统设计文档、合作协议，确认双方已明确所委托处理的数据安全级别，且数据中不包括4级数据。 2.使用工具或利用信息系统审计功能获取委托处理数据片段，确认与设计文档完全一致。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
6	个人金融信息应事先采用数据脱敏等技术防止个人金融信息泄露，因业务确需，以及国家及行业主管部门另有规定的除外。	1.文档查验 2.旁站验证 3.工具测试	1.查阅合同协议等文件，确认双方均已明确需数据委托处理的业务场景，以及所委托处理的数据类型、数据范围、处理目的、安全级别等，且明确个人金融信息已进行脱敏。 2.当存在未脱敏的个人金融信息时，查阅评估报告或相关说明，确认已明确不采取脱敏操作有充足的理由，包括业务必要性或国家及行业主管部门的规定。 3.查阅信息系统设计文档，确认已明确需数据委托处理的业务场景，以及针对个人金融信息已设计脱敏方法和脱敏技术。

序号	安全要求	评估方法	结果判定
			4.使用工具或利用信息系统审计功能获取委托处理的个人金融信息片段，确认已采取脱敏处理，且所采用的脱敏技术与设计文档完全一致。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
7	涉及2级、3级数据的，应对数据进行加密处理，并采取数据标记、数据水印等技术，降低数据被泄露、误用、滥用的风险。	1.文档查验 2.旁站验证 3.工具测试	1.查阅信息系统设计文档及合同协议等文档，确认已明确需数据委托处理的业务场景、所委托处理的数据安全级别，并针对2级、3级数据已采取加密、标记、水印等技术措施。 2.使用工具或利用信息系统审计功能获取委托处理的2级、3级数据片段，确认已进行加密、标记、水印等处理，并且所采用的技术手段与设计文档完全一致。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
8	因业务确需无法对数据进行脱敏或加密处理的，应明确相应授权审批机制，事前对委托处理的内容通过专项审批，并采取技术措施防止数据被泄露、误用、滥用。	1.文档查验	1.查阅管理制度，确认本机构已建立授权审批机制，针对未能采取脱敏或加密处理的数据进行专项审批。 2.查阅审批报告，确认本机构开展了专项审批，且审批内容包括防止数据被泄露、误用、滥用的技术措施。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
9	数据通过信息系统与委托方进行传递时，应在相应的控制节点设置安全审计功能，对数据的外发与回传进行审计，其中信息系统包括API、摆渡服务器，控制节点包括信息系统业务功能、API、服务器用户。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档，确认已明确控制节点及其范围，且包括信息系统业务功能、API、服务器用户，并为其相应设置安全审计策略、审计周期和审计内容。 2.查阅审计记录，确认审计内容与实际情况一致，且符合审计周期要求。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
10	数据以纸质介质或磁盘等存储介质与委托方进行传递时，应执行相应的内部授权审批程序，对传递数据的内容、用途、量级，数据接收方情况、使用时长、数据是否回收或由对方进行销毁等情况进行说明与审批，有关记	1.文档查验	1.查阅管理制度或相关文档，确认已明确以纸质介质或磁盘等存储介质与委托方进行传递的授权审批程序，审批要素涵盖：对数据的内容、用途、量级，数据接收方情况、使用时长、数据是否回收或由对方进行销毁等。 2.查阅授权审批记录，确认本机构对以存储介质进行的数据传递行为进行了审批。 结果评价：

序号	安全要求	评估方法	结果判定
	录留档备查，其中数据接收方细化至法人机构数据安全负责人。		符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
11	应保存委托处理过程记录与有关数据的处理情况，并留档备查。	1.文档查验	1.查阅相关委托处理过程记录及处理情况，确认材料规范详实且得到妥善保管。 结果评价： 符合：满足以上第1项 不符合：不满足以上第1项

7.2.5.10 数据共享

数据共享安全评估内容见表 7.2.14。

表 7.2.14 数据共享安全评估内容

序号	安全要求	评估方法	结果判定
1	对于数据内部共享，应梳理数据共享的各类场景，明确各类场景的安全要求和责任部门，并建立相应的审核批准机制，对数据使用目的、内容、使用时间、技术防护措施、数据使用后的处置方式等进行审批，并留存相关记录。	1.文档查验	1.查阅相关制度或文档，确认已对数据共享场景进行了梳理和分类，明确了各类场景的安全要求和责任部门。 2.查阅数据共享相关制度或策略文件，确认建立了规范的数据内部共享审核机制，审核的内容至少包括数据共享目的、内容、范围、频度、使用场景、共享方式、使用期限、数据等级、责任部门和责任人、共享参与方权责、技术防护措施、数据使用后的处置方式等。 3.查阅数据共享审批记录，确认数据共享行为符合数据共享制度，履行数据审核批准机制，对审批流程进行了记录并可对过程进行追溯。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	对于数据内部共享，在数据共享前，应开展数据安全影响评估，对共享的数据内容、数据范围、时间周期、传输方式、用途、安全管控手段等要素进行评估，涉及个人金融信息的不应超出其授权范围，数据安全保护强度不因数据共享而降低。	1.文档查验	1.查阅数据安全影响评估报告等相关文档，确认数据共享前已开展数据安全影响评估，且评估事项至少包括共享使用目的、数据内容、共享方式、数据范围、数据安全级别、时间周期、传输方式、用途、安全管控手段、是否涉及个人金融信息、共享风险、风险控制措施等。 2.对于涉及个人金融信息的数据共享，查阅数据安全影响评估报告等相关文档，确认个人金融信息的使用未超出授权范围，且所共享数据的安全保护要求与共享前保持一致。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。

序号	安全要求	评估方法	结果判定
3	对于数据内部共享，应对 2 级以及上的数据共享过程留存日志记录，记录内容至少包括共享内容、共享时间、防护技术措施等。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关业务及技术管理人员，确认本机构进行了数据分级、共享场景梳理和共享日志记录。 2.查阅共享日志、共享记录及相关文档，确认记录内容至少包括共享内容、共享时间，并明确了防护技术措施等。 3.查验并确认在不同共享场景下，针对2级及以上数据进行共享时，相关共享方式或共享平台可以留存日志记录，并做到全程可追溯。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	对于数据内部共享，采取以下措施确保 3 级及以上数据共享的安全性： ——原则上应对 3 级及以上数据进行脱敏； ——若因业务确需，无法对数据进行脱敏的，应对共享内容通过专项审批，并对数据进行加密、选用安全可靠的传输协议或在安全可控的环境中进行共享； ——脱敏方式的选取宜充分结合数据共享场景、业务需要和安全风险评估结果，选择被猜解或碰撞风险相对较低的脱敏技术； ——脱敏措施的部署应尽可能靠近数据源头，如数据库视图、应用系统底层 API 接口等。	1.文档查验 2.人员访谈 3.旁站验证	1.查阅相关制度及管理要求，确认本机构对于3级及以上数据有明确的脱敏规则和脱敏方法说明。 2.查阅相关制度及管理要求，确认本机构对数据内部共享有明确的管理制度和管理流程，对3级及以上数据未进行脱敏开展数据共享的，建立审批流程。 3.在数据接收端查验数据脱敏具体实现，对照数据共享审批记录，确认3级及以上共享数据均进行了脱敏处理。 4.对于没有进行脱敏的3级及以上共享数据，查阅相关文档，确认不进行脱敏的必要性，并通过旁站验证等方式确认使用数据加密、安全传输等功能，且能够确保共享环境安全可控。 5.查阅信息系统设计文档，确认脱敏措施的部署靠近数据源头，如数据库视图、应用系统底层API接口等，并通过旁站验证等方式确认各环节数据脱敏情况，且脱敏功能按照信息系统设计文档实施。 6.查阅相关制度及数据使用记录材料，确认数据脱敏方式的选取充分结合数据共享场景、业务需要和安全风险评估结果，被猜解或碰撞风险相对较低。（可选项） 结果评价： 符合：满足以上第1至5项或第1至6项。 基本符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
5	对于数据内部共享，不应共享 4 级数据。	1.文档查验 2.旁站验证	1.查阅并确认数据共享制度或策略文档，且已明确要求不能共享4级数据。 2.查阅共享审批记录、共享日志、共享记录等文档，确认未共享4级数据。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。

序号	安全要求	评估方法	结果判定
6	对于数据内部共享，利用自动化工具如代码、脚本、接口、算法模型、软件开发工具包等进行数据共享时，应通过身份认证、数据加密、反爬虫机制、攻击防护和流量监控等手段，有效防范网络监听、接口滥用等网络攻击，并定期检查和评估自动化工具安全性和可靠性。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈并组织问卷调查，确认本机构数据共享使用代码、脚本、接口、算法模型、软件开发工具包等自动化工具时，采用了必要的技术控制手段，防范网络监听、接口滥用等网络攻击。 2.查阅自动化工具接口规范等文档，确认记录了自动化工具接口的访问参数，比如账户、内容、IP、MAC、访问时间等信息，并进行必要关联分析。 3.查验身份认证、数据加密、反爬虫机制、攻击防护和流量监控等安全系统功能，并演示相关功能界面和事件记录，确认相关功能正常。 4.查阅数据共享相关制度，确认已制定定期检查和评估自动化工具安全性和可靠性的相关条目，并查验定期检查和评估记录，立即停用不符合要求的自动化工具。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
7	对于数据内部共享，数据使用部门应根据共享前约定的数据使用期限，对数据进行安全处置，数据共享方应对处置结果进行确认。	1.文档查验 2.人员访谈	1.查阅数据共享审批记录或合同约定，对照共享日志、共享记录、使用部门处置记录等，确认数据使用部门严格按照约定的使用期限使用并处置数据。 2.访谈数据使用部门，确认已明确数据使用期限，且明确数据到期后处置措施，处置措施包括删除、销毁、加密存储等。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
8	对于数据外部共享，应满足表7.2.14第1至7项安全要求。	同表7.2.14第1至7项	同表7.2.14第1至7项
9	对于数据外部共享，应与数据接收方通过合同协议等方式，明确双方在数据安全方面的责任及义务，并约定共享数据的内容和用途、使用范围等。	1.文档查验	1.查阅涉及数据外部共享的合同协议等约定条款，确认已书面明确双方数据保护权责划分，明确共享数据的内容和用途、使用范围、数据期限和到期处置方式等内容要求。 2.查阅涉及外部数据共享的合同协议等约定条款，确认已书面明确双方数据保护权责划分，明确共享数据的内容和用途、使用范围、数据期限和到期处置方式等内容要求。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
10	对于数据外部共享，应定期对数据接收方的数据安全保护能力进行评估，确保数据接收方具备足够的数据安全保护能力，当数	1.文档查验 2.人员访谈 3.问卷调查	1.查阅相关制度或评估报告，确认数据接收方在组织架构、内控管理、意识培训、技术防护、合同履约、应急保障等方面具备的数据安全保护能力。

序号	安全要求	评估方法	结果判定
	据接收方丧失数据安全保护能力时，应启动应急响应程序。		2.查阅金融业机构针对共享数据安全事件的应急预案相关文件，确认预案至少包括数据安全应急处置组织架构、应急响应程序、应急资源准备、应急人员联系方式等内容，还应针对应急预案制定演练方案，定期开展应急演练，规范记录演练过程，相关人员熟悉数据安全应急响应流程和步骤。 3.访谈并组织调查数据接收方过往发生数据安全事件或丧失数据保护能力的情况，查验相关文档，确认金融业机构按照应急预案启动应急响应程序。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
11	对于数据外部共享，应向个人金融信息主体等告知共享数据的目的、数据接收方的类型，并事先征得相应授权。	1.文档查验 2.问卷调查	1.查阅相关制度或管理规定，确认本机构数据对外共享具有授权告知程序、流程和功能，至少包括告知书、公示、短信或电话等方式，向个人金融信息主体告知包括共享数据目的、数据接收方类型、共享期限、法律责任等信息，用户拒绝共享的，不能对相关数据进行外部共享。 2.查阅隐私政策、与客户的合同协议等文档，确认本机构对数据共享事项向金融信息主题进行了告知，且包括了共享数据目的、数据接收方类型。用户拒绝共享的，信息系统不能对相关数据进行共享。 3.问卷调查个人金融信息主体，确认其已知悉数据共享事宜。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
12	对于数据外部共享，应帮助个人金融信息主体等了解数据接收方数据的存储、使用等情况。	1.文档查验 2.问卷调查	1.查阅隐私政策、与客户的合同协议等文档，确认本机构数据对外共享前已告知个人金融信息主体数据接收方的情况，或提供便利措施，引导个人金融信息主体获得相关内容。 2.问卷调查个人金融信息主体，确认其已知悉数据对外共享事宜，以及了解数据接收方相关情况。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
13	对于数据外部共享，应执行以下安全控制措施：——共享数据涉及 2 级、3 级数据时，应对数据进行加密处理，并采取数据标记、数据水印等技术，降低数据被泄露、误用、滥用的风险；	1.文档查验 2.旁站验证	1.查阅信息系统设计文档及合同协议等文档，确认已明确需数据外部共享的业务场景、所共享数据安全级别，并针对2级、3级数据已在加密的基础上采取标记、水印等技术措施。 2.查阅数据安全审计报告，确认本机构定期对数据共享进行安全审计，且审计报告内容详实完备。报告至少包括数据的使用

序号	安全要求	评估方法	结果判定
	——应定期对共享的数据进行安全审计； ——应配套建立应急响应机制，必要时应及时切断数据共享。		对象、使用期限、使用范围、操作记录、存储方式、到期处置情况等内容。 3.查阅并确认具备共享场景相关数据安全应急预案，预案内容至少包括应急组织架构、应急响应程序、应急资源准备、应急人员联系方式等，并已明确切断数据共享的条件和具体操作方式。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
14	对于数据外部共享，应按照国家及行业主管部门有关要求，向行业主管和监管部门等有关机构履行数据报送义务时，应采取有效措施确保数据接收方的身份真实性、数据的保密性、真实性与完整性。	1.问卷调查 2.人员访谈 3.文档查验 4.旁站验证	1.访谈并确认依据国家和行业主管部门对于外部共享数据报送的要求，已明确包括报送方式、报送途径、报送周期、报送接收部门或人员等要求。 2.查验针对报送数据进行的安全保护措施，确认采用专网专人报送、数字证书等方式确保数据接收方身份真实性，使用数据加密、数字签名等方式确保数据传输过程保密性、真实性和完整性。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。

7.2.6 数据删除

数据删除安全评估内容见表7.2.15。

表7.2.15 数据删除安全评估内容

序号	安全要求	评估方法	结果判定
1	应依据国家及行业主管部门有关规定及与个人金融信息主体约定的时限等，针对不同类型的数据设定其数据保存期，对于多个不同保存期数据的集合，保存期限选择最长时限为该数据集合的保存期。	1.文档查验 2.旁站验证	1.查阅并确认具备数据删除相关制度、策略文档，且已明确对于不同类型数据保存期、以及多个数据集合的保存期的规定，保存期应符合数据安全相关法律法规、行业规章、制度标准的要求。其中，对于多个不同保存期数据的集合，选择其中最长保存时限作为该数据集合的保存权限。 2.演示不同类型数据以及多个数据集合的实际保存期情况，确认符合相关管理制度或合同约定的要求。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
2	超过国家及行业主管部门有关规定、内部规章及合同协议所述保存期限的数据，应执行数据删除操作。	1.人员访谈 2.问卷调查 2.文档查验 3.旁站验证	1.访谈并组织问卷填写，调查数据删除执行依据、执行方式，同时查验信息系统数据删除日志，确认被删除数据的保存期限符合法律法规、监管规定、内部规章或合同协议的要求。 2.演示数据删除功能与机制，确认已被删除的数据不能被检索、访问和使用。

序号	安全要求	评估方法	结果判定
			结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
3	应采取技术手段，在金融产品和服务所涉及的系统中去除待删除的数据。	1.文档查验 2.旁站验证	1.查阅金融产品和服务涉及信息系统的设计文档，确认可通过技术手段去除待删除的数据。 2.演示使用技术手段去除待删除数据，确认有删除记录或日志，确认任何产品和信息系统均不能检索、访问和使用已删除数据。 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第1项。
4	开发测试、数据分析等金融业机构内部数据使用需求执行完毕后，应由数据使用部门依据金融业机构数据删除有关规定，对其使用的有关数据进行删除，记录处理过程，并将处理结果及时反馈至内部数据安全管理部门，由其进行数据删除情况确认。	1.文档查验 2.配置核查 3.人员访谈	1.查阅数据删除相关制度、操作规程，确认开发测试、数据分析等内部数据删除要求应符合国家法律法规和行业监管要求。 2.查验开发测试、数据分析环境的数据删除记录、删除日志，确认数据使用和删除符合金融业机构数据安全管理要求。 3.访谈相关人员，确认内部数据安全管理部门已对数据使用部门删除数据情况进行确认，并核对确认记录与使用部门删除记录一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
5	3 级及以上数据应建立数据删除的有效性复核机制，定期检查能否通过业务前台与管理后台访问已被删除数据。	1.文档查验 2.工具测试	1.查阅数据删除相关制度、策略文档，确认对 3 级及以上数据删除建立了完备的申请、审核、复核流程机制，能够确保超过保存期限的数据得到有效删除。 2.查阅并确认具备对于生产环境、测试环境、容灾备份环境中被删除 3 级及以上数据的复核记录。 3.查阅数据删除记录或日志，并分别在业务前台和管理后台访问测试已删除数据，确认已删除数据不能再被访问。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
6	个人金融信息主体要求删除个人金融信息时，应依据国家及行业主管部门有关规定，以及与个人金融信息主体的约定予以响应。	1.文档查验 2.旁站验证	1.查阅并确认具备数据删除相关制度、策略文档或操作规程，且包括涉及个人金融信息主体要求删除个人金融信息的申请方法、响应流程和响应时间等要求。 2.查验个人金融信息主体要求删除个人金融信息的操作步骤和响应流程，确认其符合国家、行业和内部制度规定要求。

序号	安全要求	评估方法	结果判定
			3.查阅用户申请记录，对照数据删除记录或日志，确认已按国家及行业主管部门要求、或在合同约定的时间内，按个人金融信息主体要求删除了个人金融信息。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
7	在停止其提供的金融产品或服务时，应对其在提供该金融产品或服务过程中所收集的个人金融信息进行删除或匿名化处理，与个人金融信息主体另有约定的除外，国家及行业主管部门另有规定的按照相关规定执行。	1.文档查验 2.人员访谈 3.旁站验证	1.查阅数据删除相关制度、策略文档或操作规程，确认有对于金融产品或服务停止使用后数据删除和处置的相关要求。 2.访谈或调查本机构已停止使用的产品和停止提供的服务，查阅其设计文档、合作协议、日志记录等资料，确认其收集的个人金融信息内容，以及停止服务后的个人金融信息处置方式等。 3.查验已停用产品和服务的数据删除记录或日志，确认个人金融信息均已删除，没有删除的应查验并确认已匿名化收集个人金融信息，否则应有其他合理的理由。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
8	金融产品或服务的用户主动提出删除其数据的情形，如账户注销，应对其相应信息进行删除，与个人金融信息主体另有约定的除外，国家及行业主管部门另有规定的按照相关规定执行。	1.文档查验 2.人员访谈 3.旁站验证	1.查阅并确认具备数据安全相关制度、策略文档，以及金融产品或服务的设计文档、合同约定等，确认已明确按照用户要求进行账户注销、删除数据等条目的要求。 2.查验并确认金融产品或服务用户自主提出删除数据时的相关操作方式、操作步骤和响应方式。 3.查验并确认用户自主申请删除数据的记录，对照查验数据删除记录日志，没有按用户要求删除的应有合法合规的理由和依据。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。

7.2.7 数据销毁

数据销毁安全评估内容见表7.2.16。

表 7.2.16 数据销毁安全评估内容

序号	安全要求	评估方法	结果判定
1	应制定数据存储介质销毁操作规程，明确数据存储介质销毁场景、销毁技术措施，以及销毁过程的安全管理要求，并对已共享或已被机构内部部门使用的数	1.文档查验	1.查阅数据销毁相关制度，确认已结合数据分类分级要求，建立数据存储介质（闪存、移动硬盘、固态硬盘、硬盘、磁带、光盘等）销毁操作规程，明确数据销毁安全管理要求（责任人员、责任部门、申请授权、双人复核、操作步骤等），并对于不同介质销毁场景（如业务下线、服务停止、用户注销、节点失效、过多备份、数据试用结束、超出数据保存期限等），有

序号	安全要求	评估方法	结果判定
	据提出有针对性的数据存储介质销毁管控规程。		明确的销毁技术措施或销毁要求（物理销毁如高压击穿、消磁及熔炉焚化、熔炼、借助外力研磨、粉碎磁盘表面等，化学销毁如运用化学物质溶解、腐蚀、活化、溶解等）。 2.对于已共享的数据，查阅数据销毁操作规程或数据共享等相关数据安全管理制度，确认已明确对共享数据存储介质的销毁要求，并查阅共享记录、审批文档和已销毁介质情况，确认符合管理要求。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
2	存储数据的介质如不再使用，应采用不可恢复的方式如消磁、焚烧、粉碎等对介质进行销毁处理。	1.文档查验 2.旁站验证	1.查阅数据销毁相关制度，确认已明确对于不再使用的存储数据提出采用不可恢复的方式对介质进行销毁处理。 2.查阅销毁申请审批记录或销毁过程记录等记录了存储介质销毁方式的文档，确认采用了不可恢复的方式（如消磁、焚烧、粉碎等）对介质进行销毁。 3.查验并确认物理销毁或化学销毁的设施设备可达到不可恢复的销毁效果。（可选项） 结果评价： 符合：满足以上第 1 至 2 项或第 1 至 3 项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
3	存储介质如还需继续使用，不应只采用删除索引、删除文件系统的方式进行数据销毁，应通过多次覆写等方式安全地擦除数据，确保介质中的数据不可再被恢复或以其他形式被利用，具体措施至少包括： 1)采用数据擦除方式销毁数据时，明确定义数据填充方式与擦除次数如全零、全一以及随机零一最少填写 7 次，并保证数据擦除所填充的字符完全覆盖存储数据区域。 2)通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据销毁结果。 3)针对数据擦除后擦除失败的存储介质，进一步采用物理方式进行销毁。	1.文档查验 2.工具测试	1.查阅并确认数据销毁相关制度、规程和策略中对于使用数据擦除方式进行数据销毁的要求，一是应明确不应只采用删除索引、删除文件系统的方式进行销毁，而是应通过多次覆写等方式进行销毁，确保介质中的数据不可再被恢复或被其他形式利用；二是应要求使用数据恢复工具或数据发现工具验证数据销毁结果；三是应要求对于擦除失败的介质，应采用消磁、粉碎等方式进行物理销毁。 2.查阅并确认具备数据销毁工具、程序或模块的设计文档或使用说明，并查验数据擦除操作过程，确认擦除方式符合要求。 3.查阅并确认数据销毁记录和验证记录，且对于擦除或验证销毁未成功的，确认已进一步采用物理销毁的方式。 4.通过数据恢复工具或数据发现工具抽样查验已完成数据擦除销毁的存储介质，确认已销毁数据不可恢复。 结果评价： 符合：满足以上第 1 至 4 项。 不符合：不满足以上第 1 至 4 项中的一项或多项。

序号	安全要求	评估方法	结果判定
4	应明确数据销毁效果评估机制，定期对数据销毁效果进行抽样认定，通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据删除结果。	1.文档查验 2.工具测试	1.查阅数据销毁相关制度、规程和策略，确认已明确对数据销毁效果进行评估，确定评估周期、检查方式等要求。 2.查阅数据销毁效果评估报告或记录，确认内容包括评估时间、评估人、评估介质编号、数据类型、数据等级、销毁方式、验证方式、验证结果等内容。 3.对于使用数据擦除进行的数据销毁，确认已使用数据恢复工具或数据发现工具对已删除数据进行恢复测试，并确认评估报告结果。 结果评价： 符合：满足以上第 1 至 3 项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
5	应采取双人制实施数据销毁，分别作为执行人和复核人，并对数据销毁全过程进行记录，定期对数据销毁记录进行检查和审计。	1.文档查验	1.查阅并确认具备数据销毁相关制度、规程和策略，针对销毁过程应有执行人、复核人的双人制安全管理要求，并要求对销毁过程进行详细的记录，记录的要素至少包括存储介质类别、介质编号、介质所属单位（部门）、销毁服务机构、介质应用系统、数据类型、数据安全等级、销毁方式、销毁地点、销毁时间、执行人、复核人、监督人等。 2.查阅数据销毁记录，确认记录内容符合销毁相关制度、规程和策略的要求。 3.查阅并确认数据销毁检查或审计记录，审计内容应包括存储介质销毁台账与实际情况的一致性，销毁审批手续履行到位的情况，销毁过程记录要素的完备性，对销毁效果进行评估等。 结果评价： 符合：满足以上第 1 至 3 项。 基本符合：满足以上第 1 项。 不符合：不满足以上第 1 项。
6	3 级及以上数据存储介质不应移作他用，销毁时应采用物理销毁的方式对其进行处理，如消磁或磁介质、粉碎、融化等。	1.文档查验 2.旁站验证	1.查阅数据销毁相关制度、规程和策略，确认已明确 3 级及以上数据存储介质再使用时不可改变其使用环境和性质、不再使用的 3 级及以上的数据存储介质应采用物理销毁方式进行销毁的安全要求。 2.查阅数据销毁记录，确认 3 级及以上数据存储介质使用消磁或磁介质粉碎、融化等方式进行销毁。 3.查验已再使用的 3 级及以上数据存储介质编号，对照数据存储介质使用记录，确认未改变其使用环境和性质。 结果评价： 符合：满足以上第 1 至 3 项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
7	4 级数据存储介质的销毁应参照国家及行业涉密载体管理有关规定，由具备相应资质的服务机构或数据销毁部门进行专门	1.文档查验	1.查阅数据销毁相关制度、规程和策略，确认已明确 4 级数据存储介质的销毁应参照涉密载体管理规定，由专业机构进行处理，本机构相应岗位人员应对销毁过程进行全程监督求。

序号	安全要求	评估方法	结果判定
	处理，并由金融业机构相应岗位人员对其进行全程监督。		2.查阅数据销毁记录，确认 4 级数据销毁服务机构、资质情况、销毁方式、销毁地点、销毁时间、监督人等符合管理要求。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 项中的一项或多项。

8 金融数据安全运维评估 S3

8.1 边界管控

边界管控评估内容见表8.1.1。

表8.1.1 边界管控评估内容

序号	安全要求	评估方法	结果判定
1	应在内网边界按照“最小权限”原则严格控制外部机构的访问权限，管控措施至少包括：防火墙、入侵防御、应用安全防护、API 网关、数据安全防护等。	1.人员访谈 2.文档查验 3.旁站验证 4.配置核查	1.访谈相关人员并查阅网络建设和运维相关文档,确认制订了对外部机构的访问控制策略和措施，并要求访问控制符合“最小权限”原则。 2.查验并确认内网边界处已按照网络建设、运维文档要求，部署防火墙、入侵防御、应用安全防护、API 网关或数据安全防护等管控设备。 3.查阅外部机构的访问申请授权文档,并比对管控设备访问控制策略已严格按照授权进行配置,确认不存在多余或无效访问控制规则，且配置符合“最小权限”原则。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
2	互联网区和外联接入区为不可控区域,应在内部可控区域与不可控区域之间进行隔离,并根据应用需求和数据传输需要逐一开通访问关系，默认为禁止访问。	1.人员访谈 2.文档查验 3.旁站验证 4.配置核查	1.访谈相关人员并查阅网络建设和运维文档,确认外联接入区和互联网区对生产网等内部区域的数据访问设计了有效的隔离措施。 2.查验并确认根据应用需求和数据传输需求开通访问关系的申请及审核记录。 3.查验网络配置文件,确认可控区域与不可控区域之间默认为禁止访问，已设置的访问控制规则与申请审核记录一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
3	应避免将重要网段部署在网络边界处且直接连接外部信息系统,重要网段与其他网段之间应采取技术手段进行隔离。	1.人员访谈 2.旁站验证 3.配置核查	1.访谈相关人员，确认网络拓扑图已覆盖重要网段信息。 2.查验并确认网络拓扑图与实际网络运行环境一致,避免将重要网段部署在网络边界处且直接连接外部信息系统。 3.查验并确认重要网络区域与其他网络区域之间采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表（ACL）等。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
4	应明确生产网络接入和数据传输接口开通相关审批流程。	1.文档查验 2.人员访谈 3.配置核查	1.访谈相关人员并查阅网络管理相关制度规程，确认已制定明确的生产网络接入和数据传输接口开通申请审批流程，申请要素至少包括申请原因、接入或开通时间、涉及信息系统及数据内容、申请部门、使用人员、审批人员等。 2.查验相关审批记录，并进行配置核查，确认生产网络接入和数据传输接口开通情况与审批记录一致。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
5	数据跨边界传输应通过边界设备提供的受控接口进行通信。	1.人员访谈 2.旁站验证 3.配置核查	1.访谈相关人员并确认，在网络边界处已部署访问控制设备。 2.查验设备配置信息，确认已指定端口进行跨越边界的网络通信，指定端口已配置并启用了安全策略。 3.采用其他技术手段（如非法无线网络设备定位、查验设备配置信息等），确认不存在其他未受控端口进行跨越边界的网络通信。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
6	对使用 API 进行数据跨域流动的边界，应使用 API 防护技术，对 API 使用者进行身份认证，并对 API 访问行为进行检查，对异常访问行为采取限速、阻断等措施。	1.文档查验 2.旁站验证 3.人员访谈 4.工具测试	1.访谈相关人员并查验信息系统设计文档，确认内网边界使用 API 进行数据跨界流动时，对 API 使用者身份进行认证，对 API 行为进行检查，以及明确对异常访问的发现手段和控制措施。 2.演示 API 防护技术相关功能和 API 防护相关日志，确认身份认证、API 访问行为检查及异常访问行为处置等功能实施情况。 3.通过模拟 API 异常访问事件，查验 API 防护技术有效性，确认 API 访问行为检查和异常访问行为处置有效性。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
7	应使用设备主动发现等技术及时发现非授权设备私自连接到内部网络的情况，使用网络访问行为管理技术对内部网络私自连接到外部网络的行为进行检查，准确定位接入点，并对其进行有效阻断。	1.人员访谈 2.旁站验证 3.配置核查	1.访谈相关人员并确认已采用技术措施防止非授权设备接入内部网络。 2.查验并确认所有路由器、交换机等相关设备除业务、运维、应用、监控等端口均已关闭、禁用或有效控制。 3.查验防范非法内联和非法外联相关设备和策略配置情况，检查过往监测记录，确认能够准确定位接入点。 4.演示相关功能，确认对非法内联和非法外联的网络行为分析、攻击检测及预警、攻击阻断或限制、攻击行为记录等功能正常。

序号	安全要求	评估方法	结果判定
			结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
8	在内部建立 WLAN 时，接入终端应经过事先审批授权，采取网络准入控制措施，防止终端非法接入内部网络，并应采取终端合规检查、终端安全状态感知等技术手段防止操作系统管理权限被非法破解的终端设备接入内网 WLAN。	1.文档查验 2.旁站验证 3.配置核查 4.人员访谈	1.访谈相关人员，确认内部 WLAN 建立情况，终端接入手续和 WLAN 采取的网络准入控制措施。 2.查阅网络管理相关制度规程，确认已制定明确的接入申请审批流程，申请表中至少包括接入原因、接入时间、申请部门、使用人员、审批人员等信息。 3.查验 WLAN 终端接入审批记录，并查验网络设备配置文件，确认与审批情况一致。 4.查验终端管理情况，确认或查验存在防止操作系统管理权限被非法破解的能力或措施。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
9	终端通过互联网接入内网时，应采取代理或前置机等方式在边界网络区域落地，实现技术隔离，避免直接透传至内部网络。	1.人员访谈 2.文档查验 3.配置核查 4.人员访谈	1.访谈相关人员并查阅网络管理相关制度，确认明确了终端通过互联网接入内网的途径、接入点以及采取的技术隔离手段。 2.查阅网络拓扑图等相关文档，确认已采取了代理或前置机等方式进行部署。 3.查验代理或前置机配置情况，确认部署在边界网络区域，并采取技术隔离措施。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
10	应通过多因素认证技术，标识和验证使用者身份，使用设备证书确定设备身份，根据终端常用位置和目前位置、设备属性、安全状态、访问行为等信息动态授权其访问权限。	1.人员访谈 2.文档查验 3.旁站验证 4.人员访谈	1.访谈相关人员并查阅信息系统设计文档，确认已明确要求采用多因素认证，且具备根据终端常用位置和目前位置、设备属性、安全状态、访问行为等信息进行动态授权的功能。 2.查验信息系统多因素认证功能，确认动态授权等功能正常。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。

8.2 访问控制

8.2.1 访问控制策略

访问控制策略评估内容见表8.2.1。

表8.2.1 访问控制策略评估内容

序号	安全要求	评估方法	结果判定
1	应依据“业务必需、最小权限、职责分离”的原则，设计数据库	1.人员访谈 2.文档查验	1.访谈相关人员并查阅数据安全相关制度，确认已明确数据库系统与文件系统的用户权限大小、职责范围。

序号	安全要求	评估方法	结果判定
	系统与文件系统的用户鉴别和访问控制策略，并对各类系统用户设计其工作必需的最小访问权限。	3.配置核查	2.查阅数据库系统和文件系统设计文档，确认已依据“业务必需、最小权限、职责分离”的原则，根据各用户的权限、职责设计数据库系统与文件系统的用户鉴别和访问控制策略。 3.查验各系统的数据库与文件系统相关配置，确认用户鉴别及访问控制规则的配置与设计文档一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
2	应依据“业务必需、最小权限、职责分离”的原则，设计业务系统用户对系统业务功能与相应系统业务数据的访问控制策略，并对各类业务系统用户的访问控制实现方式和具体授权机制进行明确说明。	1.人员访谈 2.文档查验 3.配置核查	1.访谈相关人员并查阅业务系统相关制度，确认已明确业务系统用户的业务功能与业务数据访问权限。 2.查阅信息系统设计文档，确认已制定针对不同级别业务系统用户的用户鉴别和访问控制策略，其中业务系统用户包括管理员、操作员、审计员等，操作范围符合最小化原则，并对用户的访问控制实现方式和具体授权机制进行明确说明。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
3	访问控制策略应使用白名单机制，明确定义允许的行为。	1.人员访谈 2.文档查验 3.配置核查	1.访谈相关人员并查阅信息系统设计文档，确认访问控制策略使用白名单机制，并明确定义允许的行为。 2.查验各类访问控制策略，确认白名单配置情况，与信息系统设计文档一致。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
4	对数据库系统、存储系统、文件管理系统与存储介质管理有关管理员用户，应建立管理员身份标识与鉴别机制，并对其防控权限与操作规程进行详细说明。	1.文档查验 2.人员访谈 3.配置核查	1.访谈相关人员并查阅数据安全管理相关制度，确认已建立管理员身份标识与鉴别机制。 2.查阅信息系统设计文档，确认已按制度要求，详细说明具体防控权限与操作规程。 3.查验信息系统权限管理配置，确认管理员权限、操作范围与设计文档一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
5	应建立面向数据应用的安全控制机制，包括访问控制时效的管理和验证，以及应用接入数据存储的合法性和安全性取证机制，宜建立基于用户行为或设备行为的数据存储安全监测与控制机制。	1.文档查验 2.人员访谈 3.配置核查	1.访谈相关人员并查阅数据安全管理相关制度，确认包括面向数据应用的安全控制的管理要求，如：应用设计阶段，需审核应用的安全控制机制，包括单次访问连接超时机制等。 2.查验信息系统设计文档，确认包括访问控制实效管理和验证、应用接入数据存储合法性和安全性取证等面向数据应用的安全控制机制。如：应用设计评审阶段，需审核访问核心数据的存储时的合法性和安全性。

序号	安全要求	评估方法	结果判定
			3.查验信息系统相关配置，确认面向数据应用的安全控制机制，与设计文档一致。 4.查阅相关设计或说明文档，对数据存储安全检测与控制机制进行配置核查，确认该机制基于用户行为或设备行为。（可选项） 结果评价： 符合：满足以上第1至3项或第1至4项。 基本符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。

8.2.2 物理环境访问控制

物理环境访问控制评估内容见表 8.2.2。

表 8.2.2 物理环境访问控制评估内容

序号	安全要求	评估方法	结果判定
1	数据存储系统应部署在高安全等级区域，存储系统服务器与带库等设备机房出入口应部署电子门禁、视频监控等措施控制、鉴别和记录进入的人员。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查验数据存储系统所在机房，确认已按不同安全等级划分区域，区域存在显著标识，确认对各个区域都有专门的安全管理要求，数据存储系统已部署在高安全等级的区域。 2.查验数据存储系统所在机房，确认具备电子门禁、视频监控及入侵报警等基础设施，各项基础设施运行正常，其运行记录保存时间符合国家法律法规和等级保护等要求。 3.查验机房管理相关制度，确认存在门禁管理、出入管理、保密管理等内容，其中包括外来人员进出、门禁权限申请及权限变更等审批、登记流程。 4.查验门禁、视频、入侵记录及上述各项审批登记资料，确认无违规事件发生。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第 1 至 4 项中的一项或多项。
2	第三方机构人员访问存储系统服务器与带库区域应执行严格的授权审批程序，使用明显标识标志其访客身份，由金融业机构人员全程陪同，记录出入时间，并限制和监控其活动范围。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅相关管理制度，确认已建立明确的第三方机构访问授权审批流程，其中包括出入时间、出入原因、出入人员、携带物品、操作内容、操作结果、陪同人员、审批人员等。 2.查验机房门禁、视频监控记录及外来人员出入审批登记资料，确认第三方机构人员身份标识明确、由工作人员全程陪同且无违规事件发生。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
3	应对包括备份介质在内的存储介质出入库采取措施进行出入	1.人员访谈 2.文档查验	1.访谈相关人员并查阅存储介质管理相关制度，确认明确了对存储介质出入库采取安全措施进行控制的管理要求。

序号	安全要求	评估方法	结果判定
	库控制，并由金融业机构内部指定岗位人员完成，未经金融业机构授权，任何存储介质不应带离磁带库房。	3.旁站验证	2.查阅并确认存储介质出入库审批文档，存储介质出入库审批要素包括介质内容、介质形式、介质编号（或序列号）、介质数量、出入库原因、出入库时间、经手人员、审批人员等。 3.查验库房门禁、视频监控记录及介质出入库管理登记文档、岗位职责文档，确认无违规事件发生。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。

8.2.3 信息系统与介质访问控制

信息系统访问控制机制评估内容见表8.2.3。

表 8.2.3 信息系统访问控制机制评估内容

序号	安全要求	评估方法	结果判定
1	访问金融数据的业务应用系统用户角色的定义和权限设计应遵循以下原则：1)参考业务职能，确定系统中需设置的各类用户角色如经办人员、操作人员、管理人员、审计人员等权限。 2)用户角色定义和权限设计能够体现职责分离的安全制约原则，如经办人员和审计人员权限分离。 3)严格限制系统中缺省用户的权限。	1.人员访谈 2.文档查验 3.配置核查 4.旁站验证	1.访谈相关人员并查阅业务应用系统设计文档，确认已按相关制度要求进行角色设置及权限划分，并符合权限分离等安全制约原则。 2.演示业务应用系统，确认该系统中用户角色和权限分配情况与其设计文档一致，确认实际业务人员职责与该系统设置的用户角色职责一致。 3.查验业务应用系统，确认已对缺省用户的权限进行严格限制，如默认设置缺省用户无权访问资源或按最小授权原则对缺省用户进行授权。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
2	访问金融数据的业务应用系统用户角色的访问范围和方式应满足以下要求：1)控制用户对业务功能的访问范围，如功能菜单、业务文件、数据库表、表中的业务数据字段和其他资源。 2)控制用户对业务数据的访问方式，如读、写、删除、创建等。	1.人员访谈 2.文档查验 3.配置核查 4.旁站验证	1.访谈相关人员并查阅业务应用系统设计文档，确认已按相关制度要求对不同用户角色的访问范围（如功能菜单、业务文件、数据库表、表中的业务数据 字段和其他资源）和访问方式（如读、写、删除、创建）进行有效控制。 2.查验业务应用系统，确认其具备对不同用户角色设置不同访问范围和访问方式的功能。 3.查验并确认业务应用系统控制用户角色的访问范围和方式功能的有效性，尝试使用不同角色用户登录该系统，确认其匹配的访问范围和访问方式与该系统设置保持一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
3	访问金融数据的业务应用系统应具备登录失败处理功能，可采取结束会话、限制非法登录次	1.人员访谈 2.文档查验 3.配置核查 4.旁站验证	1.访谈相关人员并查阅业务应用系统设计文档，确认已按相关制度要求制定业务应用系统登录失败处理措施（如结束会话、限制非法登录次数、设置抑制时间或网络登录连接超时自动退出等）。

序号	安全要求	评估方法	结果判定
	数、设置抑制时间和网络登录连接超时自动退出等措施。		2.查验业务应用系统，确认其采用的登录失败处理措施与设计文档描述一致。 3.查验并确认示业务应用系统登录失败处理功能的有效性。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
4	对于承载 4 级及以上数据的信息系统，业务系统以及所承载的基础设施的访问，应结合访问者身份及系统安全状态进行访问授权和控制。	1.人员访谈 2.文档查验 3.配置核查 4.旁站验证	1.访谈相关人员，确认承载 4 级及以上数据的信息系统、业务系统和基础设施范围。 2.查阅信息系统设计文档，确认已按相关制度要求，对承载 4 级及以上数据信息系统，针对不同访问者、不同信息系统安全状态，制定了不同的授权机制及访问控制策略。 3.查验信息系统配置与设计文档一致，确认访问授权、访问控制等功能正常。 4.查验并确认不同访问者、不同信息系统安全状态下，对数据资源的访问授权和控制。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。

8.2.4 数据存储系统的访问控制

数据存储系统访问控制机制评估内容见表见表8.2.4。

表 8.2.4 据存储系统访问控制机制评估内容

序号	安全要求	评估方法	结果判定
1	存储系统应设计访问控制策略，并实现访问控制，对访问对象的访问范围和操作权限不超出预定义的范围，且满足最小授权原则。	1.人员访谈 2.文档查验 3.配置核查	1.访谈相关人员，确认存储系统的使用对象、使用场景及采用的访问控制策略。 2.查阅存储系统管理相关制度及存储系统设计文档，确认已按相关制度要求制定访问控制策略，并针对不同访问对象明确定义了访问范围和操作权限。 3.查验存储系统相关配置，确认其采用的访问控制策略与系统设计文档描述一致。 4.演示不同访问对象对存储系统的访问，确认访问范围和操作权限没有超出预定义的范围，且满足最小授权原则。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。
2	存储系统访问控制机制应对业务平面和管理平面各自可访问的资源策略进行独立配置，并对业务平面和管理平面的相互访问进行隔离。	1.人员访谈 2.文档查验 3.配置核查	1.访谈相关人员并查阅存储系统设计文档，确认已按相关制度要求，对业务和管理进行资源独立授权和访问隔离，并具有相应访问隔离措施。

序号	安全要求	评估方法	结果判定
			2.查验业务用户和管理用户登录存储系统，确认已实现区分业务权限和管理权限资源授权的独立配置，业务权限和管理权限相互访问已采取隔离措施，彼此访问资源无任何相关性。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
3	应使用存储访问控制模块部署数据用户身份标识与鉴别策略、数据访问控制策略、数据扩容及复制策略，并执行相关安全控制措施。	1.人员访谈 2.旁站验证	1.访谈相关人员并查阅信息系统设计文档，确认已按相关制度要求，设计访问控制模块，并制定了数据用户身份标识与鉴别、数据访问控制、数据扩容及复制等策略。 2.查验存储系统访问控制模块功能，确认其与设计文档描述一致，相关策略处于生效状态。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
4	对访问存储业务的应用进行鉴别，对应用身份进行唯一标识，并将标识和与其相关的所有可审计事件相关联，且不应存在可绕过鉴别机制的访问方式。	1.人员访谈 2.文档查验 3.旁站验证 4.工具测试	1.访谈相关人员并查阅存储系统设计文档，确认已按相关制度要求，设计身份鉴别机制。 2.查验存储系统日志记录，确认已对应用身份进行唯一标识，并查阅事件日志中的事件已与应用身份标识关联。 3.查验并确认不存在绕过鉴别机制的访问方式，或直接提供相关渗透测试报告。（可选项） 结果评价： 符合：满足以上第1至2项或第1至3项。 不符合：不满足以上第1至2项中的一项或多项。
5	存储 3 级及以上数据的系统应采用数字证书、多因素身份认证等技术对用户进行身份鉴别，并完整记录用户行为，供事后审计。	1.人员访谈 2.文档查验 3.操作验证	1.访谈相关人员，确认数据分级情况，以及 3 级以上数据采用的身份鉴别机制。 2.查阅信息系统设计文档，确认已按相关制度要求，采用数字证书、多因素身份认证等技术对用户进行身份鉴别。 3.查验信息系统日志记录，确认已完整记录用户行为。 4.查验信息系统的身份鉴别功能，确认功能与设计文档描述一致。 结果评价： 符合：满足以上第1至4项。 不符合：不满足以上第1至4项中的一项或多项。

8.3 安全监测

8.3.1 数据溯源

金融业机构如具备数据溯源能力，评估内容可参见表8.3.1。

表8.3.1 数据溯源能力评估内容

序号	安全要求	评估方法	结果判定
1	应制定金融数据溯源的策略和机制，明确溯源数据的安全存储、分析使用等管理制度。	1.人员访谈 2.文档查验	1.访谈相关人员并查阅相关文件，确认正式发布的溯源数据管理内容的文件制度，覆盖数据溯源相关策略和机制，溯源数据的安全存储、分析使用等内容 结果评价： 符合：满足以上第1项。 不符合：不满足以上第 1 项。
2	应标识外部数据的来源合法性，并对外部数据的真实性和准确性等数据质量进行评估。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员，查阅数据评估记录或报告，确认覆盖外部数据真实性、准确性等数据质量相关内容。 2.查验与外部数据供应商签订相关合约性文件，确认已对外部数据的真实性和准确性提出了相应的要求及双方约束性条款。 3.查验信息系统设计文档，确认具备对外部数据的来源合法性进行标记的功能。 4.查验并确认数据库或文件系统中的外部数据来源合法性标记。 结果评价： 符合：满足以上第 1 至 4 项。 基本符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
3	宜建立金融数据资产地图，从数据类型、数据量级、数据特征等维度对金融数据进行盘点和梳理，按需对特定数据对象进行标记和跟踪，构建和维护数据血缘关系。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员，确认数据资产地图实现方式，按需实现对特定数据对象的标记和跟踪，构建、维护数据血缘关系。（可选项） 2.通过信息系统实现的，查验信息系统设计文档，确认覆盖了数据资产地图功能，并实现数据盘点梳理、跟踪标记等功能设计。（可选项） 3.通过信息系统实现的，查验数据资产地图相关功能，确认功能正常。（可选项） 4.通过人工方式实现的，查验相关文档，确认从数据类型、数据量级、数据特征等维度对金融数据进行盘点和梳理。（可选项） 结果评价： 符合：满足以上第1至3项或满足1、4项。 不符合：不满足以上第 1 至 3 项中的一项或多项或不满足第 1、4 项中的一项或多项。
4	应记录数据操作过程及关键数据要素，在出现数据泄露事件后可根据泄露的数据进行溯源。	1.人员访谈 2.文档查验 3.旁站验证 4.工具测试	1.访谈相关人员并查阅信息系统设计文档，确认覆盖了数据采集、传输、存储、使用、删除、销毁等数据生命周期相关操作溯源能力设计。 2.查验数据溯源相关操作，如数据标注、标签嵌入与验证、水印嵌入与提取等，查验并确认数据操作的溯源性。

序号	安全要求	评估方法	结果判定
			3.通过模拟数据泄露事件，查验对应数据已记录数据操作过程及关键数据要素，查验并确认对泄露数据溯源的有效性。（可选项） 结果评价： 符合：满足以上第1至2项或第1至3项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
5	宜构建数据溯源的安全模型，增强数据操作的可追溯性。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅信息系统设计文档，确认覆盖了数据溯源安全模型及其系统实现相关设计。（可选项） 2.查验数据溯源安全模型系统中的溯源功能，并确认功能正常。（可选项） 结果评价： 符合：满足以上第1至2项。 基本符合：满足以上第1项。 不符合：不满足以上第 1 项。
6	应对关键溯源数据进行备份，并采取技术手段对溯源数据和备份数据进行安全保护。	1.人员访谈 2.文档查验 3.配置核查	1.访谈相关人员，确认关键溯源数据的备份和采取的备份保护技术手段的实现方式。其中，关键溯源数据至少包括：3 级以上核心数据或高等级业务系统中的数据等。 2.查阅信息系统设计文档，确认关键溯源数据的备份机制、备份策略，以及采用密码技术、权限控制等技术措施保证溯源数据和备份数据的完整性、可用性、保密性。 3.查验并确认数据存储或备份管理平台中溯源数据和备份数据的技术防护手段和信息系统设计文档一致。 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第 1 至 3 项中的一项或多项。
7	应采取访问控制、加密等技术措施保证溯源数据的安全性。	1.人员访谈 2.文档查验 3.配置核查	1.访谈相关人员，并查阅信息系统设计文档，确认溯源数据采取访问控制、加密等技术进行防护。 2.查验数据存储相关平台或信息系统中溯源数据技术防护手段和信息系统设计文档一致，确认对溯源数据采取了加密等安全措施；确认对访问数据的权限，采取最小化、分立等访问控制原则。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
8	应以泄露数据为线索，建立对高安全等级数据事件记录进行检索溯源的机制，支持对接口、IP、账号、时间进行溯源集中度分析，定位追踪到相关责任人。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员，并查阅信息系统设计文档，确认具备对高安全等级数据事件记录进行检索溯源的能力，覆盖了对接口、IP、账号、时间集中度分析，具备定位追踪的功能设计。 2.查验溯源系统的运行，查验数据操作的追溯情况（包括高安全等级数据事件），抽样检查并确认按照应用、接口、IP、账号、时间进行溯源集中度分析，确认定位追踪到相关责任人。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
9	应建立以批量泄露数据、多类型数据作为线索进行溯源的能力，加强基于数据线索的数据溯源分析能力，加强数据溯源的时效性和准确率。	1.人员访谈 2.文档查验 3.旁站验证 4.工具测试	1.访谈相关人员，并查阅信息系统设计文档，确认具备以批量泄露数据、多类型数据作为线索进行溯源能力。 2.查验相关溯源功能，确认能够按照批量泄露数据、多类型数据作为线索进行溯源。 3.测试检查溯源系统的运行情况，抽样检查并确认支持批量数据和多类型数据的分析、溯源能力，检查数据溯源的实效性和准确性能力。 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
10	宜建立主体溯源分析能力，对涉及高安全等级数据的疑似泄露事件进行影响范围评估，做好同范围内尚未泄露的数据安全保护工作。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅设计文档，确认已建立主体溯源分析能力，针对疑似泄露事件进行预警和泄漏情况统计，并确认已开展影响范围评估和未泄露数据的安全保护工作。（可选项） 2.查验溯源系统，确认能够按照主体进行溯源分析，具备识别高安全等级数据的能力，能够针对疑似泄露事件进行预警和泄漏情况统计，指导后续的影响范围评估工作。（可选项） 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。

8.3.2 流量分析

流量分析能力评估内容见表8.3.2。

表8.3.2 流量分析能力评估内容

序号	安全要求	评估方法	结果判定
1	宜采取流量分析技术对数据采集、传输、处理、分析等关键节点进行监测。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅设计文档，确认覆盖对数据采集、传输、处理、分析等关键节点的监测能力设计。（可选项） 2.查验流量分析系统或设备，确认可以有效监测数据采集、传输、处理、分析等关键节点。（可选项） 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
2	应部署以数据为中心的数据流量分析系统，识别并分析高安全等级数据流动情况，包括流动类型、流动范围、数据载体、日均量级、数据账号访问情况、数据流向等信息，并对异常流量、行为等进行告警。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅流量分析系统或设备产品说明书、信息系统设计文档等技术资料，确认具备识别并分析高安全等级数据流动情况，包括：数据的流动类型、流动范围、数据载体、日均量级、数据账号访问情况、数据流向等信息，并对异常流量、行为等进行告警的能力。

序号	安全要求	评估方法	结果判定
			2.查验流量分析系统或设备，确认能够识别并分析数据的流动类型、流动范围、数据载体、日均量级、数据账号访问情况、数据流向等信息，并具备针对异常流量、行为等的告警功能。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
3	应对比分析流量中数据流动异常情况如不安全的采集设备与采集内容、非授权时段访问高安全等级数据、未授权访问、频繁访问、超量数据传输、多次尝试、批量下载等，及时发现风险问题并进行处置。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员，确认实现数据流动异常情况的监测分析和处置的方式。 2.若采用人工分析方式，查阅并确认已留存分析日志、事件记录等资料。 3.若采用信息系统或产品实现，查验流量分析系统或设备产品说明书、信息系统设计文档等技术资料，确认具备对数据流动异常情况和访问行为的监测、处置能力。 4.若采用信息系统或产品实现，查验系流量分析系统或设备，确认具备对数据流动异常情况和访问行为的监测、记录及报警功能；检查针对已发现的异常情况已处置。 结果评价： 符合：满足以上第1至4项。 基本符合：满足以上第1至2项或满足以上第1、3、4项。 不符合：不满足以上第 1 至 2 项中的一项或多项或不满足以上第 1、3、4 项中的一项或多项。
4	宜对比分析数据流量变化和规律，构建数据流动流量基线和高安全等级数据流动基线，及时形成总结报告，并对安全防护措施进行针对性调整。	1.人员访谈 2.文档查验 3.配置核查	1.访谈相关人员并查阅总结报告、数据流量监测基线相关等文档，确认基线根据数据流量情况制定了对应防护措施。（可选项） 2.查验并确认留存安全措施调整记录，且安全防护措施的配置情况与基线规范相符合。（可选项） 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
5	应对互联网出口流量进行实时检测，发现数据流量异常、数据流向未经授权等行为并及时处置。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅流量异常情况分析和处置记录，确认对数据流量异常、数据流向未经授权等异常情况进行了监测分析。 2.查验流量监测分析系统或设备，确认具备相关监测分析能力，并确认覆盖了全部网络出口。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。

8.3.3 异常行为监测

异常行为监测评估内容见表8.3.3。

表8.3.3 异常行为监测评估内容

序号	安全要求	评估方法	结果判定
1	应建立异常行为监测指标，包括IP、账号、数据、使用场景等多个维度，对异常行为事件进行识别、发现、跟踪和监控。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅异常行为监测指标说明文档或用户异常行为监测报告，确认覆盖用户IP、账号、数据、使用场景等多个维度。 2.如采用人工监测，则查阅监测记录，确认实施了相关操作；如采用信息系统和产品实现，查阅设计文档，确认具备对异常行为事件进行识别、发现、跟踪和监控的能力。 3.查验识别、发现、跟踪和监控功能，确认相关信息系统能够检查通过从IP、账号、数据、使用场景等多个维度对异常行为事件进行识别、发现、跟踪和监控。 结果评价： 符合：满足以上第1至2项或满足第1、3项。 不符合：不满足以上第1至2项中的一项或多项或不满足1、3项中的一项或多项。
2	应采取措施监测用户数据访问行为，防止未经授权的数据传输或下载。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅设计文档，确认具备监测功能，对未授权数据传输或下载具备监测和阻断功能。 2.查验用户数据访问行为监测功能，确认防止未授权传输或下载功能正常。 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第1至2项中的一项或多项。
3	宜采取措施监测数据传输过程，并联动管理系统和安全防护设备，记录并预警数据未经授权或高风险的数据下载和传输等行为，防止数据泄露。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅设计文档，确认对未授权数据传输或下载具备监测、预警和阻断功能。（可选项） 2.查验数据传输监测功能，确认记录、预警和联动功能正常。（可选项） 3.查验用户异常行为日常监测报告、异常处置记录文档，确认能够监测及响应未经授权或高风险的数据下载和传输等行为。（可选项） 结果评价： 符合：满足以上第1至3项。 不符合：不满足以上第1至3项中的一项或多项。
4	应利用系统运行日志、上网行为、终端等安全系统日志监控资源，结合业务操作日志，对数据异常使用、用户异常行为进行分析，形成数据安全分析报告，并对异常情况及时处置。	1.人员访谈 2.文档查验	1.访谈相关人员并查阅数据安全分析报告和处置记录等文档，确认利用安全系统日志和业务操作日志，对数据异常使用和用户异常行为进行了分析和处置。 结果评价： 符合：满足以上第1项。 不符合：不满足以上第1项。

8.3.4 态势感知

态势感知能力评估内容见表8.3.4。

表8.3.4 态势感知能力评估内容

序号	安全要求	评估方法	结果判定
1	宜在内部各个关键节点，通过安全设备、探针等检测相关信息，至少包括设备指纹、上网行为日志、管理平台的审批日志、业务操作日志、数据库日志、流量日志。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅信息系统设计文档，确认覆盖了配备安全设备、探针设备的关键节点。（可选项） 2.分别登录安全设备、探针设备，并展示对设备指纹、上网行为日志、管理平台的审批日志、业务操作日志、数据库日志、流量日志的检测功能，确认有效性。（可选项） 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
2	宜对账号、IP、数据接口、数据系统、数据设备进行画像，通过算法模型检测内部潜在的账户盗用、数据滥用、数据外发、数据篡改、数据窃取、数据爬取等安全风险和威胁，并进行可视化展示各类风险和数据流动态势。	1.人员访谈 2.文档查验 3.工具测试 4.旁站验证	1.访谈相关人员并查阅信息系统设计文档，确认画像数据采集范围以及对安全风险和威胁实施了检测。（可选项） 2.查验数据画像和对账户盗用、数据滥用、数据外发、数据篡改、数据窃取、数据爬取等数据安全风险及数据流动态势的可视化界面，确认功能正常。（可选项） 3.利用工具模拟数据窃取、数据外发、数据爬取等行为，查验并确认态势感知系统算法的有效性。（可选项） 结果评价： 符合：满足以上第1至3项。 基本符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。
3	宜结合实时安全漏洞资讯、错报等信息对态势感知平台的底层规则进行及时更新。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员并查阅信息系统设计文档，确认态势感知平台覆盖了自动或手动更新底层规则的功能设计。（可选项） 2.查验态势感知平台规则更新功能，查验规则更新记录，与最新安全漏洞通报或错报进行比对，确认同步更新。（可选项） 结果评价： 符合：满足以上第1至2项。 不符合：不满足以上第 1 至 2 项中的一项或多项。

8.4 安全审计

安全审计能力评估内容见表8.4.1。

表8.4.1 安全审计能力评估内容

序号	安全要求	评估方法	结果判定
1	应制定日志数据管理与安全审计规范，明确日志的存储、分析、检查等要求。	1.文档查验	1.查阅日志数据管理与安全审计规范，确认规范内容包括对日志存储、分析、检查的具体要求。 结果评价： 符合：满足以上第 1 项。 不符合：不满足以上第 1 项。

序号	安全要求	评估方法	结果判定
2	安全审计范围应覆盖至每个有权使用数据的用户，至少包括数据库管理员、数据库用户、操作系统管理员、操作系统用户、存储介质管理员、业务管理员、业务使用者、存储介质用户等。	1.人员访谈 2.文档查验	1.访谈相关人员，确认用户名单和审计覆盖范围。 2.根据用户名单，比对审计记录，确认覆盖至每个有权使用数据的使用方（包括不限于数据库管理员、数据库用户、操作系统管理员、操作系统用户、存储介质管理员、业务管理员、业务使用者、存储介质用户等）。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
3	日志记录内容应包括时间、用户、IP 地址、操作对象、操作内容、操作行为和操作结果等相关信息。	1.配置核查	1.查验日志记录相关配置、操作，确认日志记录包括时间、用户、IP 地址、操作对象、操作内容、操作行为和操作结果等相关信息。 结果评价： 符合：满足以上第 1 项。 不符合：不满足以上第 1 项。
4	日志内容中不应出现 4 级及以上数据。	1.配置核查	1.查验数据操作行为日志记录配置情况及记录内容，确认日志中无 4 级及以上数据。 结果评价： 符合：满足以上第 1 项。 不符合：不满足以上第 1 项。
5	包括 3 级数据的日志，对其访问应进行访问控制。	1.配置核查	1.对含 3 级数据的日志，查验其采用的访问控制策略，确认访问控制策略有效。 结果评价： 符合：满足以上第 1 项。 不符合：不满足以上第 1 项。
6	宜搭建数据安全审计系统，对日志进行统一管理和处理，建立并执行审计策略，提供对审计记录进行统计、查询、分析及生成审计报表的功能，形成审计报告反馈相关部门。	1.文档查验 2.旁站验证	1.查阅信息系统设计文档并查验信息系统，确认具备日志统一管理和处理、建立并执行审计策略、提供对审计记录进行统计、查询、分析及生成审计报表的功能，确认相关功能正常。（可选项） 2.查阅数据安全审计策略文档，并调阅审计执行情况和记录，确认包括审计报表和审计报告等。（可选项） 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
7	应对日志进行备份，避免受到非预期的删除、修改或覆盖等。	1.人员访谈 2.旁站验证	1.访谈相关人员，确认日志备份的周期、策略，日志的加密方式等。 2.实地查验，确认备份介质的真实、有效。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。

序号	安全要求	评估方法	结果判定
8	应安排专人定期查看日志，对事件日志、告警事件进行分析和处置，并对发现的安全事件和可疑问题进行相应的处置和响应。	1.人员访谈 2.文档查验	1.访谈相关岗位人员，确认其履行定期查看日志、事件分析、告警处置和响应等岗位职责。 2.查阅岗位分工职责表、用户行为日志，确认专人定期实施事件分析、处置和响应工作。 3.查阅相关日志，确认安全事件和可疑问题有相应的分析、处置记录。 结果评价： 符合：满足以上第 1 至 3 项。 不符合：不满足以上第 1 至 3 中的一项或多项。
9	应对数据生命周期全过程进行日志记录并开展以数据为中心的安全审计。	1.文档查验 2.旁站验证	1.查阅并确认留存采集、传输、存储、使用、删除、销毁等阶段的数据有相应日志记录。 2.查阅审计记录，确认安全审计围绕上述生命周期的数据开展。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
10	应定期对 3 级及以上数据生命周期全过程进行内部审计。	1.文档查验 2.旁站验证	1.参考 JR/T 0197—2020 中《金融业机构典型数据定级规则参考表》查验 3 级及以上数据内容。 2.查阅内部审计记录，确认覆盖数据采集、传输、存储、使用、删除、销毁等生命周期阶段，并且覆盖 3 级及以上数据。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
11	审计记录应至少包括事件的日期和时间、事件类型、主体身份、事件内容、事件结果等。	1.旁站验证	1.查阅审计记录，确认内容包括事件的日期和时间、事件类型、主体身份、事件内容、事件结果等。 结果评价： 符合：满足以上第 1 项。 不符合：不满足以上第 1 项。
12	应对审计记录进行安全保护，防止未授权的访问和输出。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员和查阅文档，确认对审计记录采取了安全防护措施。 2.查验信息系统对审计记录的保护功能，确认能够防止未授权的访问和输出。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
13	应具备审计记录分权管理能力，可针对不同的角色和组设置审计范围，各组无法看到自己管理的审计范围以外的数据，保证审计数据的安全。	1.文档查验 2.旁站验证 3.工具测试	1.查阅文档，确认已明确角色设置与审计范围划分。 2.查验审计记录分权管理功能，使用不同角色登录尝试访问审计范围以外的数据，确认审计记录分权管理的有效性。 3.必要时使用工具筛选同一角色的数据访问记录，核验并确认角色未超范围访问数据。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第 1 至 3 项。 基本符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
14	日志和审计记录的留存时间应不少于 6 个月。	1.旁站验证	1.登录信息系统查验，确认日志和审计记录的留存时间不少于 6 个月。 结果评价： 符合：满足以上第 1 项。 不符合：不满足以上第 1 项。

8.5 安全检查

安全检查评估内容见表8.5.1。

表8.5.1 安全检查评估内容

序号	安全要求	评估方法	结果判定
1	应建立数据安全检查评估机制，定期制定数据安全检查评估计划。	1.人员访谈 2.文档查验	1.访谈相关人员，确认建立了检查评估机制，并定期制定检查评估计划。 2.查阅管理制度文档，确认包括数据安全检查评估机制具体内容。 3.查验检查评估计划，确认按既定周期制定检查评估计划。 结果评价： 符合：满足以上第 1 至 3 项。 基本符合：满足以上第 2 至 3 项。 不符合：不满足以上第 2 至 3 中的一项或多项。
2	在产品或服务发布前，或业务功能发生重大变化时，应及时做好数据安全评估。	1.文档查验	1.查阅管理制度文档，确认已明确“在发布产品或服务前”、“业务功能发生重大变化时”等关键时间点应及时开展数据安全评估的具体要求。 2.查阅数据安全评估记录、信息系统变更记录、监管报备记录等，确认关键时间点没有遗漏。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
3	在国家及行业主管部门的相关要求发生变化时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，应进行数据安全评估。	1.文档查验	1.查阅管理制度文档，确认已明确“在国家及行业主管部门的相关要求发生变化时”、“业务模式、信息系统、运行环境发生重大变更时”、“发生重大数据安全事件时”等关键时间点应开展数据安全评估的具体要求。 2.查阅数据安全评估记录、信息系统变更记录、监管报备记录、数据安全事件应急响应文档等，确认关键时间点没有遗漏。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。

序号	安全要求	评估方法	结果判定
4	应形成数据安全评估报告，并以此采取措施降低风险及可能带来的损失。	1.人员访谈 2.文档查验	1.查阅数据安全评估报告，确认与安全评估记录对应，并且包括降低风险的具体措施。 2.访谈相关人员和查阅实施记录等文档，确认安全评估报告中的降低风险措施得以实施。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
5	每年至少应开展 1 次全面的数据安全检查评估，评估方式至少包括自评估、外部第三方机构评估等。	1.人员访谈 2.文档查验	1.查阅管理制度文档，确认已明确“每年至少应开展 1 次全面的数据安全检查评估，评估方式至少包括自评估、外部第三方机构评估等”的要求。 2.访谈相关人员和查阅文档记录，确认全面的数据安全检查评估频度每年不少于 1 次，确认评估范围和评估方式。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
6	数据安全检查宜采取多种形式，如自查、内部检查和外部检查等，执行管理和技术并重的检查原则，并通过技术工具对相关管理检查内容进行验证和确认。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员和查阅文档记录，确认已开展数据安全检查，确认检查形式、内容，并采用技术工具辅助开展检查。（可选项） 2.查验相关技术工具的使用，确认具备辅助检查的相关功能。（可选项） 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
7	针对检查评估过程中发现的问题，应指定责任部门，制定适宜的整改计划，并跟踪落实。	1.人员访谈 2.文档查验	1.访谈相关人员和查阅文档记录，确认针对检查中发现的问题制定整改计划，明确责任部门，并留存整改情况记录。 结果评价： 符合：满足以上第 1 项。 不符合：不满足以上第 1 项。
8	应妥善留存有关安全评估报告，确保可供相关方查阅，并以适宜的形式对外公开。	1.人员访谈 2.文档查验	1.访谈相关人员和查阅制度文档，确认在制度文档中明确安全评估报告留存、查阅、公开等事项要求，确认制度文档中包括安全评估报告的查阅、公开的范围和审批流程。如：按照国家法律法规要求公开、履行合作协议公开、机构自身要求公开等，并执行相应的审批流程。 2.访谈相关人员和查阅文档登记簿，确认安全评估报告安全保管，查阅、公开审批流程安全有效。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。

序号	安全要求	评估方法	结果判定
9	应采取技术措施确保检查评估记录和检查报告的安全留存。（9.5-i）	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员和查阅文档，确认已采用技术措施确保检查评估记录和报告的安全留存。 2.查验所采用技术措施，确认功能正常、有效。 3.通过访谈、查阅文档等形式，查验并确认未发生检查评估记录和检查报告失泄密事件。 结果评价： 符合：满足以上第 1 至 3 项。 基本符合：满足以上第 2 至 3 项。 不符合：不满足以上第 2 至 3 中的一项或多项。

8.6 应急响应与事件处置

应急响应与事件处置评估内容见表8.6.1。

表8.6.1 应急响应与事件处置评估内容

序号	安全要求	评估方法	结果判定
1	制定应急响应与事件处置规范，建立完善的应急响应与事件处置和问责机制，做好应急预案，组织应急演练，确保在紧急情况下重要信息资源的可用性。	1.人员访谈 2.文档查验	1.访谈相关人员和查阅管理制度文档，确认已制定数据安全应急响应与事件处置规范和应急预案。 2.查阅数据安全应急响应与事件处置规范，确认包括应急响应与事件处置和问责具体内容。 3.访谈相关人员和查阅记录文档，确认定期进行应急预案的评审和更新。 4.访谈相关人员和查阅记录文档，确认定期进行应急预案的培训。 5.访谈相关人员和查阅记录文档，确认定期组织开展数据安全应急演练。 结果评价： 符合：满足以上第 1 至 5 项。 基本符合：满足以上第 1、2、5 项。 不符合：不满足以上第 1、2、5 项中的一项或多项。
2	应依据国家及行业主管部门规定、事件性质、影响范围等，对安全事件进行分级管理。	1.人员访谈 2.文档查验	1.访谈相关人员和查阅管理制度文档，确认制度文档中包括依据管理规定、事件性质、影响范围等相关内容对安全事件进行分级管理，制度文档至少包括明确的安全事件分级。 结果评价： 符合：满足以上第 1 项。 基本符合：部分满足以上第 1 项（进行了分级管理，但分级依据不完善，未按管理规定进行）。 不符合：不满足以上第 1 项。
3	应制定安全策略，对不同级别的安全事件进行相应处置，重大事件发生后应及时启动应急响应机制。	1.人员访谈 2.文档查验	1.访谈相关人员和查阅策略文档，确认策略文档中包括针对不同级别安全事件的相应处置内容，其处置内容至少包括响应流程、响应时间、人员安排、处置时间、事件分析、改进措施。 2.访谈相关人员和查阅记录文档，确认重大数据安全事件发生后，能够按照安全策略，及时响应并处置，其处置记录中至少

序号	安全要求	评估方法	结果判定
			包括定级记录、响应时间、人员安排、处置时间、事件分析、改进措施。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
4	应按照金融主管部门有关规定，向金融主管部门上报数据安全事件及其处置情况。	1.人员访谈 2.文档查验	1.访谈相关人员及查阅制度文档，确认建立了数据安全事件上报机制，其上报机制至少包括上报组织。 2.访谈相关人员和查阅记录文档，确认事件发生后，按照国家及行业的法律法规规定对事件及处置情况进行了上报。 结果评价： 符合：满足以上第 1 至 2 项。 不符合：不满足以上第 1 至 2 中的一项或多项。
5	发生金融数据泄露事件时，金融业机构应及时采取补救措施，并按照合同协议等有关约定履行客户及合作方告知义务。	1.人员访谈 2.文档查验	1.访谈相关人员，确认已建立金融数据泄露等事件的事件处理机制。 2.访谈相关人员和查阅记录文档，确认金融数据泄露事件发生时，及时采取了补救措施。 3.访谈相关人员和查阅合同文档，确认与客户及合同方的合同协议中包括了告知义务等内容。 4.访谈相关人员和查阅记录文档，确认在发生金融数据泄露事件时，按约定履行告知义务，并给出减少损失的建议。 结果评价： 符合：满足以上第 1 至 4 项。 基本符合：满足以上第 1、2、4 项，第 3 项部分满足（合同协议未规定告知义务，但实际告知）。 不符合：不满足以上第 1、2、4 中的一项或多项。
6	数据用于生产事件重现或排查等用途时，应建立相应的数据保护规则，并事前经过审批授权并采取相应的技术保护措施，降低数据泄露、丢失等安全风险。	1.人员访谈 2.文档查验 3.旁站验证	1.访谈相关人员和查阅管理制度文档，确认在文档中明确数据在用于生产事件重现或排查等用途时的保护规则、事前审批授权流程及相应技术保护措施。 2.访谈相关人员和查阅记录文档，确认事前审批流程得以落实，审批流程至少包括原因、可能的影响、使用时间。 3.查验技术保护措施，确认相关功能真实有效。 结果评价： 符合：满足以上第 1 至 3 项。 不符合：不满足以上第 1 至 3 中的一项或多项。
7	事件处置结束后，应分析和总结原因和存在的问题，形成调查记录和事件清单，调整数据安全策略，避免事件再次发生，并形成总结报告。	1.人员访谈 2.文档查验	1.访谈相关人员和查阅记录文档，确认事件处置结束后形成了事件调查记录、事件清单和总结报告。 2.访谈相关人员和查阅记录文档，确认事件调查记录和事件清单包括原因分析、问题总结等要素。 3.访谈相关人员和查阅记录文档，确认事件处置结束后，根据情况对安全策略进行了调整，制定改进措施。 结果评价：

序号	安全要求	评估方法	结果判定
			符合：满足以上第 1 至 3 项。 不符合：不满足以上第 1 至 3 中的一项或多项。

9 金融数据安全评估结果

数据安全评估结果评分由综合得分计算公式得出，参见表9.1。

表 9.1 数据安全评估结果依据

评估结论	判别依据	综合得分
优	被评估方无重大不符合项，综合评定基本符合与符合项评分，且总分 90 分以上（含 90 分）。	综合得分计算公式如下。
良	被评估方存在安全问题，但不会导致被评估方面临高等级安全风险，且总分 80 分以上（含 80 分）。	
中	被评估方存在安全问题，但不会导致被评估方面临高等级安全风险，且总分 70 分以上（含 70 分）。	
差	被评估方存在安全问题，而且会导致被评估方面临高等级安全风险，或总分低于 70 分。	

综合得分计算方法如下：

设M为被评估方的综合得分，$M = V_t \cdot \frac{t}{n} + V_m \cdot \frac{m}{n} + V_o \cdot \frac{o}{n}$

$$V_t = \sum_{k=1}^{t} x_k \cdot \frac{100}{t} \qquad V_m = \sum_{k=1}^{m} x_k \cdot \frac{100}{m} \qquad V_o = \sum_{k=1}^{o} x_k \cdot \frac{100}{o} \qquad x_k = (0, 0.5, 1)$$

其中，n为总体评估项数，x_k为单项评估得分，符合为1分，基本符合为0.5分，不符合为0分。V_t为数据安全管理评估得分，t为数据安全管理评估项数。V_m为数据安全保护评估得分，m为数据安全保护评估项数。V_o为数据安全运维评估得分，o为数据安全运维评估项数。

9.1 安全问题等级

根据严重程度，将评估过程中发现的数据安全问题等级划分为严重性问题、一般性问题和建议性问题。问题等级的划分标准如下：

a) 严重性问题：与相关法律法规、标准规范有明显冲突；存在较高数据安全风险，且可能金融消费者、金融业机构及其相关合作方等的合法权益造成严重的损害，甚至会对国家安全、社会公众权益及金融稳定等产生影响；

b) 一般性问题：未与相关法律法规、标准规范有明显冲突，但存在一般数据安全风险，且可能对金融消费者、金融业机构及其相关合作方等的合法权益造成一般或潜在的损害，但不影响国家安全、社会公众权益及金融稳定；

c) 建议性问题：未与相关法律法规、标准规范有明显冲突，具备基本安全保障能力，未对金融消费者、金融业机构及其相关合作方等的合法权益造成明显威胁或损害，且不影响国家安全、社会公众权益及金融稳定，但机构自身数据安全建设存在安全管理体系不健全、不完善、安全措施执行不到位或安全管理技术易用性差等风险。

9.2 评估判定原则

9.2.1 符合

该评估项中所有非可选项结果判定项为“符合”，则该评估项的判定结果为“符合”。

9.2.2 基本符合

该评估项中部分非可选项结果判定项为“不符合”，但所有为满足该安全要求的必要结果判定项为“符合”，则该评估项的判定结果为“基本符合”。

9.2.3 不符合

该评估项中多个非可选项结果判定项或所有为满足该安全要求的必要结果判定项为“不符合”，则该评估项的判定结果为“不符合”。

9.3 评估结果判定

9.3.1 符合

所有评估域的评估结果为“符合”，则数据安全评估结果为“符合”。其中：

a) 属于安全管理评估的结果判定项，其非可选项判定结果中“符合”率大于 50%且“不符合”率小于 15%，则判定该评估域的评估结果为“符合”；
b) 属于安全保护评估的结果判定项，其非可选项判定结果中“符合”率大于 50%且“不符合”率小于 15%，则判定该评估域的评估结果为“符合”；
c) 属于安全运维评估的结果判定项，其非可选项判定结果中“符合”率大于 50%且“不符合”率小于 15%，则判定该评估域的评估结果为“符合”。

9.3.2 基本符合

所有评估域的评估结果为“符合”或“基本符合”，则数据安全评估结果为“基本符合”。其中：

a) 属于安全管理评估的结果判定项，其非可选项判定结果中“符合”率小于或等于 50%且“不符合”率小于 15%，则判定该评估域的评估结果为“基本符合”；
b) 属于安全保护评估的结果判定项，其非可选项判定结果中“符合”率小于或等于 50%且“不符合”率小于 15%，则判定该评估域的评估结果为“基本符合”；
c) 属于安全运维评估的结果判定项，其非可选项判定结果中“符合”率小于或等于 50%且“不符合”率小于 15%，则判定该评估域的评估结果为“基本符合”。

9.3.3 不符合

存在评估域的评估结果为“不符合”，则数据安全评估结果为“不符合”。其中：

a) 属于安全管理评估的结果判定项，其非可选项判定结果中 “不符合”率大于或等于 15%，则判定该评估域的评估结果为“不符合”；
b) 属于安全保护评估的结果判定项，其非可选项判定结果中“不符合”率大于或等于 15%，则判定该评估域的评估结果为“不符合”；
c) 属于安全运维评估的结果判定项，其非可选项判定结果中“不符合”率大于或等于 15%，则判定该评估域的评估结果为“不符合”。

附 录 A
（资料性）
金融数据资产清单

本附录给出了金融数据资产清单及其主要内容要素的参考描述，供金融业机构开展自身数据资产盘点梳理和数据安全分级管理过程参考使用。

金融数据资产清单是对金融业机构自身数据资产用途、分类、分级、数据类型、分布位置、合规及安全要求等实际应用情况的综合性登记表单，且应具有唯一性、准确性及全面性。其中：

a) 唯一性：是指金融业机构应确认在其生产经营及安全管理等过程中所确定、使用及维护的金融数据资产清单在本机构范围内保持统一、同步，不应出现虚假、废旧、残缺或多张表单混用等情况。

b) 准确性：是指金融业机构应确认其确定、使用及维护的金融数据资产清单内容的准确、真实，并定期进行表单审核、按需及时进行表单内容的更新，确保其与实际生产经营及安全管理等过程中产生、存储和使用的各项数据相符。

c) 全面性：是指金融业机构应确认其确定、使用及维护的金融数据资产清单内容覆盖本机构确定范围（如机构全量数据、某业务全量等）内的全部数据资产，其生产经营及安全管理等过程中不应出现表外数据的采集和使用等数据活动。

数据资产与金融业机构所发布的产品和服务相关，数据资产清单参见表A.1，从对产品和服务的维度进行梳理，从而识别不同产品和服务中对应的数据资产以及其实际应用情况。其中，主要内容要素为：

表 A.1 数据资产清单

序号	产品和服务	功能	数据描述	主责部门	数据级别	数据承载介质	数据类型	业务合规要求	安全合规要求	数据量级

a) 产品和服务：该项金融产品和服务的具体名称、代码及版本号。

b) 功能：对产品和服务具体功能的解释说明。

c) 数据描述：描述与产品和服务相关的数据具体形态，如结构化数据，可描述如数据类别、信息系统名、数据库名、表名、字段名、字段含义、数据类型、数据格式、数据源等信息；非结构化数据，描述其格式类型、内容含义、数据来源、数据用途等内容特性。

d) 主责部门：描述该数据相关使用、管理及安全等责任的归属部门。

e) 数据级别：描述该数据的安全级别。

f) 数据承载介质：描述该数据通过何种介质存储。

g) 数据类型：描述该数据为员工数据、用户数据、业务数据等。

h) 业务合规要求：描述该数据在业务层面上受到何种法律、法规、监管要求及内部管理制度的约束。

i) 安全合规要求：描述该数据在安全层面上受到何种法律、法规、监管要求及内部管理制度的约

束。

j) 数据量级：描述数据记录条数的量级，如：十万级、百万级、千万级等（非具体数字）。

附 录 B
（资料性）
金融数据生命周期安全保护分析表

数据生命周期安全保护分析是对金融业机构当前数据保护实际情况的统计和分析。表B.1给出的数据生命周期安全保护分析表是根据数据活动设计的数据防护安全合规要求对应关系表。

表 B.1 数据生命周期安全保护分析表

数据活动	数据场景	产品和服务	系统、设备、应用、接口及工具	相关部门及责权分工	主要安全岗位及人员	主要制度依据（含内外部）	保护措施	初步评价
数据采集								
数据传输								
数据存储								
数据使用	数据访问							
	数据导出							
	数据加工							
	数据展示							
	开发测试							
	汇聚融合							
	公开披露							
	数据转让							
	委托处理							
	数据共享							
数据删除								

数据活动	数据场景	产品和服务	系统、设备、应用、接口及工具	相关部门及责权分工	主要安全岗位及人员	主要制度依据（含内外部）	保护措施	初步评价
数据销毁								

参 考 文 献

[1] GB/T 4754—2017 国民经济行业分类
[2] GB/T 5271.1—2000 信息技术 词汇 第1部分：基本术语
[3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[4] GB/T 25058—2019 信息安全技术 网络安全等级保护实施指
[5] GB/T 37092—2018 密码模块安全检测要求
[6] GB/T 37939—2019 信息安全技术 网络存储安全技术要求
[7] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[8] GM/Z 0001—2013 密码术语
[9] GM/T 0002—2012 SM4分组密码算法
[10] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范
[11] JR/T 0167—2018 云计算技术金融应用规范 安全技术要求
[12] JR/T 0068—2020 网上银行系统信息安全通用规范
[13] JR/T 0071—2020 金融行业信息系统信息安全等级保护实施指引
[14] ISO/IEC 20889:2018 Information technology-Security techniques-Privacy enhancing data de-identification terminology and classification of techniques
[15] ISO/IEC 27038:2014 Information technology-Security techniques-Specification for digital redaction
[16] Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST Special Publication 800-171, Revision 1, 2016
[17] Assessing Security Requirements for Controlled Unclassified Information, NIST Special Publication 800-171A, 2018