2024
金融机构数据安全合规建设
调查研究报告

指导单位

DCMM金融行业社区技术委员会

发起单位

双态IT论坛、翰纬科技、安全牛

编委成员

张兵
上海翰纬信息科技有限公司

王岩
保险行业专家

李欣韦
上海翰纬信息科技有限公司

王志超
北京谷安天下科技有限公司

韩佶卿
上海浦东发展银行股份有限公司

张越然
中信建投证券股份有限公司

陶蓉
保险行业专家

沈力克
中银富登村镇银行股份有限公司

许立芳
中信建投证券股份有限公司

师俊强
上海翰纬信息科技有限公司

目 录 Contents

序

随着数字化转型的加速，金融机构不仅在业务创新上迎来了前所未有的机遇，同时也面临着日益严峻的数据安全挑战。数据的安全性和合规性直接关系到金融机构的稳健运营、客户信任乃至整个金融市场的稳定。因此，金融机构的数据安全合规建设，已成为行业发展的关键议题。

本报告在 DCMM 金融行业社区技术委员会的指导下，由双态 IT 论坛、翰纬科技、安全牛联合发起，通过《2024 金融机构数据安全合规建设》问卷调查活动，深入分析了我国金融机构在数据安全管理方面的实践情况。通过对 44 家金融机构的问卷调研，我们全面评估了金融机构在数据安全组织架构、分类分级、管理、技术、个人信息保护、风险监测等多个关键领域的实践和挑战。

报告的编写过程严格遵循科学研究方法，从调研设计、数据收集与分析、专家报告编制、深度访谈与案例研究，到专家评审和报告修订，每一步都凝聚了众多专家学者和行业实践者的心血与智慧。我们希望通过这份报告，不仅为金融机构提供数据安全合规建设的参考和指导，也为监管机构、行业协会以及所有关注数据安全领域的人士提供决策支持和思路启发。

在报告的序言中，我们特别感谢所有参与调研的金融机构、贡献宝贵意见和建议的专家，以及所有支持和关注本研究的组织和个人。没有大家的共同努力和支持，这份报告的完成是不可想象的。

最后，我们期待本报告能够成为推动我国金融机构数据安全合规建设的一股力量，促进行业内的交流与合作，共同应对数据安全挑战，保障金融行业的健康稳定发展。

谨以此报告献给所有致力于数据安全合规建设的同仁们。

第一章　概述

第一节 研究背景和目的

随着数字化转型的加速，数据已成为金融机构最宝贵的资产之一。然而，数据的海量增长和广泛应用也带来了前所未有的安全挑战。金融机构掌握着海量的敏感客户数据，这些数据的安全性直接关系到客户资产的保护、个人隐私的维护以及金融机构自身的品牌和商誉。在这一背景下，数据安全问题已成为金融机构数字化发展进程中的核心关切。

网络威胁的日益复杂化要求金融机构必须采取更为严格的数据安全措施。这些措施不仅需要确保数据的完整性、保密性和可用性，而且对于维护客户信任和机构的稳健运营至关重要。面对这一挑战，金融机构的数据安全建设必须遵循严格的国家法律法规和行业标准，以确保合规性和安全性。

具体而言，金融机构需要遵循以下法律法规和行业标准：

- 《中华人民共和国网络安全法》：为网络空间的安全提供法律框架，明确了网络运营者的安全义务。
- 《中华人民共和国数据安全法》：规定了数据处理活动的基本原则和要求，强化了数据安全保护。
- 《中华人民共和国个人信息保护法》：保护个人信息权益，规范个人信息处理活动。
- 《个人金融信息保护技术规范》(JR/T 0171-2020)、《金融数据安全 数据安全分级指南》（JRT 0197-2020）和《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）：由中国人民银行发布，为金融数据的安全管理和技术保护提供了规范。
- 《证券期货业数据分类分级指引》（JR/T 0158-2018）和《证券期货业数据安全管理与保护指引》（JR/T 0250-2022）：由证监会发布，为证券期货业的数据安全管理提供了指导。
- 《银行保险机构数据安全管理办法（征求意见稿）》：由国家金融监督管理总局发布，针对银行保险机构的数据安全管理提出了具体要求。
- 《中国人民银行业务领域数据安全管理办法（征求意见稿）》：由中国人民银行研究起草，指导督促相关数据处理者依法依规开展中国人民银行业务领域数据处理活动，履行数据安全保护义务。

为了深入了解我国金融机构在数据安全管理方面的实践情况，发现其中的难点和挑战，在 DCMM 金融行业社区技术委员会指导下，双态 IT 论坛、翰纬科技、安全牛共同发起了《2024 金融机构数据安全合规建设》问卷调查活动。问卷涵盖了数据安全的组织架构、分类分级、管理、技术、个人信息保护、风险监测等多个领域，旨在全面评估金融机构的数据安全实践。

本次调研面向国内银行、保险、证券等金融机构的数据安全管理者，确保数据的准确性和代表性。根

据调查结果，我们将联合编制《2024 年度金融机构数据安全合规建设》研究报告。该报告将在 2024 年举办的第十三届双态 IT 用户大会上正式发布，旨在促进行业内的交流与合作，共同推动金融机构数据安全合规的进步。

第二节 研究方法

本研究旨在深入分析和理解金融机构在数据安全合规建设方面的现状、问题和挑战，并提出相应的改进建议。为此，我们采用了以下研究方法：

一、调研设计与问卷编制：首先，我们设计了一份包含 22 道单选题或多选题的问卷，覆盖数据安全的组织架构、分类分级、管理、技术、个人信息保护、风险监测等领域。问卷设计充分考虑了金融机构的业务特点和数据安全的实际需求。

二、数据收集：问卷通过 DCMM 金融行业社区技术委员会、双态 IT 论坛、翰纬科技、安全牛等渠道发放给国内银行、保险、证券、基金等金融机构的数据安全管理者。我们确保了调研对象的代表性和广泛性，以收集高质量的数据。

三、数据统计与分析：收集到的数据经过严格的筛选和清洗，剔除了不符合要求的受访人填报信息。然后，我们运用统计学方法对数据进行描述性分析，识别出金融机构在数据安全合规建设方面的主要特点和趋势。

四、专家分析报告编制：我们邀请了金融行业数据安全领域的专家，基于调研结果、他们对数据安全的理解以及对金融行业的深入了解，编制了分析报告。报告内容涵盖了数据安全合规监管要求、金融机构在数据安全合规建设的现状、面临的问题和挑战、改进建议等关键方面。

五、深度访谈：为了更深入地理解金融机构在数据安全合规建设中的具体做法和经验，我们还进行了一系列的深度访谈。这些访谈对象包括金融机构的数据安全负责人、技术专家和业务管理者。

六、案例研究：通过对一些金融机构的数据安全合规建设实践进行案例研究，我们能够更具体地分析和总结其成功经验和存在的不足。

七、专家评审：报告初稿完成后，我们邀请了金融行业数据安全领域的专家进行评审。评审专家从不同角度对报告的内容、结构和建议进行了严格的审核。

八、报告修订：根据专家评审的意见和建议，我们对报告进行了多轮修订和完善。这一过程确保了报告的质量和实用性。

九、最终发布：经过多轮的修订和完善，最终的研究报告将在 2024 年举办的第十三届双态 IT 用户大

会上正式发布。这不仅为金融机构提供了宝贵的参考和指导，也为行业内外的交流与合作提供了平台。

通过这一系列严谨的研究方法，我们确保了研究报告的科学性、客观性和实用性。我们相信，这份研究报告将为金融机构在数据安全合规建设方面提供有力的支持和指导。

第三节　研究过程

本研究旨在全面了解金融机构在数据安全合规建设方面的现状、挑战和改进需求。以下是详细的研究过程：

一、问卷调查发放（2024 年 7 月 1 日）：

1. DCMM 金融行业社区技术委员会、双态 IT 论坛、翰纬科技、安全牛联合发起了《金融机构数据安全合规建设用户问卷调查》。
2. 问卷通过各自官方渠道发放，旨在收集来自不同金融机构的数据安全管理者的意见和信息。

二、问卷收集与初步筛选（2024 年 7 月 12 日）：

1. 经过 2 周的问卷发放，共收集到来自银行、保险、证券、基金等金融机构的 44 份有效问卷。
2. 对收集到的问卷进行了初步筛选，确保数据的质量和代表性。

三、数据统计与分析（2024 年 7 月 15 日至 26 日）：

1. 组织专家对问卷调研结果进行了详细的统计分析。
2. 分析结果揭示了金融机构在数据安全合规建设方面的现状、存在的问题和挑战。

四、起草研究报告（2024 年 7 月 15 日至 8 月 16 日）：

1. 基于统计分析结果，专家组开始编写研究报告。
2. 报告内容包括数据安全合规监管要求、金融机构数据安全合规建设现状、面临的主要问题和挑战，以及改进建议。

五、深度访谈与案例研究（2024 年 7 月 29 日至 8 月 16 日）：

1. 组织专家对金融机构的数据安全负责人、技术专家和业务管理者进行了深度访谈。
2. 对数据安全合规建设的典型案例进行了研究，以获取更深入的见解和经验。

六、专家评审（2024 年 8 月 19 日至 8 月 30 日）：

1. 邀请了金融行业数据安全领域的专家对研究报告进行了评审。
2. 评审专家从不同角度对报告的内容、结构和建议进行了严格的审核，并提供了宝贵的反馈。

七、报告修订（2024 年 9 月 2 日至 9 月 6 日）：

1. 根据专家评审的意见和建议，对研究报告进行了修订。
2. 修订过程确保了报告的准确性、完整性和实用性。

八、报告最终定稿：

1. 经过多轮的修订和完善，研究报告最终定稿。
2. 报告将在 2024 年 10 月举办的第十三届双态 IT 用户大会上正式发布。

第四节　可能存在的不足

在编写金融机构数据安全合规建设的研究报告时，可能存在以下不足之处：

一、样本代表性：尽管我们努力收集了来自不同金融机构的问卷，但样本数量可能仍然有限，这可能影响研究结果的普遍性和代表性。

二、数据收集偏差：问卷调查可能受到受访者主观性的影响，导致数据收集存在偏差，影响分析结果的准确性。

三、深度访谈的局限性：尽管深度访谈可以提供深入见解，但受访者的选择可能具有主观性，且访谈结果可能受到受访者个人经验和观点的限制。

四、专家评审的主观性：专家评审虽然可以提供专业意见，但评审意见可能受到专家个人专业背景和观点的影响，存在一定的主观性。

五、技术发展迅速：数据安全技术和标准在不断进步，研究过程中可能未能完全涵盖最新的技术和行业动态。

六、法规更新滞后：法律法规可能在研究过程中发生变化，报告中的法规分析可能存在时效性问题。

七、报告的实用性：报告可能在某些方面过于理论化，未能充分考虑金融机构实际操作中的复杂性和可行性。

八、跨行业比较的困难：不同金融机构在规模、业务范围、技术基础等方面存在差异，进行跨行业比较可能存在困难。

九、数据安全实践的多样性：金融机构在数据安全合规建设方面的实践可能非常多样，报告可能未能涵盖所有类型的实践。

十、文化和地域差异：不同地区和文化背景下的金融机构可能有不同的数据安全合规需求和实践，报告可能未能充分考虑这些差异。

十一、资源和时间限制：研究过程中可能受到资源和时间的限制，导致某些方面的研究不够深入或全面。

为了克服这些潜在的不足，研究团队将持续关注行业动态，扩大样本量，采用多种研究方法进行交叉验证，并定期更新研究报告以反映最新的数据安全合规趋势和实践。同时，鼓励更多的金融机构参与到研究中来，以提高研究的深度和广度。

第五节　重要发现

一、分析模型

为了深入分析和理解调研结果，我们构建了一个简洁的数学模型，称为“两线三型模型”。该模型基于两条基准线和三种能力类型来评估金融机构的数据安全合规水平。具体来说：

两线：我们设定了两条基准线，即：

- **均线**（平均线）：设定在 60%，表示 60%及以上机构应具备的基本合规能力。
- **标线**（标杆线）：设定在 40%，表示少于 40%的机构所具备的卓越合规能力。 满足度介于 60%到 40%之间的能力项，我们定义为增强合规能力。

三型：根据机构具备的数据安全合规能力状况，我们将机构分为三种类型：

- **基本型**：机构满足基本合规能力。
- **增强型**：机构在满足基本合规能力的基础上，还具备增强能力。
- **卓越型**：机构不仅满足基本和增强能力，还具备卓越能力，且总体上满足数据安全合规要求。

通过应用这一“两线三型”模型，金融机构不仅可以了解整个行业在数据安全合规建设方面的现状，而且能够对照自身情况，为未来的合规建设规划提供有力的数据支持。

二、对全部金融机构分析结果如下：

数据安全合规基本能力			
编号	能力类别	能力项	比率
1	数据安全管理	制定了数据安全管理办法	95%
2	数据安全管理	制定了从生产环境提取数据的管理流程	95%
3	数据安全技术	具备日志审计技术能力	93%
4	数据安全管理	实施数据收集管理	91%
5	数据安全管理	实施数据使用管理	91%
6	数据安全技术	实施用户身份管理技术	89%
7	个人信息保护	建立了个人信息保护管理体系	89%
8	数据安全技术	实施数据脱敏技术	89%
9	数据分类分级	制定了数据分类分级保护制度	86%
10	数据安全管理	建立了企业级的数据架构	86%
11	数据安全管理	实施数据加工管理	86%
12	数据安全技术	制定用户对数据的访问策略	86%
13	数据安全技术	部署了数据防泄漏 DLP 产品	86%
14	数据安全技术	大数据平台安全采用高可用设计	84%
15	数据安全技术	实施数据备份技术	84%
16	数据安全管理	建立了专职数据服务团队	82%
17	数据安全技术	将数据纳入网络安全等级保护	82%
18	数据安全技术	敏感数据传输采用安全的传输方式	82%
19	数据分类分级	对数据进行了分类分级	80%
20	数据安全技术	实现了数据安全保护措施与信息系统的同步规划、同步建设、同步使用	80%
21	数据安全技术	敏感数据采取安全存储措施	80%
22	数据安全技术	建立了大数据服务访问授权机制	80%
23	数据安全治理	建立了数据安全责任制	75%
24	数据安全治理	建立了覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构	73%
25	数据分类分级	建立了数据分类分级规范	73%

26	数据安全管理	从生产环境提取数据明确了数据脱敏要求	73%
27	数据安全风险监测与处置	对客户有关数据安全的投诉实施监测	73%
28	数据安全风险监测与处置	对数据泄露、仿冒欺诈等负面舆情实施监测	73%
29	数据安全技术	部署了数据库审计产品	73%
30	数据安全管理	实施数据删除与销毁管理	70%
31	数据安全技术	将敏感数据纳入信息系统保护	70%
32	数据安全风险监测与处置	对内部人员异常访问、使用数据实施监测	70%
33	数据安全治理	明确了公司主要负责人为数据安全第一责任人	68%
34	数据安全管理	实施数据共享及集团内部共享管理	68%
35	数据安全技术	实施用户行为监测技术	68%
36	数据安全治理	明确了公司分管数据安全的领导为直接责任人	66%
37	数据安全风险监测与处置	对超范围授权或者使用系统特权账号实施监测	66%
38	数据安全技术	对大数据平台实施安全加固	64%
39	数据安全技术	部署了运维人员管理系统	64%
40	数据安全管理	统筹了内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动	61%
41	数据安全管理	实施外部数据采购管理	61%
42	数据安全管理	从生产环境提取数据的审批环节中包含数据所有者	61%

数据安全合规增强能力			
编号	能力类别	能力项	比率
1	数据分类分级	建立了数据目录	59%
2	数据安全管理	从生产环境提取数据的审批环节中包含数据安全岗位	59%
3	数据安全管理	从生产环境提取数据明确了数据使用或者保存期限	59%
4	数据安全技术	实施网间摆渡技术	59%
5	数据安全管理	实施数据公开管理	57%

6	数据安全技术	敏感数据达到使用或者保存期限后，采取技术措施及时删除或者销毁	57%
7	数据安全技术	与外部交互数据采用了 API 安全的技术措施	57%
8	数据安全治理	明确了党委（党组）、董（理）事会对本单位数据安全工作负主体责任	55%
9	数据安全管理	制定了数据服务规范	55%
10	数据安全管理	实施数据跨境管理	55%
11	数据安全风险监测与处置	对数据集中共享的系统或者平台的网络安全、数据安全威胁实施监测	55%
12	数据安全风险监测与处置	对外包、第三方合作中的数据处理异常或者数据泄露、丢失和篡改实施监测	55%
13	数据安全技术	实施 API 安全技术	55%
14	数据安全技术	实施文档加密技术	55%
15	数据安全管理	实施委托处理数据管理	52%
16	数据安全技术	建设了与外部交互数据的专用平台	52%
17	数据安全技术	动态监测与审计大数据访问行为	50%
18	数据安全风险监测与处置	对移动存储介质的异常使用实施监测	50%
19	数据分类分级	使用自动化分类分级工具	48%
20	数据安全管理	实施数据共同处理管理	48%
21	数据安全管理	实施数据转移管理	45%
22	数据安全管理	在处理敏感数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，事先开展了数据安全评估	43%
23	数据安全技术	建立了针对大数据、云计算、移动互联网、物联网等多元异构环境下的数据安全技术保护体系	43%
24	数据安全技术	实施数据库防火墙（网关）技术	43%
25	数据安全技术	实施用户行为分析技术	43%

数据安全合规卓越能力

编号	能力类别	能力项	比率
1	数据安全技术	实施数据匿名化技术	39%
2	数据安全技术	对人工智能模型开发应用进行统一管理	36%
3	数据安全风险监测与处置	对敏感数据在不同区域的异常流动实施监测	36%
4	数据安全技术	对模型研发过程进行主动管理，实现模型算法可验证、可审核、可追溯	34%
5	数据安全技术	实施数据分类分级自动化工具	34%
6	数据安全治理	开展数据安全认证	34%
7	数据安全技术	实施数据库加密存储技术	32%
8	数据分类分级	对全部数据进行了分类分级	30%
9	数据安全技术	模型算法投入使用时，开展数据安全审查	27%
10	数据安全管理	采用信息系统支持，实现了数据地图	25%
11	数据分类分级	自动化分类分级工具识别准确率超过 50%	23%
12	数据安全技术	建立模型算法产品外部引入的准入机制	23%
13	数据安全技术	使用人工智能技术开展业务时就数据对决策结果影响进行解释说明和信息披露	20%
14	数据安全技术	实施数据虚拟化技术	16%
15	数据安全技术	实时监测自动化处理与系统运行结果	16%
16	数据安全技术	建立人工智能应用的风险缓释措施	16%

三、对银行保险金融机构的分析结果如下：

数据安全合规基本能力			
编号	能力类别	能力项	比率
1	数据安全管理	制定了数据安全管理办法	100%
2	数据安全管理	实施数据使用管理	100%
3	数据安全管理	制定了从生产环境提取数据的管理流程	100%
4	数据分类分级	制定了数据分类分级保护制度	96%
5	数据安全管理	实施数据收集管理	96%
6	数据安全技术	实施用户身份管理技术	96%

7	数据安全管理	实施数据加工管理	92%
8	数据安全技术	敏感数据传输采用安全的传输方式	92%
9	数据安全技术	敏感数据采取安全存储措施	92%
10	数据安全技术	具备日志审计技术能力	92%
11	个人信息保护	建立了个人信息保护管理体系	92%
12	数据安全技术	部署了数据防泄漏 DLP 产品	92%
13	数据安全技术	实施数据脱敏技术	92%
14	数据安全管理	建立了企业级的数据架构	88%
15	数据安全管理	建立了专职数据服务团队	88%
16	数据安全技术	大数据平台安全采用高可用设计	88%
17	数据安全技术	实施数据备份技术	88%
18	数据安全治理	建立了数据安全责任制	84%
19	数据分类分级	对数据进行了分类分级	84%
20	数据安全管理	从生产环境提取数据明确了数据脱敏要求	84%
21	数据安全技术	将敏感数据纳入信息系统保护	84%
22	数据安全技术	制定用户对数据的访问策略	84%
23	数据安全技术	建立了大数据服务访问授权机制	84%
24	数据安全风险监测与处置	对超范围授权或者使用系统特权账号实施监测	84%
25	数据安全治理	建立了覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构	80%
26	数据安全管理	实施数据删除与销毁管理	80%
27	数据安全技术	将数据纳入网络安全等级保护	80%
28	数据安全技术	实施用户行为监测技术	80%
29	数据安全风险监测与处置	对内部人员异常访问、使用数据实施监测	80%
30	数据安全风险监测与处置	对客户有关数据安全的投诉实施监测	80%
31	数据安全治理	明确了公司主要负责人为数据安全第一责任人	76%
32	数据安全管理	实施外部数据采购管理	76%

33	数据安全管理	从生产环境提取数据明确了数据使用或者保存期限	76%
34	数据安全技术	实现了数据安全保护措施与信息系统的同步规划、同步建设、同步使用	76%
35	数据安全治理	明确了公司分管数据安全的领导为直接责任人	72%
36	数据分类分级	建立了数据分类分级规范	72%
37	数据安全管理	实施数据公开管理	72%
38	数据安全风险监测与处置	对数据泄露、仿冒欺诈等负面舆情实施监测	72%
39	数据安全技术	部署了数据库审计产品	72%
40	数据安全治理	明确了党委（党组）、董（理）事会对本单位数据安全工作负主体责任	68%
41	数据安全管理	制定了数据服务规范	68%
42	数据安全管理	实施数据共享及集团内部共享管理	68%
43	数据安全管理	从生产环境提取数据的审批环节中包含数据所有者	68%
44	数据安全技术	敏感数据达到使用或者保存期限后，采取技术措施及时删除或者销毁	68%
45	数据安全技术	对大数据平台实施安全加固	68%
46	数据安全技术	建设了与外部交互数据的专用平台	68%
47	数据安全技术	与外部交互数据采用了 API 安全的技术措施	68%
48	数据安全风险监测与处置	对数据集中共享的系统或者平台的网络安全、数据安全威胁实施监测	68%
49	数据安全风险监测与处置	对移动存储介质的异常使用实施监测	68%
50	数据安全技术	部署了运维人员管理系统	68%
51	数据分类分级	建立了数据目录	64%
52	数据安全管理	统筹了内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动	64%
53	数据安全管理	实施委托处理数据管理	64%
54	数据安全管理	实施数据转移管理	64%
55	数据安全风险监测与	对外包、第三方合作中的数据处理异常或者数据泄露、	64%

	处置	丢失和篡改实施监测	
56	数据安全技术	实施 API 安全技术	64%
57	数据安全管理	实施数据共同处理管理	60%
58	数据安全管理	实施数据跨境管理	60%
59	数据安全管理	从生产环境提取数据的审批环节中包含数据安全岗位	60%
60	数据安全技术	动态监测与审计大数据访问行为	60%
61	数据安全技术	实施文档加密技术	60%

数据安全合规增强能力			
编号	能力类别	能力项	比率
1	数据安全技术	实施用户行为分析技术	52%
2	数据安全管理	在处理敏感数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，事先开展了数据安全评估	48%
3	数据安全技术	建立了针对大数据、云计算、移动互联网、物联网等多元异构环境下的数据安全技术保护体系	48%
4	数据安全技术	实施数据匿名化技术	48%
5	数据安全技术	对人工智能模型开发应用进行统一管理	48%
6	数据安全风险监测与处置	对敏感数据在不同区域的异常流动实施监测	48%
7	数据安全治理	开展数据安全认证	48%
8	数据分类分级	使用自动化分类分级工具	44%
9	数据安全技术	实施数据库防火墙（网关）技术	44%
10	数据安全技术	实施数据库加密存储技术	44%
11	数据安全技术	对模型研发过程进行主动管理，实现模型算法可验证、可审核、可追溯	40%
12	数据安全技术	实施网间摆渡技术	40%

数据安全合规卓越能力			
编号	能力类别	能力项	比率

1	数据安全技术	模型算法投入使用时，开展数据安全审查	36%
2	数据安全技术	建立模型算法产品外部引入的准入机制	32%
3	数据安全技术	实施数据分类分级自动化工具	32%
4	数据分类分级	对全部数据进行了分类分级	28%
5	数据安全技术	使用人工智能技术开展业务时就数据对决策结果影响进行解释说明和信息披露	28%
6	数据安全技术	实时监测自动化处理与系统运行结果	28%
7	数据分类分级	自动化分类分级工具识别准确率超过 50%	24%
8	数据安全管理	采用信息系统支持，实现了数据地图	24%
9	数据安全技术	实施数据虚拟化技术	24%
10	数据安全技术	建立人工智能应用的风险缓释措施	24%

四、对证券基金金融机构的分析结果如下：

数据安全合规基本能力			
编号	能力类别	能力项	比率
1	数据安全技术	具备日志审计技术能力	95%
2	数据安全管理	制定了数据安全管理办法	89%
3	数据安全管理	制定了从生产环境提取数据的管理流程	89%
4	数据安全技术	制定用户对数据的访问策略	89%
5	数据安全管理	建立了企业级的数据架构	84%
6	数据安全管理	实施数据收集管理	84%
7	数据安全技术	实现了数据安全保护措施与信息系统的同步规划、同步建设、同步使用	84%
8	数据安全技术	将数据纳入网络安全等级保护	84%
9	个人信息保护	建立了个人信息保护管理体系	84%
10	数据安全技术	实施数据脱敏技术	84%
11	数据安全技术	实施网间摆渡技术	84%
12	数据安全管理	实施数据加工管理	79%
13	数据安全管理	实施数据使用管理	79%
14	数据安全技术	实施用户身份管理技术	79%

15	数据安全技术	大数据平台安全采用高可用设计	79%
16	数据安全技术	实施数据备份技术	79%
17	数据安全技术	部署了数据防泄漏 DLP 产品	79%
18	数据分类分级	制定了数据分类分级保护制度	74%
19	数据分类分级	建立了数据分类分级规范	74%
20	数据分类分级	对数据进行了分类分级	74%
21	数据安全管理	建立了专职数据服务团队	74%
22	数据安全技术	建立了大数据服务访问授权机制	74%
23	数据安全风险监测与处置	对数据泄露、仿冒欺诈等负面舆情实施监测	74%
24	数据安全技术	部署了数据库审计产品	74%
25	数据安全管理	实施数据共享及集团内部共享管理	68%
26	数据安全技术	敏感数据传输采用安全的传输方式	68%
27	数据安全治理	建立了覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构	63%
28	数据安全治理	建立了数据安全责任制	63%
29	数据安全技术	敏感数据采取安全存储措施	63%
30	数据安全风险监测与处置	对客户有关数据安全的投诉实施监测	63%

数据安全合规增强能力			
编号	能力类别	能力项	比率
1	数据安全治理	明确了公司主要负责人为数据安全第一责任人	58%
2	数据安全治理	明确了公司分管数据安全的领导为直接责任人	58%
3	数据安全管理	统筹了内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动	58%
4	数据安全管理	实施数据删除与销毁管理	58%
5	数据安全管理	从生产环境提取数据的审批环节中包含数据安全岗位	58%
6	数据安全管理	从生产环境提取数据明确了数据脱敏要求	58%
7	数据安全技术	对大数据平台实施安全加固	58%

8	数据安全风险监测与处置	对内部人员异常访问、使用数据实施监测	58%
9	数据安全技术	部署了运维人员管理系统	58%
10	数据分类分级	建立了数据目录	53%
11	数据分类分级	使用自动化分类分级工具	53%
12	数据安全管理	从生产环境提取数据的审批环节中包含数据所有者	53%
13	数据安全技术	将敏感数据纳入信息系统保护	53%
14	数据安全技术	实施用户行为监测技术	53%
15	数据安全管理	实施数据跨境管理	47%
16	数据安全技术	实施文档加密技术	47%
17	数据安全管理	实施外部数据采购管理	42%
18	数据安全技术	敏感数据达到使用或者保存期限后，采取技术措施及时删除或者销毁	42%
19	数据安全技术	与外部交互数据采用了 API 安全的技术措施	42%
20	数据安全风险监测与处置	对超范围授权或者使用系统特权账号实施监测	42%
21	数据安全风险监测与处置	对外包、第三方合作中的数据处理异常或者数据泄露、丢失和篡改实施监测	42%
22	数据安全技术	实施数据库防火墙（网关）技术	42%
23	数据安全技术	实施 API 安全技术	42%

数据安全合规卓越能力			
编号	能力类别	能力项	比率
1	数据安全治理	明确了党委（党组）、董（理）事会对本单位数据安全工作负主体责任	37%
2	数据安全管理	在处理敏感数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，事先开展了数据安全评估	37%
3	数据安全管理	制定了数据服务规范	37%
4	数据安全管理	实施委托处理数据管理	37%

5	数据安全管理	实施数据公开管理	37%
6	数据安全管理	从生产环境提取数据明确了数据使用或者保存期限	37%
7	数据安全技术	建立了针对大数据、云计算、移动互联网、物联网等多元异构环境下的数据安全技术保护体系	37%
8	数据安全技术	动态监测与审计大数据访问行为	37%
9	数据安全风险监测与处置	对数据集中共享的系统或者平台的网络安全、数据安全威胁实施监测	37%
10	数据安全技术	实施数据分类分级自动化工具	37%
11	数据分类分级	对全部数据进行了分类分级	32%
12	数据安全管理	实施数据共同处理管理	32%
13	数据安全技术	建设了与外部交互数据的专用平台	32%
14	数据安全技术	实施用户行为分析技术	32%
15	数据安全管理	采用信息系统支持，实现了数据地图	26%
16	数据安全技术	实施数据匿名化技术	26%
17	数据安全技术	对模型研发过程进行主动管理，实现模型算法可验证、可审核、可追溯	26%
18	数据安全风险监测与处置	对移动存储介质的异常使用实施监测	26%
19	数据分类分级	自动化分类分级工具识别准确率超过 50%	21%
20	数据安全管理	实施数据转移管理	21%
21	数据安全技术	对人工智能模型开发应用进行统一管理	21%
22	数据安全风险监测与处置	对敏感数据在不同区域的异常流动实施监测	21%
23	数据安全技术	模型算法投入使用时，开展数据安全审查	16%
24	数据安全技术	实施数据库加密存储技术	16%
25	数据安全治理	开展数据安全认证	16%
26	数据安全技术	建立模型算法产品外部引入的准入机制	11%
27	数据安全技术	使用人工智能技术开展业务时就数据对决策结果影响进行解释说明和信息披露	11%
28	数据安全技术	实施数据虚拟化技术	5%

29	数据安全技术	建立人工智能应用的风险缓释措施	5%
30	数据安全技术	实时监测自动化处理与系统运行结果	0%

第六节　金融机构数据安全合规建设的态势

一、组织架构和责任制方面进展明显

- 超过 70%的机构已经构建了包含董（理）事会、高层管理、数据安全统筹及技术保护等部门的全面数据安全管理架构。
- 这些机构确立了数据安全责任制，指定了公司主要负责人担任数据安全的第一责任人，并明确了分管数据安全领导的直接责任。
- 52%的机构进一步明确了党委（党组）和董（理）事会在本单位数据安全工作中承担主体责任。

为持续提升数据安全管理效能，金融机构应采取以下措施：

- 加强治理结构的参与度：确保治理层对数据安全议题的持续关注和积极介入。
- 细化各级责任：明确不同层级和部门在数据安全管理中的具体职责和任务。
- 持续执行与优化：对数据安全措施进行定期审查，确保其有效性，并根据技术发展和业务需求进行适时调整。

二、制度建设成效显著

金融机构通过一系列制度建设，确保了数据安全合规的顶层设计的有效性，显著提升了数据安全管理的整体水平：

- 全面的数据安全管理办法：96%的机构已经制定了全面的数据安全管理办法，为数据安全管理提供了明确的指导和规范。
- 精细化的数据分类分级制度：81%的机构不仅制定了数据分类分级保护制度，还建立了相应的数据分类分级规范，这有助于对不同级别的数据实施差异化的安全措施。
- 严格的数据提取管理流程：96%的机构制定了从生产环境提取数据的严格管理流程，确保了数据在提取过程中的安全性。
- 全流程的安全管理：90%的机构对数据收集、加工、使用等关键环节进行了全面的安全管理，实现了数据生命周期的安全管理覆盖。

这些制度的建立和执行，不仅提高了金融机构对数据安全的控制能力，也加强了对数据安全风险的预防和应对。随着数据安全环境的不断变化，金融机构应持续审视和更新这些制度，确保其始终符合最新的安全要求和业务需求，以实现数据安全合规的持续优化和提升。

三、个人信息保护体系日趋完善

随着《个人信息保护法》的颁布和金融行业对个人金融信息保护的强化监管，金融机构在构建个人信息保护体系方面取得了积极进展，93%的机构建立了个人信息保护管理体系。这一体系的完善体现在以下几个方面：

- 法规遵循：金融机构严格遵守《个人信息保护法》《个人金融信息保护技术规范》等相关法律法规和行业标准，确保个人信息保护措施与国家和监管要求保持一致。
- 体系完善：通过建立和完善个人信息保护管理体系，金融机构确立了一套系统的保护机制，涵盖了个人信息的收集、存储、使用、共享和销毁等各个环节。
- 有效执行：金融机构不仅在制度上进行了建设，更在实际操作中有效执行了这些保护措施，确保了个人信息的安全。
- 风险控制：随着个人信息保护体系的完善，金融机构在风险控制方面的能力得到了显著提升，有效预防和减少了个人信息泄露的风险。
- 客户信任：完善的个人信息保护体系增强了客户对金融机构的信任，让客户更加放心地分享个人信息，从而促进了业务的健康发展。
- 持续改进：金融机构持续关注个人信息保护的最新动态和最佳实践，不断优化和升级保护体系，以应对不断变化的安全挑战。
- 技术应用：采用先进的技术手段，如数据加密、访问控制和数据脱敏等，进一步加强了个人信息的安全性。
- 员工培训：通过定期对员工进行个人信息保护的培训，提高了员工的安全意识和操作规范性，确保了保护措施的有效执行。

金融机构在个人信息保护方面的进步不仅提升了自身的合规性，也为保护客户隐私权益和促进金融行业的健康发展做出了重要贡献。

四、数据分类分级设计优良，执行欠佳

尽管金融机构在数据分类分级体系的框架建设上取得了积极进展，但实际落地实施的效果尚需进一步提高。具体来看：

- 制度和规范的建立：81%的机构已经制定了数据分类分级保护制度，并建立了相应的规范，这为

数据的安全管理提供了基础性的指导。

- 分类分级的广泛开展：92%的机构已经开展了数据分类分级工作，显示出金融机构对于数据安全管理的高度重视。
- 数据目录的建立：67%的机构建立了数据目录，这有助于更系统地管理和检索数据资源。
- 全面性有待加强：然而，只有 41%的机构对全部数据进行了分类分级，表明在数据全面性管理上还有较大的提升空间。
- 自动化工具的应用：41%的机构已经开始使用自动化分类分级工具，这有助于提高分类分级工作的效率和准确性，但普及率仍有提升空间。

为了进一步提升数据分类分级体系的实施效果，金融机构可采取以下措施：

- 加强全面性管理：确保所有数据，特别是个人金融信息，都纳入分类分级管理的范畴。
- 提升自动化水平：扩大自动化分类分级工具的应用范围，减少人为错误，提高管理效率。
- 持续优化制度：根据业务发展和技术进步，不断优化数据分类分级的制度和规范。
- 强化员工培训：提高员工对数据分类分级重要性的认识，加强相关技能的培训。
- 定期审查和评估：定期对数据分类分级的实施效果进行审查和评估，及时发现并解决存在的问题。

五、数据安全技术防护基础坚实，但新领域技术防护不足

金融机构在数据安全技术防护的基础层面做得较为扎实，但在应对新兴技术领域的挑战时，仍需加强技术防护措施，以确保数据安全防护的全面性和适应性。

- 同步规划与建设：80%的金融机构实现了数据安全保护措施与信息系统的同步规划、同步建设和同步使用，确保了基础防护的一致性和全面性。
- 网络安全等级保护：82%的机构将数据纳入网络安全等级保护，提升了数据的安全性。
- 数据防泄漏与脱敏：86%的机构部署了数据防泄漏技术工具，89%的机构实施了数据脱敏，增强了数据在传输和处理过程中的保护。
- 多元异构环境的挑战：仅有 43%的机构建立了针对大数据、云计算、移动互联网、物联网等多元异构环境下的数据安全技术保护体系，显示出在这些新兴技术领域的防护措施尚不充分。
- 敏感数据保护：70%的机构将敏感级及以上数据纳入信息系统保护，但仍有提升空间。
- 身份管理和日志审计：89%的机构实施了用户身份管理，93%的机构实施了日志审计，这些措施有助于监控和追踪数据访问和使用情况。
- 大数据平台的高可用性：84%的机构实施了大数据平台的高可用设计，确保了数据处理的稳定性和可靠性。

- 人工智能模型管理：36%的机构对人工智能模型开发应用进行统一管理，但仅 23%的机构建立了模型算法产品外部引入的准入机制，15%的机构实时监测自动化处理与系统运行结果，这表明在人工智能领域的数据安全管理还有较大的提升空间。

六、数据安全风险监测基础具备，体系化待完善

金融机构已经建立了数据安全风险监测的基础，通过日志审计、数据防泄漏、数据库审计等自动化手段，结合手工记录等人工方法，实施日常的风险监测操作。这些措施构成了数据安全风险管理的一道防线，为日常运营提供了必要的保障。

然而，作为风险管理的第二道防线，现有的监测体系尚有显著的提升空间。金融机构需进一步强化风险监测体系，实现对数据安全风险的更全面、更系统的管理。

为实现这一目标，金融机构应采取以下措施：

- 全面风险管理：将数据安全风险纳入整体风险管理体系，确保风险管理的一致性和协调性。
- 三道防线理念：采用三道防线的风险管理架构，明确各防线的职责和工作重点。
- 风险识别与评估：加强对数据安全风险的识别和评估，及时发现潜在的风险点。
- 风险处置：制定有效的风险处置策略和措施，对识别的风险进行及时、有效的应对。
- 技术与流程优化：利用先进技术优化监测流程，提高风险监测的自动化和智能化水平。
- 人员培训与文化建设：加强员工的数据安全意识培训，营造全员参与的风险管理文化。

第七节　金融机构在数据安全合规建设方面面临的挑战

金融机构的数据安全合规建设面临一些具体的挑战，主要有：

一、数据分类分级落地效果欠佳。

数据分类分级工作面临诸多挑战，如周期漫长和成本高昂，这些因素共同作用导致其在实际应用中的落地效果不尽如人意。

- 周期长：数据分类分级需要细致的分析和评估，这一过程往往耗时较长，影响了快速响应和实施的能力。
- 投资大：实施数据分类分级所需的资源投入较大，包括人力、技术和财务资源，这可能导致一些机构在推进过程中犹豫不决。

二、数据地图的线上化率较低。

作为理解和管理数据的关键工具，数据地图能够帮助机构可视化数据流、数据存储位置和数据关系。然而，目前仅有 25%的机构实现了数据地图，这反映出金融机构在数据可视化和理解方面存在显著的提升空间。

三、数据安全评估的普及程度有待提高。

当前，仅 43%的金融机构开展了数据安全评估，这一比例远低于理想状态。可能的原因包括管理层面的疏漏、人员专业能力的不足以及实践经验的缺乏等。

四、需要提升数据安全管理的全面性。

在对金融机构进行的全面调研中，我们审视了数据收集等 11 个关键领域。结果显示，其中 7 个领域的数据安全管理措施的实施率均低于 70%，这一发现揭示了金融机构在构建全面的数据安全防护网方面存在显著的缺口。

五、数据安全技术防护亟需体系化升级。

目前，多数机构在数据安全技术防护方面，往往侧重于单一的防护手段，如数据防泄漏、数据库审计等，而缺乏宏观的、整体的体系化设计。这种局部的、零散的防护措施难以应对日益复杂的数据安全挑战。

在当前大数据、云计算、移动互联网、物联网等多元异构的技术环境下，仅有 43%的机构建立了相应的数据安全技术保护体系。这一比例明显偏低，表明金融机构在构建全面的技术防护体系方面还有很大的提升空间。

六、人工智能技术的安全管理缺口较大。

作为引领未来的新兴技术，人工智能正迅速渗透到各个行业和领域，包括金融行业。然而，目前业界对于人工智能的安全防护方法仍在研究和探索之中，整体上还处于发展不成熟的阶段。这一现状为金融机构在人工智能领域的安全防护工作带来了不小的挑战。

尽管数据安全合规的基本要求已经明确，但金融机构在满足这些要求方面的比率仍然较低。这种安全管理的缺失不仅增加了人工智能应用过程中的安全风险，也可能导致合规性问题。

七、与外部交互数据的安全技术防护亟需加强。

在数据安全领域，与外部系统和实体的数据交互构成了一个显著的风险点。金融机构必须采取更为严格的安全措施，以确保数据在交互过程中的安全性和完整性。建设与外部交互数据的专用平台和采用 API

安全的技术措施可以说是标准配置。目前，许多机构在这方面的技术和策略尚显不足。

八、数据安全风险监测存在明显漏洞。

在数据安全管理的基本面，如超范围授权、系统特权账号使用、内部人员异常访问行为、数据使用监控以及移动存储介质的规范操作等方面，许多机构的管理措施仍显不足，这些疏漏显著增加了数据安全的风险。

九、数据安全防护技术工具的应用程度不足。

在数据安全管理的多个关键环节，如敏感数据的识别、防护、监测和恢复等方面，技术工具的支撑至关重要。然而，目前许多机构在这方面的应用仍然不足，这严重影响了数据安全管理的效率和效果。

没有有效的技术工具，机构将难以实现对敏感数据的全面识别和精确防护，难以及时发现和响应安全威胁，也难以在数据安全事件发生后迅速进行数据恢复。这些问题的存在，不仅增加了数据泄露和滥用的风险，也可能导致机构在面对数据安全事件时反应迟缓，损失严重。

第八节　对金融机构数据安全合规建设的建议

金融机构的数据安全合规建设是一项全面而多维的任务，需特别关注战略规划、治理机制、人力资源投入、资金配置以及体系建设等方面。

一、战略规划：

- 长期视角：确立以未来为导向的战略规划，预见技术发展和法规变化，提前做好准备。
- 业务对齐：确保数据安全战略与业务目标和公司愿景相符，支持业务增长和创新。
- 风险管理：将风险管理作为核心组成部分，定期评估潜在威胁并制定应对策略。

二、治理机制：

- 组织架构：建立清晰的数据安全治理架构，明确各层级职责和决策流程。
- 政策与程序：制定全面的数据安全政策和操作程序，确保一致性和合规性。
- 监督与评估：实施有效的监督机制，定期评估治理结构的效能并进行必要的调整。

三、人力资源投入：

- 专业团队建设：组建由数据安全专家组成的专业团队，负责日常管理和战略实施。
- 全员培训：实施全员数据安全培训计划，提升机构整体的安全意识和能力。
- 职业发展：为数据安全团队提供职业发展路径，吸引和保留关键人才。

四、资金配置：

- 预算规划：在年度预算中明确数据安全投入，确保有足够的资源支持战略实施。
- 投资优先级：基于风险评估确定投资优先级，合理分配资金以最大化安全效益。
- 成本效益分析：定期进行成本效益分析，评估安全投资的回报，优化资源分配。

五、体系建设：

- 技术基础设施：构建强大的技术基础设施。
- 流程标准化：制定标准化的数据安全流程，确保各项操作的一致性和可追溯性。
- 合规性保障：确保体系建设满足所有相关法律法规要求，及时响应合规性变化。

第二章　数据安全治理的组织架构

第九节　数据安全治理的组织架构和责任制

第 4 题　　贵公司是否建立了清晰的数据安全治理组织架构？ [多选题]

选项	小计	比例
建立了覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构	32	72.73%
建立了数据安全责任制	33	75%
明确了党委（党组）、董（理）事会对本单位数据安全工作负主体责任	24	54.55%
明确了公司主要负责人为数据安全第一责任人	30	68.18%

明确了公司分管数据安全的领导为直接责任人	29	65.91%
以上都没有	3	6.82%
本题有效填写人次	44	

监管部门对金融机构的数据安全治理提出了明确要求，主要包括：

- 建立覆盖全机构的数据安全管理组织架构。
- 明确各级管理层的数据安全责任，包括党委（党组）、董（理）事会的主体责任，以及主要负责人的第一责任人角色。

这些要求旨在确保金融机构从组织架构到责任落实，构建起坚实的数据安全防线。

调研结果显示，在 44 家参与调研的金融机构中，数据安全组织架构和责任制的建设情况如下：

- 大约 73%的机构建立了覆盖关键管理层的数据安全管理组织架构。
- 75%的机构建立了数据安全责任制度。
- 接近 55%的机构明确了党委（党组）、董事会或监事会对数据安全工作的主体责任。
- 超过 68%的机构指定公司主要负责人为数据安全的第一责任人。
- 约 66%的机构明确了分管数据安全的领导为数据安全的直接责任人。
- 然而，仍有近 7%的机构在数据安全治理的组织建设方面尚未采取任何措施。

尽管多数金融机构已在数据安全组织架构建设方面取得进展，但与监管要求相比，仍存在差距：

- 组织架构的覆盖度：部分机构尚未完全覆盖所有关键部门，特别是在技术保护方面。
- 责任落实的明确性：一些机构在明确各级责任人方面仍有欠缺，特别是对于党委（党组）、董（理）事会的主体责任。
- 制度执行的严格性：即使建立了相关制度，但在执行过程中的严格性和有效性仍需加强。
- 全员参与度：数据安全不仅是管理层的责任，更需要全员的参与和意识。

金融机构在数据安全治理方面面临的挑战包括：

- 技术发展迅速：新技术的不断涌现要求金融机构不断更新数据安全策略和技术手段。
- 人才短缺：数据安全领域专业人才的缺乏限制了治理能力的提升。
- 监管适应性：监管要求的更新速度可能跟不上技术发展的步伐，导致金融机构在合规性方面面临压力。

- 文化建设：在机构内部建立数据安全文化，增强员工的安全意识和参与度。

为缩小监管要求与实践的差距，提出以下建议：

- 加强顶层设计：确保数据安全治理与整体业务战略紧密结合，从顶层推动治理架构和责任制度的建立与执行。
- 完善组织架构：对现有组织架构进行审查，确保所有关键部门和层级都被纳入数据安全治理体系。
- 明确责任分配：进一步明确各级管理层的责任，特别是党委（党组）、董（理）事会的主体责任，以及主要负责人和分管领导的具体职责。
- 强化制度执行：建立监督和问责机制，确保数据安全制度得到严格执行。
- 培养专业人才：加强数据安全领域的人才培养和引进，提高治理团队的专业能力。
- 建立数据安全文化：通过培训和宣传活动，增强全体员工的数据安全意识，形成人人参与的良好氛围。
- 技术投入与更新：持续投资于数据安全技术，及时更新安全策略，以应对新兴的安全威胁。
- 监管沟通与合作：与监管部门保持密切沟通，及时了解和适应监管要求的变化。

金融机构的数据安全治理是确保数据资产安全、维护客户信任和满足监管要求的关键。虽然调研结果显示多数机构已在数据安全治理方面取得一定进展，但与监管要求相比仍有提升空间。通过加强顶层设计、完善组织架构、明确责任分配、强化制度执行、培养专业人才、建立数据安全文化、加大技术投入和更新，以及加强监管沟通与合作，金融机构可以进一步提高数据安全治理水平，构建更加安全、可靠和合规的数据环境。

第三章　数据的分类分级

第十节　数据分类分级的管理机制

第 5 题　　贵公司是否建立了完善的数据分类分级管理机制？ [多选题]

选项	小计	比例
已制定数据分类分级保护制度	38	86.36%

建立了数据目录	26	59.09%
建立了数据分类分级规范	32	72.73%
以上都没有	1	2.27%
本题有效填写人次	44	

国家法律和金融行业监管部门对数据分类分级有明确的要求。

《中华人民共和国数据安全法》第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）第三条探索数据产权结构性分置制度。建立公共数据、企业数据、个人数据的分类分级确权授权制度。

国家金融监督管理总局发布的《银行保险机构数据安全管理办法（征求意见稿）》第十六条（总体要求）银行保险机构应当制定数据分类分级保护制度，建立数据目录和分类分级规范，动态管理和维护数据目录，采取差异化安全保护措施。

证监会发布的《证券期货业数据安全管理与保护指引》（JR/T 0250-2022）明确了“数据安全管理部门牵头负责数据安全管理工作，主要职责包括：组织制定数据管理制度，根据数据分类分级原则明确各类数据的分类分级，对数据进行分类分级管理，规范不同分类分级数据的处理方式和处理人员。”

中国证券业协会发布的《证券公司网络和信息安全三年提升计划（2023-2025）》，明确了“加强数据安全管理体系建设。贯彻落实国家法律法规和行业监管要求，加强数据安全管理体系建设，在明确数据权责的基础上，对数据进行分类分级，并以数据全生命周期安全防护要求为重点，构建目标明确、职责清晰、层次分明、落地性强的制度规范。”

数据分类与分级是确保数据安全治理有效性的关键步骤，其核心目标在于识别并保护那些敏感且价值高的数据资产。为了实现这一目标，必须建立一套周密的机制来确保数据分类分级的实施既系统又高效。

现状：

最新调查数据显示，金融机构已经充分意识到建立一套完善的数据分类分级管理机制的重要性，并在制度和操作流程上进行了明确规定。具体来说，超过 86%的金融机构已经制定了相应的数据保护政策和分类分级标准，从而在制度层面满足了合规性要求。然而，仅有不到 60%的机构构建了数据目录，而数据目录是数据分类与分级工作的具体成果。约有 27%的机构在数据分类与分级的实际执行上存在不足，需要进一步深化这项工作，并确保在制度规范的框架下，将数据分类分级真正落到实处。

在数据安全合规建设方面，约有 14%的机构在数据分类分级管理机制的建设上明显滞后于行业平均水平，这一现象迫切需要引起管理层的高度重视。为了迅速缩小与行业领先水平的差距，管理层应当采取积极措施，包括但不限于调配必要的资源、学习行业内领先机构的最佳实践，并在此基础上，从体系化建设的角度出发，加速推动机构达到数据安全合规的要求。

具体而言，管理层需要：

- 明确数据分类分级的重要性，并将其作为数据安全管理的核心内容。
- 分析当前数据分类分级管理机制的不足之处，识别改进的关键点。
- 制定详细的改进计划，包括时间表、责任分配和预期成果。
- 加强员工培训，提升员工对数据分类分级重要性的认识和实际操作能力。
- 形成机构级别的数据目录，易于员工查找数据分类分级结果。
- 试点数据分类分级的应用场景，将数据分类分级成果融入金融机构日常数据安全管理工作中。
- 建立持续的监控和评估机制，确保数据分类分级管理机制的有效执行和持续优化。

第十一节　数据分类分级的开展

第 6 题　　贵公司是否开展了数据分类分级工作？ [多选题]

选项	小计	比例
依据人行的《金融数据 数据安全分级指南》对数据进行了分类分级	23	52.27%
依据证监会的《证券期货业数据分类分级指引》对数据进行了分类分级	17	38.64%
依据金融监督管理总局的《银行保险机构数据安全	14	31.82%

管理办法》（征求意见稿）对数据进行了分类分级		
对全部数据进行了分类分级	13	29.55%
对个人金融信息进行了分类分级	17	38.64%
以上都没有	4	9.09%
本题有效填写人次	44	

金融机构在进行数据分类分级时，主要参照中国证券监督管理委员会、中国人民银行、国家金融监督管理总局、国家市场监督管理总局、国家标准化管理委员会发布的金融行业标准和管理办法，参见下表。

编号	参照标准名称	标准号	发布单位	发布时间	实施时间	适用范围
1	《证券期货业数据分类分级指引》	JR/T 0158-2018	中国证券监督管理委员会	2018-9-27	2018-9-27	证券期货行业机构
2	《证券期货业数据安全风险防控 数据分类分级指引》	GB/T 42775-2023	国家市场监督管理总局、国家标准化管理委员会	2023-8-6	2023-8-6	证券期货行业机构
3	《个人金融信息保护技术规范》	JR/T 0171-2020	中国人民银行	2020-2-13	2020-2-13	金融业机构
4	《金融数据 数据安全分级指南》	JR/T 0197-2020	中国人民银行	2020-9-23	2020-9-23	金融业机构
5	《银行保险机构数据安全管理办法（征求意见稿）》		国家金融监督管理总局	2024-3		在中华人民共和国境内设立的开发性金融机构、政策性银行、商业银行、农村合作银行、农村信用社，保险集团（控股）公司、保险公司、保险资产管理公司、金融

						资产管理公司、信托公司、财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、理财公司

《证券期货业数据分类分级指引》（JR/T 0158-2018）是由中国证券监督管理委员会发布的金融行业推荐性标准，旨在规范证券期货行业的数据分类和分级工作。该标准详细描述了数据分类分级的方法，并就关键问题处理提供了建议。

该标准的适用范围包括证券期货行业机构、相关专项业务服务机构以及相关信息技术服务机构。通过采用规范的数据分类和分级方法，有助于行业机构厘清数据资产、确定数据的重要性和敏感度，从而有效甄别合理化的数据使用需求、识别数据风险隐患、加强数据安全管理、建立健全数据管理制度，并采取必要的数据安全防护措施。

《证券期货业数据分类分级指引》通过确立从业务到数据的分析框架，加强了数据分类与业务流程之间的紧密联系。该指引旨在引导金融机构实现数据分类分级的实际操作，针对会管单位、行业协会、证券公司、期货公司和基金管理公司等不同业务特点，分别设计了定制化的数据分类分级模板。

表 A.4 证券公司典型数据分类分级模板（续）

业务细分		数据归类和细分				最低参考数据级别	备注
业务条线一级子类	业务条线二级子类	数据一级子类	数据类型说明	数据二级子类	数据类型说明		
交易	交易管理	交易日志信息	一般指投资者行为相关信息，可分为注册登录日志、信息变更日志等多类，包含营业部编码、账户编码、发生日期、发生时间、来源等信息。	注册登录日志	一般指投资者设备注册、登录等，包含营业部编码、账户编码、设备类型、手机号、发生日期、发生时间、来源等信息。	3	
				信息变更	一般指投资者信息变更，如开通权限、修改密码等，包含营业部编码、账户编码、变更内容、发生日期、发生时间、来源等信息。	3	
	结算管理	持仓信息	一般指投资者持有某一证券、期货、基金等品种的信息，包含营业部编码、账户编码、证券账户编码、市场代码、证券代码、持仓数量、持仓日期、市值等。			3	
		资金划转信息	一般指证券期货行业证券产品交易、结算相关的资金划转信息，包含营业部编码、账户编码、银行账户编码、发生日期、发生时间、币种代码、资金划转方向代码、出入金额等。			2	
		银行账务信息	一般指投资者开立的用于交易、结算业务的账户信息，包含营业部编码、账户编码、开户网点信息、银行账户、币种代码等。			3	

作为证券期货业金融机构进行数据分类分级的核心参考，该指引对提升行业数据安全治理水平具有显著影响，确保了数据管理的规范性和有效性。

《证券期货业数据安全风险防控 数据分类分级指引》（GB/T 42775-2023）是由国家市场监督管理总局、国家标准化管理委员会发布的面向证券期货行业的国家标准，旨在进一步规范证券期货行业的数据分类和分级工作。该标准以《证券期货行业数据模型 第 1 部分：抽象模型设计方法》（JR/T0176.1-2019）的业务线条划分为基础，提出从业务到数据逐级划分的数据分类分级方法，并调整了原《证券期货业数据分类分级指引》的分类分级建议，增加了投资者 4 级数据的建议，适用于证券期货行业防控数据安全风险、开展数据分类分级使用。

《个人金融信息保护技术规范》（JR/T 0171-2020）是由中国人民银行发布的一项金融行业标准，旨在规范金融业机构在收集、传输、存储、使用、删除和销毁等生命周期各环节对个人金融信息的安全防护要求。

《个人金融信息保护技术规范》从安全技术和安全管理两个方面提出了具体的规范性要求。具体来说，它将个人金融信息按敏感程度分为 C3、C2、C1 三个类别，并针对每个类别的信息在不同环节的安全防护进行了详细规定。这些信息包括但不限于账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息和借贷信息等。

类别	说明	举例
C3	C3 类别信息主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害。	● 银行卡磁道数据（或芯片等效信息）、卡片验证码（CVN 和 CVN2）、卡片有效期、银行卡密码、网络支付交易密码； ● 账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码； ● 用于用户鉴别的个人生物识别信息。
C2	C2 类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害。	● 支付账号及其等效信息，如支付账号、证件类识别标识与证件信息（身份证、护照等）手机号码。 ● 账户（包括但不限于支付账号、证券账户、保险账户）登录的用户名。 ● 用户鉴别辅助信息，如动态口令、短信验证码、密码提示问题答案、动态声纹密码；若用户鉴别辅助信息与账号结合使用可直接完成用户鉴别，则属于 C3 类别信息。 ● 直接反映个人金融信息主体金融状况的信息，如个人

		财产信息（包括网络支付账号余额）、借贷信息。 ● 用于金融产品与服务的关键信息，如交易信息（如交易指令、交易流水、证券委托、保险理赔）等。 ● 用于履行了解你的客户（KYC）要求，以及按行业主管部门存证、保全等需要，在提供产品和服务过程中收集的个人金融信息主体照片、音视频等影像信息。 ● 其他能够识别出特定主体的信息，如家庭地址等。
C1	C1 类别信息主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响。	● 账户开立时间、开户机构； ● 基于账户信息产生的支付标记信息； ● C2 和 C3 类别信息中未包含的其他个人金融信息。

《金融数据安全 数据安全分级指南》（JRT 0197-2020）是由中国人民银行正式发布的金融行业标准。该标准详细阐述了金融数据安全分级的目标、原则和范围，并明确了数据安全定级的要素、规则和定级过程。

根据该标准，金融业机构在开展电子数据安全分级工作时，需要遵循一定的规则和流程。具体来说，标准将数据安全级别从高到低划分为五级，即非常严重、严重、中等、轻微和无影响。每一级的数据特征都有明确的说明，以便金融机构能够更好地进行数据分类和保护。

《指南》对金融数据进行了细致的分类，将其划分为四大一级子类：客户数据、业务数据、经营管理数据和监管数据。这一框架进一步细分为四级子类，并特别整合了个人金融信息的分类。每个最小子类都设定了相应的最低安全级别，用 1 至 5 的数字标识，以表示安全级别的高低。

表 A.1 金融业机构典型数据定级规则参考表

数据归类和细分							安全级别	备注
一级子类	二级子类	定义说明	三级子类	定义说明	四级子类	内容	最低安全级别参考	
客户	个人	指金融业机构提供各种业务服务的自然人对象相关的各类信息。	个人自然信息	指个人的自然属性信息，即个人本身具有的属性，而非在金融业机构业务开展过程中产生的属性信息。	个人基本概况信息	指个人基本情况数据，如个人姓名、性别、国籍、《海外账户纳税法案》（FATCA）有关个人身份数据、民族、婚姻状况、证件类型、证件号码、证件生效日期、证件到期日期、家庭住址等。	3	
					个人财产信息	指个人的财产数据，如个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额、个人社保与医保存缴金额等。	3	
					个人联系信息	指个人各类通信联系方式数据，如手机、固定电话、电子邮箱地址、微信号等。	3	
					个人健康生理信息	指个人生病医治过程中产生的相关记录数据，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的其他信息，如吸烟史等。	4	
					个人地理位置信息	指描述能具体定位到个人的地理位置数据，如包含所在国家、城市、区域、街道、经纬度等维度信息下的常在位置和当前位置等 。	3	

《指南》以其严密的逻辑和实用性，成为金融行业数据分类分级的重要参考。在国家金融监督管理总局发布《银行保险机构数据安全管理办法（征求意见稿）》之前，几乎所有银行都以《指南》为标准进行数据分类分级，对银行业的数据安全管理和建设起到了关键性的作用。《指南》的实施，不仅提高了数据管理的规范性，也加强了金融机构对数据安全的重视，为行业的稳健发展提供了有力保障。

《银行保险机构数据安全管理办法（征求意见稿）》（以下简称《办法》）是由国家金融监督管理总局起草的，旨在规范银行业和保险业的数据处理活动，保障数据安全和金融安全，促进数据的合理开发利用，并保护个人和组织的合法权益。

《办法》要求：“银行保险机构应当对机构业务及经营管理过程中获取、产生的数据进行分类管理，数据类型包括客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。”“银行保险机构应当根据数据的重要性和敏感程度，将数据分为核心数据、重要数据、一般数据。其中，一般数据细分为敏感数据和其他一般数据。”

《银行保险机构数据安全管理办法（征求意见稿）》一经发布，因其强大的监管属性，迅速成为金融行业关注的焦点。监管范围内的机构纷纷响应，组织深入学习研讨，并着手进行合规性评估与建设工作。

然而，《办法》在数据分类分级的定义上与《金融数据安全 数据安全分级指南》存在差异，且《办法》仅对数据进行了一级分类，缺乏进一步的细化指导，这给机构在合规建设过程中带来了一定的挑战。为了应对这些挑战，行业内提出了以下三种解决方案：

- 推倒重建：全面采纳《银行保险机构数据安全管理办法（征求意见稿）》的分类分级标准，放弃原有的《金融数据安全 数据安全分级指南》，重新构建数据分类分级体系。这种方法可能会带来较大的工作量和成本，但有助于确保与监管要求的一致性。
- 双轨并行：保持《银行保险机构数据安全管理办法（征求意见稿）》和《金融数据安全 数据安

全分级指南》两套标准并行使用。机构可以根据不同的业务场景和数据类型，灵活选择适用的分类分级标准。这种方法可以减少因标准变更带来的冲击，但可能会导致管理上的复杂性和不一致性。

- 融合创新：将《银行保险机构数据安全管理办法（征求意见稿）》和《金融数据安全 数据安全分级指南》两套标准进行整合，形成一套融合了两者优点的新标准。这种方法需要深入分析两套标准的差异和联系，通过创新来解决兼容性问题，最终实现数据分类分级的统一和优化。

统计数据揭示了金融行业在数据安全方面的积极进展，其中超过 90%的单位依据行业标准开展了数据分类分级工作，这表明整个行业对数据安全问题给予了高度重视。然而，只有不到 30%的单位对所有数据进行了分类分级，这反映出数据分类分级工作的复杂性，可能由以下几个因素导致：

- 数据多样性：金融行业涉及的数据类型繁多，包括交易数据、客户信息等，每种数据都有其特定的属性和安全要求。
- 数据信息壁垒：金融行业普遍采用直接采购的应用系统，但系统供应商往往不提供关键信息，如数据字典。这种情况导致金融机构难以准确理解数据表和数据字段的具体含义。
- 技术挑战：数据分类分级需要精确的技术手段来识别、分类和分级数据，这对技术能力和系统支持提出了较高要求。
- 资源限制：进行数据分类分级可能需要大量的人力和财力资源，一些单位可能因为资源有限而无法全面实施。
- 组织文化和流程：单位内部的数据管理文化和流程可能影响数据分类分级的实施效率和效果。

为了应对上述挑战，行业内提出了以下解决方案：

- 优先采用最新监管文件要求，辅以行业/国家标准开展金融机构数据分类分级。主要采取其中 1-2 份文件作为分类分级的重要参考。
- 开展信息系统元数据规范工作，补充信息系统、表单、字段元数据信息，去除无效表、无效字段，提升数据含义的可读性；
- 制定数据分类分级的具体规则，采用系统自动化辅以人工校验的方式，对数据进行分类分级，映射到表单、字段。
- 在人力财力资源有限的前提下，可由技术部门牵头开展数据分类分级工作，形成数据分类分级结果由业务部门调整、确认。

加强金融机构数据分类分级的知识宣贯，试点数据分类分级应用场景，让更多部门、更多员工融入数据分类分级安全管理工作中，切实体会数据分类分级工作为机构带来的安全、合规方面的提升。

第十二节　自动化数据分类分级工具

第 7 题　　贵公司使用自动化分类分级工具的效果如何？ [单选题]

选项	小计	比例
自动化程度较高、准确率较高，能够自动识别 50%以上的数据	10	22.73%
自动化程度一般、准确率一般，大部分工作需要人工介入	11	25%
没有采用自动化分类分级工具	23	52.27%
本题有效填写人次	44	

行业普遍认为，金融机构在没有使用数据分类分级自动化工具的情况下，将面临以下挑战，从而难以有效完成数据分类分级工作：

- 数据量庞大：金融机构处理的数据量通常非常庞大，手动进行数据分类分级不仅耗时耗力，而且难以保证效率和准确性。自动化工具可以快速处理大量数据，提高工作效率。
- 准确性需求：数据分类分级的准确性直接关系到数据安全和合规性。自动化工具通过内置算法和规则库，可以更准确地识别和分类数据，减少人为错误。
- 法规遵从：随着数据安全法规的日益严格，金融机构需要确保数据分类分级符合国家和行业的标准。自动化工具通常内置了这些标准，帮助机构轻松遵从法规要求。
- 持续更新和维护：数据的分类分级不是一次性的任务，而是一个持续的过程。自动化工具可以定期扫描和更新数据分类，适应数据变化和业务发展的需求。
- 数据资源的全面梳理：金融机构需要对自身的数据资源进行全面梳理，形成统一的数据资产清单。自动化工具可以帮助机构快速完成这一步骤，为后续的分类分级工作打下基础。

数据分类分级的自动化工具是现代企业数据管理的重要组成部分，其主要目的是通过智能化技术实现对海量数据的高效、准确分类和分级。这些工具通常具备以下核心能力：

- 数据资产发现能力：这是数据分类分级自动化工作的基础，需要为整个系统提供充分的数据输入。在数据分类分级工作中，数据资产发现是必要的能力，并且对于持续的数据安全运营，数据资产发现能力也是一个必选项。

- 动态感知能力：一些工具具备数据源自动发现、DDL 变更自动捕获、数据量级动态监测等能力，实时监测数据动态变化，实现对资产的动态化、持续化感知。
- 智能化分类分级能力：采用规则匹配、智能推荐、机器学习、自然语言处理（NLP）、大模型等多种智能技术，推动分类分级智能、高效落地。
- 敏感数据识别和自动分类分级能力：利用自然语言处理技术和基于机器学习的结构化数据识别技术，辅助人工核查处理敏感数据。例如，某些工具可以根据行业敏感数据和分类分级规范要求，基于人工智能技术进行敏感数据的识别和分类分级。
- 周期性扫描和持续运营能力：自动化周期性扫描数据资产，智能分类分级，识别敏感数据，生成数据分类分级全景图，支持多样化输出方式。
- 知识库和模板能力：一些工具内置了丰富的行业分类分级标准及智能化技术，快速完成数据模型与业务模型的自动映射。

数据分类分级自动化工具的这些能力不仅提升了数据分类分级的效率和准确性，而且大大减少了人工投入的工作量，从而提升了企业的数据管理水平和安全性。在实际应用场景中，通过自动化工具直接执行数据分类分级任务，利用其高度自动化的特性，结合对策略的持续优化以适应实际情况，可以显著减少人工工作量并提升工作效能。

尽管理论上自动化分类分级工具被寄予厚望，但实际应用中的表现并不总是尽如人意。根据调研结果，在那些采用自动化工具的金融机构中，情况呈现出两极分化：大约 48%的机构报告说他们的工具“自动化程度较高，准确率也较高，能够自动识别超过 50%的数据”。然而，另外 52%的机构的体验却大相径庭，他们认为工具“自动化程度一般，准确率一般，大部分工作需要人工介入”。更有一些机构表示，他们所使用的自动化工具的识别准确率仅为 15%，这一数字远低于预期。

市场的这些反馈向数据安全厂商发出了双重信号：一方面，厂商需要不断优化工具的性能，以满足用户的实际需求；另一方面，机构与厂商之间的紧密合作至关重要，这有助于确保技术工具能够发挥出其应有的潜力和效果。关于国家/行业标准中有关数据分类分级方法在自动化分类分级工具中的落地规则和实现技术，也是未来一段时间厂商和用户合作研究、实践的热点。

目前，约 52%的机构还未采用自动化的数据分类分级工具。这些机构需要深入理解自动化工具在提升效率、降低成本和增强数据安全性方面的关键作用。依赖人工进行数据分类分级不仅效率低下，而且成本高昂，更重要的是，这种做法存在引发严重安全风险的可能。在积极推进自动化工具建设的同时，建议这些机构先从业务角度出发，对数据进行初步的粗粒度分类和分级，以尽可能实现对不同数据类别和级别的有效差异化管理，从而保障数据的安全性。

第四章　数据安全管理

第十三节　数据安全管理办法

第 8 题　　贵公司是否制定了数据安全管理办法？ [单选题]

选项	小计	比例
已制定了数据安全管理办法，但是没有参照金融监督管理总局的《银行保险机构数据安全管理办法》（征求意见稿）	28	63.64%
已参照金融监督管理总局的《银行保险机构数据安全管理办法》（征求意见稿）制定了数据安全管理办法	14	31.82%
未制定数据安全管理办法	2	4.55%
本题有效填写人次	44	

数据安全管理办法是金融机构为保障数据处理过程中的安全而制定的一系列规范和措施，旨在防止数据被非法获取、篡改、泄露或滥用，确保数据的完整性、可用性和机密性。鉴于金融机构处理大量敏感数据，如客户个人信息和交易记录，这些数据不仅具有高价值，也容易成为攻击目标。因此，建立数据安全管理办法不仅是为了遵守《中华人民共和国数据安全法》等相关法律法规，确保数据处理活动合法合规，而且是为了防止数据泄露和滥用，保护客户隐私和金融机构的声誉，确保数据的准确性和可靠性，支持业务决策和运营，同时也是履行对客户和社会的责任，保护公共利益。

在制定数据安全管理办法时，金融机构可以参考以下法律法规和行业标准，以确保其数据处理活动合法、安全且高效：

一、《数据安全法》：作为数据安全管理的基石，该法律为数据安全提供了全面的法律框架，确保数据处理活动符合国家的安全要求。

二、《个人信息保护法》：专门针对个人信息的收集、存储、使用和保护等方面提供法律指导，保障个人信息主体的合法权益。

三、《银行保险机构数据安全管理办法（征求意见稿）》：由国家金融监督管理总局起草，旨在规范银行业保险业的数据处理活动，保障数据安全和金融安全，促进数据的合理开发利用。

四、《金融数据安全 数据安全分级指南》(JR/T 0197-2020)：由中国人民银行科技司等单位起草，为金融业机构开展电子数据安全分级工作提供了目标、原则、范围以及定级要素、规则和定级过程。

五、《个人金融信息保护技术规范》(JR/T 0171-2020)：专门针对金融领域个人金融信息保护的标准，从技术和管理两个方面对个人金融信息的全生命周期保护提出规范性要求。

六、《金融数据安全 数据生命周期安全规范》(JR/T 0223-2021)：定义了数据全生命周期的安全框架，将数据分类分级的基本精神贯彻于数据生命周期的各个环节，确保数据在各个阶段的安全。

七、《银行业金融机构数据治理指引》：由中国银行保险监督管理委员会（现国家金融监督管理总局）发布，旨在加强银行业金融机构的数据治理，提高数据管理和数据质量质效。

八、《证券期货业数据安全管理与保护指引》(JR/T 0250-2022)：由中国证券监督管理委员会发布，是证券期货业机构在开展数据安全管理与保护工作时的重要参考和指引。

这些法律法规和标准为金融机构提供了一个全面的框架，指导其在数据安全管理中遵循最佳实践，确保数据的安全性和合规性。

调研发现，超过 95%的金融机构已经制定了数据安全管理办法，但其中约有 2/3 的金融机构制定的数据安全管理办法没有依据国家金融监督管理总局发布的《银行保险机构数据安全管理办法（征求意见稿）》，对于银行保险机构来说，可能制定出的数据安全管理办法在合规性上会存在不足；另约有 1/3 的机构已经根据金融监督管理总局发布的《银行保险机构数据安全管理办法（征求意见稿）》制定了相关管理办法或对原有制度进行了修订，显示出他们对法规的积极响应和较高的规范性。然而，仍有近 5%的机构未制定任何数据安全管理办法，这不仅违反了相关法规，也暴露出严重的数据安全风险。

为确保金融机构制定的数据安全管理办法符合国家法律法规和监管规定，并与机构业务流程紧密结合，金融机构可从组织结构、流程设计、技术实施、文化建设等多个方面入手，采取以下步骤优化和完善数据安全管理办法：

一、制定数据安全总体策略，明确数据安全目标：数据安全目标应与金融机构整体业务目标一致，并获得高层管理人员的支持和承诺，确保数据安全策略在全公司范围内得到重视和执行。

二、建立数据安全治理架构：建立覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构，明确岗位职责和工作机制，落实资源保障；建立数据安全责任制，明确数据安全归口管理部门、业务部门、风险合规与审计部门、数据安全技术保护部门等部门的数据安全责任，形成多层级治理架构。

三、数据分类与分级管理：开展对全域数据资产的登记管理，建立数据资产地图，作为数据安全合规工作的起点和重点；制定数据分类分级保护制度，建立数据目录，实施差异化保护措施。

四、整合数据安全流程：将数据安全控制措施整合到业务流程中，建立包括数据收集、存储、使用、

加工、传输、提供、公开等环节的管理要求和操作规程。

五、技术实施与控制：建立数据安全技术保护体系和数据安全保护基线，将数据安全保护纳入信息系统开发生命周期框架，并纳入网络安全等级保护。

六、风险监测与处置：将数据安全风险纳入现有的风险管理体系，定期开展数据安全风险评估和数据安全审计，明确机构在各阶段的合规义务。对数据生存周期进行安全监控，定期汇总、分析数据安全问题，形成数据安全知识库。

七、数据安全事件管理：建立数据安全事件应急预案，明确数据安全事件的发现、评估、上报、处置、跟踪和反馈等方面的流程和要求。数据安全事件应急响应预案应明确：责任分工、实施环节、需配套的应急响应措施，实施环节应包括事件监测、定位、分级、启动、响应处置、报告、事件评估、结束响应、应急总结、情况跟踪等阶段。

八、数据跨境管理：明确向境外提供数据的监管适用情形，禁止未经批准向境外提供境内个人信息和重要数据信息。

九、第三方合作中的数据安全管理：将外部数据采购、数据委托处理、共同处理等活动纳入信息科技外包管理范围，加强对第三方合作中的数据安全管理。同时，应限制他们对敏感数据的访问权限，仅在必要时提供最小必要的数据访问权限。企业对合作方资质进行审核，需求部门在数据合作开展前，对合作方的信用情况、是否发生过数据安全事件等进行调研，对合作方数据安全保护能力进行合规性评估，与系统合作方签订服务合同、安全保密协议等，确保其具备相应的保密及运营资质。对第三方人员进行安全培训，确保他们具备必要的数据安全意识和技能，并签署保密协议。

十、数据安全文化建设：建立数据安全培训和激励机制，推广数据安全文化，树立数据安全意识。将数据安全管理纳入考核，确保数据安全意识和行为得到有效执行和持续改进。

十一、持续改进与反馈机制：建立持续改进机制，鼓励员工提出数据安全方面的建议和改进意见。

十二、数据安全审计：应定期进行全面的数据安全审计，以识别潜在的安全漏洞和合规性问题。审计过程中，应确保对敏感数据的访问控制、加密措施和日志记录等关键安全实践进行严格评估和改进。

第十四节　企业级数据架构

第 9 题　　贵公司是否建立了企业级的数据架构？ [多选题]

选项	小计	比例

已依据监管要求开展了数据治理，建立了企业级的数据架构	27	61.36%
已根据公司业务发展需要，建立了企业级的数据架构	22	50%
已采用信息系统支持，实现了数据地图	11	25%
以上都没有	5	11.36%
本题有效填写人次	44	

企业级数据架构（Enterprise Data Architecture, EDA）是一个全面的框架，用于指导企业如何管理和使用其数据资源。它涵盖了数据的收集、存储、管理、分析和分发等各个方面。企业级数据架构的目的是确保数据的一致性、可访问性、安全性和有效利用。

金融机构建立企业级数据架构是至关重要的，因为它不仅能够确保数据处理的合规性，满足监管要求，还能够提高数据的质量和一致性，从而支持更准确和快速的业务决策。通过统一的数据视图，金融机构能够促进不同部门和系统之间的数据共享和协作，打破信息孤岛，降低数据冗余和重复投资，同时增强数据的安全性和隐私保护。此外，企业级数据架构为新业务和数据分析提供了灵活的数据支持，有助于金融机构在竞争激烈的市场中实现业务创新和提升客户服务体验。最终，这种架构的建立有助于金融机构实现数据驱动的增长，优化运营效率，降低风险，并确保在快速变化的金融环境中保持竞争力。

调研结果显示，参与调研的金融机构在推进数据治理和构建企业级数据架构方面表现出明显的差异性：

一、约有 61%的金融机构已依据监管要求开展了数据治理：表明大多数机构已经认识到了数据治理的重要性，并开始按照监管机构的要求，建立相应的数据治理机制和企业级数据架构。这一举措有助于确保数据处理的合规性，提高数据的质量和一致性。大部分机构是在监管要求的推动下开始数据治理和企业级数据架构建设的，这也表明了合规性是推动数据治理工作的重要动力。

二、50%的机构已根据公司发展需要，建立了企业级的数据架构：显示了这些机构已经将数据治理和企业级数据架构的建设与自身的业务发展紧密结合，通过优化数据管理来支持业务决策和创新。

三、25%的机构已采用信息系统支持，实现了数据地图：数据地图是企业级数据架构的重要组成部分，能够帮助机构更好地理解和管理其数据资源。这一比例较低说明许多机构在数据可视化和管理方面还有很大的提升空间。

四、约 11%的机构没有建立企业级数据架构：这一比例虽然较小，但仍然表明有一部分机构在数据治理和企业级数据架构建设方面存在滞后，可能面临数据管理混乱、数据安全风险增加等问题。

企业级数据架构在不同规模的金融机构中实施的难易程度存在显著差异，主要受以下因素影响：

一、资源投入：大型金融机构通常拥有更多的资金和人力资源，能够投入更多的资源进行数据架构的建设和优化。相比之下，中小金融机构可能在资源上相对有限，实施难度较大。

二、技术能力：大型金融机构往往拥有更强大的技术团队和更先进的技术平台，能够更好地支持复杂的数据架构设计和实施。而中小金融机构可能在技术能力上存在短板，需要更多依赖外部支持。

三、业务复杂度：不同规模的金融机构在业务复杂度上也有所不同。大型金融机构业务覆盖面广，业务流程复杂，数据架构设计需要考虑的因素更多，实施难度相对较高。中小金融机构业务相对简单，数据架构设计和实施相对容易。

四、数据治理：数据治理是企业级数据架构实施的关键环节。大型金融机构通常已经建立了较为完善的数据治理体系，能够更好地支持数据架构的实施。而中小金融机构在数据治理方面可能还不够成熟，需要加强数据治理体系建设。

五、组织架构：金融机构的组织架构也会影响数据架构的实施。大型金融机构往往拥有更为复杂的组织架构，需要在不同部门和业务条线之间进行协调和整合，实施难度较大。中小金融机构组织架构相对简单，实施起来相对容易。

六、监管要求：金融机构需要遵守严格的监管要求，不同规模的金融机构在监管要求的执行上可能存在差异。大型金融机构通常受到更为严格的监管，需要在数据架构设计中考虑更多的合规性要求，实施难度较大。

七、文化和意识：金融机构的企业文化和数据意识也会影响数据架构的实施。一些金融机构可能已经形成了较强的数据驱动文化，员工对数据的重视程度较高，这有助于数据架构的顺利实施。而一些金融机构可能在数据意识上还有待提升，需要加强员工的数据培训和教育。

八、技术选型：在技术选型方面，大型金融机构可能有更多的选择和尝试机会，能够选择更适合自身需求的技术方案。而中小金融机构在选择技术方案时可能受到预算和资源的限制，需要更加谨慎和务实。

金融机构建立企业级数据架构是一个全面而系统的过程，涉及从战略规划到技术实施的多个步骤：

一、明确监管要求：金融机构需要首先明确监管机构对数据治理和数据架构的具体要求。例如，《银行业金融机构数据治理指引》强调了数据治理架构的建立，明确了数据管理和数据质量控制的要求，并要求加强监管监督，与银行的监管评级挂钩。

二、制定数据战略：结合自身发展战略和监管要求，制定全面科学有效的数据战略，并确保其有效执行和修订。数据战略应涵盖数据的收集、存储、使用、加工、传输、提供、公开等各个环节。

三、建立数据治理架构：建立组织架构健全、职责边界清晰的数据治理架构，明确董事会、监事会、

高级管理层和相关部门的职责分工，建立多层次、相互衔接的运行机制。这有助于确保数据治理工作的有效开展和监管要求的落实。金融机构可根据自身数据战略和组织架构特征，对于数据需求较少或复杂程度较低的机构，可以采用“分散模式”，各部门负责本领域的数据管理和应用；对于数据需求较多且复杂程度较高的机构，可采用“归口管理模式”“集中+派驻模式”或“全集中模式”的数据治理组织架构。

四、制定数据管理制度：制定全面科学有效的数据管理制度，涵盖组织管理、部门职责、协调机制、安全管控、系统保障、监督检查和数据质量控制等方面，并持续更新以适应监管要求和业务发展。

五、数据分类与分级管理：实施数据分类与分级管理，进行风险评估，确保数据的安全性和合规性。

六、技术选型和实施：选择合适的数据存储、处理和分析技术，如数据仓库、大数据平台和云计算，并集成现有业务系统和数据源，确保数据的一致性和可访问性。

七、建立数据安全策略：建立数据安全策略与标准，依法合规采集、应用数据，依法保护客户隐私，划分数据安全等级，明确访问和拷贝等权限，监控访问和拷贝等行为，完善数据安全技术，定期审计数据安全。

八、数据质量管理：确立数据质量管理目标，建立控制机制，确保数据的真实性、准确性、连续性、完整性和及时性。数据质量监控体系应覆盖数据全生命周期，对数据质量持续监测、分析、反馈和纠正，确保数据的真实性、准确性、连续性、完整性和及时性。

九、数据治理自我评估：建立数据治理自我评估机制，明确评估周期、流程、结果应用、组织保障等要素的相关要求。定期评估数据治理的有效性并按年度向监管机构报送。建立持续改进机制，定期评估数据架构的有效性，并根据业务发展和技术变化进行调整。

十、监管数据报送：建立适应监管数据报送工作需要的信息系统，实现流程控制的程序化，提高监管数据加工的自动化程度，确保监管数据的准确性和及时性。同时，应加强数据采集的统一管理，明确系统间数据交换流程和标准，实现各类数据有效共享。

数据价值实现：在风险管理、业务经营与内部控制中加强数据应用，实现数据驱动，提高管理精细化程度，发挥数据价值。通过数据分析，合理制定风险管理策略、风险偏好、风险限额以及风险管理政策和程序，监控执行情况并适时优化调整。

第十五节　数据安全评估

第 10 题　贵公司是否在处理敏感级及以上数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，事先开展了数据安全评估？[单选题]

选项	小计	比例
已开展了数据安全评估	19	43.18%
只针对个人金融信息开展了安全评估	16	36.36%
未开展数据安全评估	9	20.45%
本题有效填写人次	44	

在数字经济迅猛发展的今天，数据已被视为新时代的“石油”，它不仅是经济增长的引擎，也是金融机构业绩提升的关键动力。然而，随着金融行业与各领域业务的深度融合以及新兴业态的兴起，数据的委托、共享与转让行为日益频繁，这无疑加剧了数据安全的风险。仅在 2024 年上半年，就有多起影响深远的数据泄露事件震惊业界，泄露的数据量高达十亿条，且这一数字还在不断上升。

数据泄露不仅可能导致客户信息被非法利用，引发金融诈骗和信用危机等社会问题，还可能严重损害金融机构乃至整个行业的声誉和稳定性。因此，对于敏感数据的安全管理，尤其是在业务合作和外包过程中，进行严格的数据安全评估和风险控制，对金融机构来说显得尤为关键。

在国家和行业监管层面，中国在 2021 年颁布的《中华人民共和国数据安全法》中强调了建立数据安全风险评估机制的重要性，这标志着我国在数据安全评估制度建设上迈出了重要步伐，体现了国家顶层设计与行业实践的同步发展。全国金融标准化技术委员会相继发布了《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）和《金融数据安全 数据安全评估规范（征求意见稿）》等标准，为金融机构提供了开展数据安全评估的指导。尽管如此，这些标准与实际落地执行的成熟度之间还存在一定差距。

在金融机构自身建设方面，据调研显示，约 80%的金融机构已经认识到数据安全评估对于保障业务安全稳定发展的重要性，并开始采取行动。然而，由于数据治理能力、数据分类分级水平、监管关注点、执行标准和司法解释的明确性与可执行性、数据泄露对客户的影响以及安全投资成本等因素的限制，大部分金融机构选择首先针对涉及个人金融信息的业务进行个人金融信息安全影响评估。同时，约有 43%的能力较强的机构已经开始实施针对全敏感数据的数据安全评估。

金融机构在执行数据安全评估时，面临多重挑战。首先是合规性问题，随着监管框架的不断完善，《网络安全法》《数据安全法》《个人信息保护法》为数据安全顶层监管框架，持续在出台和更新一系列《关于银行业保险业数字化转型的指导意见》《中国银保监会监管数据安全管理办法》《保险中介机构信息化工作监管办法》《证券期货业网络和信息安全管理办法》等，监管要求变得更加严格和细化，金融机构需不断适应以满足这些高标准。其次，数据分类分级工作本身复杂且耗时，尤其在处理海量数据时，现有工具在敏感数据的识别上难以达到理想效果。第三，数据流动监测同样充满挑战，伴随着业务经营模式、合作模式的不断创新，对于数据流动、挖掘、汇聚融合、智能处理需求的多样性和复杂性正在日益增加，使

得数据流动路径变长，监测工作变得更加复杂。最后，合作对象的多样性也是一个问题，不同合作机构在数据安全管理能力上存在差异，一些如互联网大厂、电信运营商、大型金融服务机构相对在供应链管理、安全管理等方面的自身能力较强，对于数据的保护较好，但也会随着大数据、云计算等新技术的应用，带来新的数据安全威胁；而一些快消、催收、法律服务类的中小型供应商则可能因科技和安全投入不足，成为数据安全控制的薄弱环节。

为提升金融机构的数据安全评估工作，以下是几点建议：

- 首先，数据安全评估是保障数据安全的重要途径，能够帮助金融机构识别潜在的安全风险并制定针对性的防范措施。根据互联网大厂的实践经验，落地数据安全评估可以基于 DSMM、DSG 等数据安全治理评估模型，从组织建设、制度流程、技术工具、人员能力四个关键维度，对数据的采集、传输、存储、处理、交换、销毁全生命周期进行风险识别和评估，发现金融数据存在的安全风险。同时，评估工作也可以借鉴金融行业外包风险管理的经验。
- 其次，数据安全评估能力建设需要依赖于数据分类分级工作的进展。建议优先对数据出口系统进行数据分类分级，以便更准确地确定评估的对象和范围。
- 第三，针对新技术应用带来的新风险，可以与技术能力强的合作机构建立供应链数据安全联盟，共同构建覆盖上下游的数据安全防护体系。同时，结合监管通报和事件中揭示的新风险，如云服务的数据泄露，通过行业协会和联盟抵制供应链中的不法供应商。

最后，针对科技能力和安全投入普遍较低的行业合作伙伴，金融机构可以利用自身的技术能力，例如开发 VDI 等安全的云服务，防止数据在供应商处落地。此外，根据业务模式特点，聚焦供应商接触处理数据的人员，从安全管理机制、背景审查、安全意识培训、操作风险防范、事件响应报告等方面，对供应商提出成本可控的安全要求，以提升其数据保护能力。

第十六节　企业级数据服务管理体系

第 11 题　　贵公司是否建立了企业级数据服务管理体系？[多选题]

选项	小计	比例
制定了数据服务规范	24	54.55%
建立了专职数据服务团队	36	81.82%

统筹了内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动	27	61.36%
以上都没有	4	9.09%
本题有效填写人次	44	

企业级数据服务管理体系（Enterprise Data Service Management System）是一套综合性的管理框架，旨在优化企业的数据资源管理、提升数据服务质量，并确保数据在企业运营中的有效利用。

金融机构建立企业级数据服务管理体系至关重要，因为它不仅有助于确保数据处理的合规性、安全性和效率，而且能够促进数据的一致性、可访问性和可利用性。通过建立企业级数据服务管理体系，金融机构能够更好地管理和利用其庞大的数据资产，支持复杂的业务决策、风险评估和客户服务。此外，随着监管要求的日益严格和市场竞争的加剧，一个健全的数据服务管理体系能够确保金融机构在快速变化的环境中保持竞争力，同时提升其对市场变化的响应速度和灵活性。更重要的是，它能够加强数据治理，提高数据质量，从而为金融机构的数字化转型和创新提供坚实的基础。通过建立企业级数据服务管理体系，金融机构能够实现数据驱动的增长，优化运营效率，降低风险，并确保在提供高质量服务的同时，满足监管和合规要求。

调研结果揭示了金融机构在数据服务管理体系建设方面的现状和差异：

- 超过半数的金融机构已经建立了数据服务规范，意识到了标准化对于提升数据服务质量和一致性的重要性，并已开始实施相关措施。
- 绝大多数金融机构，即约 82%，已经组建了专门的数据服务团队，显示出对数据服务管理的高度重视和对专业人才的投入。
- 略超过半数的机构，约 61%，能够统筹内外部数据的加工和分析，并实施数据服务的全生命周期管理，包括需求分析、服务开发、部署和监控等活动，显示了这些机构在数据服务管理上的综合性和系统性。
- 然而，仍有约 9%的机构尚未开始构建数据服务管理体系，这暗示它们可能面临数据管理不规范和服务质量不稳定的挑战，需要在数据服务管理方面进行改进和加强。

监管要求可能是推动金融机构建立数据服务管理体系的重要因素，《银行保险机构数据安全管理办法（征求意见稿）》要求“银行保险机构应当建立企业级数据服务管理体系，制定数据服务规范，建立专职数据服务团队，统筹内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动”。《银行业金融机构数据治理指引》也是重要的监管依据，明确了数据治理的基本原则、组织架构、

数据管理、数据质量控制和数据价值实现等方面的要求。金融机构需要确保其数据服务符合监管标准，以避免潜在的合规风险。并且，随着市场竞争的加剧，金融机构需要通过建立数据服务管理体系来提升服务质量和响应速度，以满足客户需求和市场变化。

金融机构建立企业级数据服务管理体系是一个战略性和系统性工程，它涉及从组织架构、流程规范到技术平台的全方位构建。以下是金融机构建立企业级数据服务管理体系的一般步骤：

一、战略规划与目标设定：首先，金融机构需要明确数据服务管理体系的战略目标，包括提升数据质量、促进数据共享、增强数据驱动决策等。

二、组织架构建设：建立一个由高层领导支持的组织架构，包括数据治理委员会、数据管理部门和跨部门协作团队，确保数据服务管理体系的有效运行。

三、数据治理章程制定：制定企业级的数据治理章程，作为数据服务管理体系的指导性文件，明确数据管理的基本原则、职责分工和操作规范。

四、数据服务规范建立：依据业务需求和监管要求，制定数据服务规范，包括数据采集、处理、存储、传输和共享的标准和流程。

五、专职团队组建：组建由数据科学家、工程师、分析师等组成的专职数据服务团队，负责数据服务的规划、开发、部署和监控。

六、内外部数据整合：统筹内外部数据资源，通过数据集成技术实现数据的统一管理和加工，确保数据的一致性和可用性。

七、需求分析与服务开发：与业务部门紧密合作，进行数据服务需求分析，开发满足业务需求的数据服务和应用。

八、技术平台建设：构建企业级的数据管理和分析平台，利用大数据、云计算等技术提高数据处理和分析的能力。

九、服务部署与监控：将开发的数据服务部署到生产环境，并通过监控系统持续跟踪服务性能和效果，确保服务质量。

十、数据安全与合规性：确保数据服务管理体系遵循数据保护法规和标准，保护客户隐私和数据安全。

十一、质量控制与持续改进：建立数据质量控制流程，持续提升数据质量，并通过反馈机制不断优化数据服务。

十二、培训与文化建设：对团队成员进行数据管理和分析技能的培训，同时培养数据驱动的企业文化，提高全行对数据价值的认识。

十三、监管要求与行业实践：密切关注监管机构的指引和要求，结合行业最佳实践，不断提升数据服务管理体系的成熟度和有效性。

通过这一系列步骤，有助于金融机构构建起全面、高效、安全且符合监管要求的企业级数据服务管理体系，为业务发展和风险管理提供强有力的数据支持。

第十七节　数据安全管理机制

第 12 题　　贵公司是否制定了以下数据安全管理机制？ [多选题]

选项	小计	比例
数据收集	40	90.91%
外部数据采购	27	61.36%
数据加工	38	86.36%
数据使用	40	90.91%
数据共享及集团内部共享	30	68.18%
委托处理数据	23	52.27%
数据共同处理	21	47.73%
数据转移	20	45.45%
数据公开	25	56.82%
数据跨境	24	54.55%
数据删除与销毁	31	70.45%
以上都没有	1	2.27%
本题有效填写人次	44	

数据安全管理机制是一套综合的策略和流程，旨在确保数据在整个生命周期中的安全性、完整性和可用性。它涵盖了数据收集、外部数据采购、数据加工、数据使用、数据共享、委托处理、数据转移、数据公开、数据跨境、数据删除与销毁等多个环节，通过制定相应的政策、标准、操作规程和技术支持，来防止数据泄露、滥用、篡改或丢失，同时确保数据的合法合规使用，保护数据主体的隐私权和企业的利益。

金融机构建立数据安全管理机制至关重要，因为它们处理着大量的敏感客户信息和金融交易数据，这些数据一旦泄露或被滥用，不仅会侵犯客户的隐私权，还可能导致巨大的经济损失和声誉风险。有效的数据安全管理机制能够帮助金融机构遵守相关法律法规，防范金融欺诈和网络攻击，从而保护客户利益和自身声誉，增强客户信任，促进业务的稳定发展。

调研结果显示，金融机构在数据安全管理机制的制定上存在一定的差异：

超过 90%的金融机构已经建立了针对数据收集和使用阶段的安全管理制度，这表明了对数据安全管理的高度重视，特别是在数据生命周期的早期阶段。

数据加工环节也受到了广泛关注，有 86%的机构已经制定了相应的安全管理措施，确保数据处理过程的安全性。

在数据删除与销毁环节，70%的公司已经制定了安全管理制度，这反映了对数据生命周期末端安全管理的重视。

在外部数据采购、数据共享及集团内部共享方面，超过 60%的机构已经建立了安全管理制度，以保障数据在流通过程中的安全。

然而，在数据委托处理、数据共同处理、数据跨境、数据公开、数据转移等环节，只有大约 50%的机构制定了安全管理制度，这表明这些环节的安全管理措施有待进一步加强。

特别值得注意的是，约 2%的机构尚未制定任何数据安全管理机制，这暴露了这些机构在数据安全管理方面可能面临的较大风险。

总体而言，金融机构在数据安全管理机制的建设上已取得一定成就，特别是在数据收集、加工和使用等关键环节。但为了确保数据全生命周期的安全，数据转移、委托处理、共同处理、公开等环节的安全管理措施仍需进一步加强和完善。

针对这些发现，金融机构在数据安全管理机制的建设上应采取以下措施：

一、加强数据转移安全：鉴于数据转移的安全管理制度覆盖率相对较低，金融机构应优先加强这一环节的安全措施，包括加密传输、安全协议和访问控制。

二、提升数据公开和跨境安全：对于数据公开和跨境传输，需要制定严格的安全政策，确保符合国内外的数据安全法规，并采取适当的技术措施来保护数据。

三、完善第三方合作安全措施：与第三方合作时，明确数据安全责任，执行严格的安全审查，并签订详尽的数据保护协议。

四、强化数据共享管理：优化数据共享流程，确保只有授权人员能够访问共享数据，并实施有效的监控和审计。

五、数据全生命周期安全管理：强化对数据全生命周期的管理，确保从数据创建到最终销毁的每个环节都有相应的安全措施。

六、持续合规性监控：建立机制以持续监控和更新数据安全措施，确保与法律法规的变化保持一致。

七、促进跨部门协作：加强不同部门间的沟通与协作，确保数据安全政策得到全面理解和执行。

八、加强客户个人信息保护：将客户个人信息保护置于核心位置，通过透明的数据处理政策和提供数据访问及更正途径，增强客户信任。

九、建立评估与反馈机制：定期评估数据安全管理措施的有效性，并根据内部和外部反馈进行必要的调整。

通过这些细致且全面的措施，金融机构能够构建一个既符合监管要求又支持业务灵活性的数据安全管理机制，确保数据安全的同时，促进业务的持续创新和发展。

第十八节　从生产环境提取数据

第 13 题　贵公司是否制定了从生产环境提取数据的管理流程？　[多选题]

选项	小计	比例
已制定管理流程	42	95.45%
审批环节中包含数据安全岗位	26	59.09%
审批环节中包含数据所有者	27	61.36%
明确了数据使用或者保存期限	26	59.09%
明确了数据脱敏要求	32	72.73%
以上都没有	0	0%
本题有效填写人次	44	

从生产环境提取数据指的是从实际运行的业务系统中检索信息和数据的过程。这些数据通常存储在生产数据库或实时运行的系统中，它们直接支持日常业务操作和客户服务。提取生产环境的数据通常是为了特定的业务需求，如报告生成、数据分析、系统测试或审计。出于数据安全和个人信息保护的考虑，访问

生产环境的数据通常需要严格的权限控制和审批流程，并采取安全措施，如使用数据加密和访问日志记录，以防止数据泄露或滥用。

金融机构建立数据提取流程至关重要，原因如下：

一、合规性：确保数据提取活动遵守相关的法律法规和行业标准，如《银行保险机构数据安全管理办法（征求意见稿）》强调了确因业务需要从生产环境提取数据的，应当建立严格的审批程序，并明确数据使用或者保存期限。

二、风险管理：通过规范的数据提取流程，降低数据泄露、滥用或误用的风险，增强数据安全性。在面对数据量激增和业务需求多样化的挑战时，有序的数据提取流程能够帮助金融机构有效管理和利用数据资源。

三、数据治理：强化数据治理，严格控制数据提取活动，确保数据资产得到全面和有效的管理。这不仅有助于维护数据的完整性和可用性，也是金融机构数据战略的关键组成部分。

调研结果表明，参与调研的金融机构普遍认识到了制定数据提取流程的重要性。超过 95%的机构已经制定了从生产环境提取数据的管理流程，显示出这些机构对数据提取过程的规范性和系统性给予了高度重视。在数据提取流程中，有几个关键点需要特别强调：

一、数据安全岗位在审批环节中的参与度不足，仅有不到 60%的机构将数据安全岗位包含在数据提取的审批流程中。

在从生产环境提取数据的管理流程中，数据安全岗位的参与至关重要，他们是确保整个流程安全、合规的关键环节。数据安全岗位运用其专业知识对数据提取流程进行风险评估，保障数据提取活动不会危害到公司的网络安全和数据安全，并监督数据安全保护措施的实施，如对敏感数据进行加密、脱敏处理以及严格的访问控制。通过将数据安全岗位纳入审批环节，金融机构能够构建一个更加稳固和可信的数据提取环境，从而在保障数据安全的同时，支持业务需求和运营效率。

二、数据所有者参与审批环节的比例约为 61%，数据提取审批流程中对数据责任人的参与还有提升空间。

数据所有者在数据提取的管理流程中扮演着至关重要的角色。他们对数据的业务含义和价值有着深刻的理解，能够确保数据提取的目的和使用方式与数据的原始业务目标保持一致。由于数据所有者对数据的敏感性和潜在风险有着充分的认识，他们能够有效评估数据提取请求，防止数据泄露或滥用的风险。此外，数据所有者确保数据的准确性和质量，满足请求者的标准，并在数据提取后监督其使用，确保数据的使用符合既定目的和范围。因此，数据所有者的参与不仅提升了数据提取流程的安全性和合规性，也保障了数据的质量和安全性，对维护金融机构的数据治理和风险管理至关重要。

三、约 59%的机构在管理流程中明确了数据使用或保存期限，这有助于确保数据在整个生命周期中的合规性和安全性。

在数据提取流程中明确数据使用或保存期限一方面有助于确保合规性，避免因违反数据存储政策而产生的法律责任，减少数据长期存储带来的泄露或滥用风险，另一方面通过释放存储空间和计算资源，优化资源配置，降低维护成本。

四、数据脱敏要求得到了较强的重视，约有 73%的公司在流程中明确规定了数据脱敏要求，有助于保护个人隐私和敏感信息。

总体而言，参与调研的机构在数据提取管理流程的制定上表现良好，特别是在数据脱敏要求方面。然而，数据安全岗位和数据所有者的参与度，以及数据使用或保存期限的明确规定方面仍有改善空间，需要进一步提高数据提取流程的全面性和有效性。

金融机构建立数据提取流程需要遵循以下步骤，以确保数据的安全、合规和高效使用：

一、明确业务需求，识别所需数据的类型、范围和目的，确保数据提取的必要性和合理性。

二、制定详细的数据提取管理流程，包括数据提取的指导原则、责任分工和操作步骤。

三、建立严格的审批流程，确保所有数据提取请求都必须经过授权审批，特别是需要数据安全岗位和数据所有者的共同参与。

四、实施基于角色的访问控制，确保只有授权人员能够根据既定权限提取数据。

五、对敏感数据进行脱敏处理，采用加密技术和安全措施保护数据在提取、传输和存储过程中的安全。

六、明确规定数据的使用目的、使用期限和保存期限，以避免数据的不必要长期存储，并确保数据按照既定的时间框架进行处理。

七、选择合适的数据提取工具和技术平台，支持自动化和手动数据提取操作。

八、建立监控机制，定期审计数据提取活动，确保流程的合规性和效率。

九、制定应急响应计划，以便在数据提取过程中出现安全事件时能够迅速有效地应对。

通过这些步骤，有助于金融机构建立一个全面、安全、高效的数据提取流程，支持业务需求的同时，保护数据安全和客户隐私。

第五章　个人信息保护

第十九节　个人信息保护管理体系

第 22 题　　贵公司是否建立了个人信息保护管理体系？ [单选题]

选项	小计	比例
已建立	39	88.64%
未建立	5	11.36%
本题有效填写人次	44	

个人信息保护管理体系是一套综合性的管理框架，旨在确保在收集、存储、使用、传输和共享个人信息的过程中遵守法律法规和行业标准，保护客户隐私和数据安全。中国人民银行早在 2011 年就发布《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》，要求银行业金融机构必须依法收集、使用和对外提供个人金融信息，强化个人金融信息保护和法制意识，防止信息泄露和滥用。2020 年中国人民银行又发布《个人金融信息保护技术规范》，明确了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求。《个人信息保护法》的施行，更明确了金融数字化发展应当遵循的基本准则和行为规范。

调研结果显示，近 90%的金融机构已经建立了个人信息保护管理体系，表明大多数机构已经认识到个人信息保护的重要性，并采取了实际行动来构建相应的管理体系。这一高比例反映了金融机构在个人信息保护方面的积极态度和强烈的责任感。

尽管金融机构在个人信息保护管理体系建设方面取得了显著成效，但它们在个人信息保护方面仍面临诸多挑战：

一、制度不完善或执行不到位

尽管部分金融机构已经制定了个人信息保护政策，但这些政策可能尚未全面覆盖《个人信息保护法》及相关法律法规的要求。例如，一些机构的隐私政策可能过于笼统，缺乏对特定数据类型或处理方式的具体规定。此外，即便政策内容详尽，实际执行过程中也可能存在偏差。例如，员工可能对政策理解不足，或者缺乏必要的培训和监督，导致制度执行不到位，从而无法有效保护客户的个人信息。这种情况不仅违反了法律法规，还可能引发公众对金融机构的信任危机。

二、组织与职责不清

个人信息保护在一些金融机构中往往被视为单一部门的专属责任，导致缺乏跨部门的协作机制。这种分散的管理方式可能形成管理孤岛，影响信息共享和政策执行的一致性。例如，技术部门可能专注于数据安全技术，而忽视了与客户服务部门的沟通，导致客户隐私问题处理不够及时或有效。

三、资源配置紧张

金融机构在人力资源、技术投入等方面存在瓶颈，这使得它们难以满足个人信息保护管理的实际需求。例如，人力资源的不足可能导致隐私政策的制定和执行缺乏足够的专业知识和经验。同时，技术投入的不足可能使得金融机构无法及时更新和维护必要的数据保护技术，从而无法有效应对日益复杂的安全威胁。

四、员工意识与技能不足

部分员工对个人信息安全的重要性认识不足，缺乏基本的保护意识和技能。这种状况可能导致在处理个人信息时出现疏忽，增加数据泄露和滥用的风险。金融机构未能定期对员工进行个人信息保护方面的专业培训，这不仅违反了相关法律法规的要求，也削弱了机构的整体数据保护能力。

五、合规与技术创新矛盾

在金融行业，技术创新是推动业务发展和提升竞争力的关键。然而，随着技术的发展，如何确保个人信息保护的合规性，成为金融机构面临的一大难题。新技术的应用可能会带来新的隐私风险，而现有的法律法规可能尚未完全覆盖这些新情况。同时，金融机构需要在遵守严格的数据保护法规和利用新技术提高服务效率之间找到平衡。

六、安全技术措施不足

部分金融机构在敏感个人信息的存储和传输过程中，未能采用先进的加密技术，这可能导致数据容易被窃取或篡改。例如，使用过时或不安全的加密方法，可能使得数据在传输过程中暴露于风险之中。此外，个人信息访问权限管理不善，可能导致未经授权的个人访问敏感信息，增加了数据泄露的风险。

在对个人信息保护管理的研究和实践中，发现随着《中华人民共和国个人信息保护法》的正式施行，金融机构在个人信息保护方面面临着更为严格的监管要求。为构建和完善个人信息保护管理体系，金融机构应从制度、组织、人员、技术、合作、权利响应、评估、应急响应及合规监督等多个维度出发，采取全面而有效的措施。以下是对金融机构个人信息保护管理体系建设的具体建议：

一、制定全面的个人信息保护制度体系，结合《个人信息保护法》的要求，制定包括数据分类、生命周期管理、隐私保护、加密标准、访问控制、事件响应等在内的政策，并定期更新和审查这些政策，确保其合规性和有效性。

二、健全组织架构与职责分工，设立个人信息保护管理部门或团队，明确各部门和岗位的具体职责，加强部门间的沟通与协作。

三、加强员工管理与培训，提高员工对数据安全重要性的认识程度，建立激励与惩罚机制。

四、强化第三方合作机构管理，严格审查其个人信息保护措施和合规记录，定期进行审计和评估。

五、提升安全技术措施，采用先进加密技术保护敏感数据的存储和传输，实施严格的访问控制策略。

六、保障个人信息主体权利，建立响应个人信息主体权利的机制，明确告知相关权利和处理方式。

七、开展个人信息保护影响评估，识别潜在风险和漏洞，制定风险应对措施。

八、完善应急响应与事件处置机制，制定预案，确保迅速响应和处理安全事件。

九、持续监督与自查，定期进行自查，积极配合监管部门的监督检查。

金融机构应从多个维度出发，构建和完善个人信息保护管理体系，确保个人信息的安全与隐私得到充分保护，符合法律法规的要求，提升机构信誉和客户信任度。

第六章　数据安全风险监测

第二十节　数据安全风险监测

第 23 题　贵公司是否对以下领域开展了数据安全风险监测？[多选题]

选项	小计	比例
超范围授权或者使用系统特权账号	29	65.91%
内部人员异常访问、使用数据	31	70.45%
对数据集中共享的系统或者平台的网络安全、数据安全威胁	24	54.55%
敏感级及以上数据在不同区域的异常流动	16	36.36%
移动存储介质的异常使用	22	50%
外包、第三方合作中的数据处理异常或者数据泄露、丢失和篡改	24	54.55%
客户有关数据安全的投诉	32	72.73%
数据泄露、仿冒欺诈等负面舆情	32	72.73%

以上都没有	3	6.82%
本题有效填写人次	44	

数据安全风险监测是确保数据安全的关键环节，涉及对数据处理活动的持续监控，以识别和评估潜在的安全风险。根据《中华人民共和国数据安全法》第二十九条的规定，开展数据处理活动应当加强风险监测，一旦发现数据安全缺陷或漏洞等风险，应立即采取补救措施；如果发生数据安全事件，也应立即采取处置措施，并按规定及时告知用户和向有关主管部门报告。

对于金融机构而言，中国人民银行发布的《中国人民银行业务领域数据安全管理办法（征求意见稿）》，以及国家金融监督管理总局发布的《银行保险机构数据安全管理办法（征求意见稿）》，都进一步明确了数据安全风险监测的范围和要求。这些规定强调机构应将数据安全风险纳入全面风险管理体系，并明确风险监测评估、应急响应报告、事件处置的组织架构和管理流程。同时，要求建立数据安全风险监测和告警机制，制定数据安全事件定级判定标准和应急预案，规范应急演练、事件处置、风险评估和审计等工作。

《中国人民银行业务领域数据安全管理办法（征求意见稿）》在第六章详细规定了数据处理活动风险监测、数据安全风险情报监测和数据安全通报预警监测的具体要求，列举了 14 项需要重点关注的风险监测事项，包括恶意程序、数据漏洞、未授权数据存储和使用、身份认证强度、数据加工和传输安全等；以及 5 项情报监测事项，包括数据泄露、兜售数据、非法收集、造谣传谣、负面舆情等。《银行保险机构数据安全管理办法（征求意见稿）》第七章第六十五条则明确了 9 项数据安全监测内容，涉及系统账号使用、内部人员数据访问、数据共享平台安全、数据流动监控、移动存储介质使用、外包和第三方合作数据处理、客户投诉、负面舆情以及其他潜在风险事件。

这些规定共同构建了一个全面的框架，它为金融机构提供了一套系统化的风险监测和管理工具，有助于金融机构提升对数据安全风险的识别、防范和响应能力，确保数据的安全性和符合法规要求。

根据调研结果，金融机构在数据安全风险监测方面采取了多项措施，包括但不限于系统特权账号监测、内部人员行为监测、网络安全和数据安全威胁监测等方面，具体如下：

- 系统特权账号的监测：约有 66%的金融机构对超范围授权或使用系统特权账号进行了监测，表明多数机构意识到了对特权账号管理的重要性。
- 内部人员行为监测：约有 70%的金融机构对内部人员异常访问或使用数据的行为进行了监测，说明这些机构非常关注内部人员造成的安全威胁。
- 网络安全和数据安全威胁监测：约有 55%的金融机构对数据集中共享的系统或平台的网络安全和数据安全威胁进行了监测，这反映了对数据共享环境潜在风险的认识。

- 数据流动监测：约有 36%的金融机构对敏感数据在不同区域的异常流动进行了监测，表明超过三分之一的金融机构已经意识到了对数据流动进行监控的重要性，尤其是在不同区域之间对敏感数据的监控。
- 移动存储介质使用监测：50%的金融机构对移动存储介质的异常使用进行了监测，显示了对移动设备潜在风险的关注。
- 外包和第三方合作监测：约有 55%的金融机构对外包或第三方合作中的数据处理异常或数据泄露、丢失和篡改进行了风险监测，表明这些机构在管理第三方风险方面采取了积极措施。
- 客户数据安全投诉监测：约有 72.73%的金融机构对客户有关数据安全的投诉进行了监测，显示了对客户反馈的高度重视。
- 负面舆情监测：约有 73%的金融机构对数据泄露、仿冒欺诈等负面舆情进行了监测，这表明这些机构在维护声誉和应对危机方面采取了措施。
- 约有 7%的金融机构反馈没有进行任何形式的数据安全风险监测，表明这些机构在数据安全风险管理方面存在缺口。

总体来看，调研结果显示多数金融机构已经开展了不同领域的数据安全风险监测工作，但仍有改进空间，特别是在数据流动监测、外包和第三方合作监测等方面。

在数据安全风险监测方面，金融机构还普遍面临着重视度不足、组织与职责认识不足、资源配置不足以及缺乏统一标准和流程等方面的问题和挑战：

一、对数据安全风险监测的重视度不足。金融机构可能过于侧重于数据安全事件的预防，而忽视了监测和检测的重要性，可能导致无法及时验证阻止措施的有效性或发现新的安全威胁。

二、对数据安全风险监测的组织与职责认识不足。数据安全风险监测不应仅被视为科技部门的责任，而是一个需要业务、管理和审计等多个部门共同参与的跨部门任务。缺乏统筹协调和清晰的职责划分可能导致监测工作的碎片化。

三、资源配置不足。人员和资源的有限配置可能导致数据安全管理岗位的工作负担过重，从而影响监测工作的专注度和效率。此外，缺乏足够的技术工具和解决方案也可能限制监测能力。

四、缺乏统一标准和流程：金融机构可能缺少统一的数据安全风险监测标准和流程，这可能导致监测活动的效果和效率参差不齐。此外，缺乏有效的风险评估和响应机制可能导致对安全事件的响应不够及时。

为了应对这些挑战，金融机构需要提升对数据安全风险监测的重视，明确监测的组织架构与职责，增加资源配置，并制定统一的标准和流程。具体措施包括：

一、提升对数据安全风险监测的重视：金融机构需认识到，仅依靠技术手段和管理措施进行数据安全防护是不够的，还应建立一个全面的监测体系，以验证防护措施的有效性，并及时发现、报告潜在的安全

威胁。将数据安全风险监测作为数据安全治理的核心组成部分，确保有足够的资源和注意力投入到监测活动中。

二、明确数据安全风险监测的组织架构与职责：金融机构应认识到数据安全是全机构的责任，而不仅仅是科技部门的事务。需要构建一个跨部门的协作机制，确保业务、管理和审计等部门都能在数据安全风险监测中发挥作用。此外，应设立一个统筹协调部门，负责资源的集中调配和监测工作的统一规划，以打破数据安全风险监测的孤岛效应，并在组织架构中明确职责划分和流程定义。

三、增加资源配置以强化数据安全风险监测：增加数据安全风险监测的人力和技术支持，减少兼职现象，确保监测工作的专业性和效率。

数据安全管理岗位应专注于监控和检查管控措施的执行情况，而非同时承担前台管控工作，如处理数据防泄漏系统的报警等。

四、制定统一标准和流程：金融机构需要将数据安全风险纳入全面风险管理体系，建立数据安全风险监测和告警机制，加强数据安全风险情报监测、核查、处置与行业共享，制定数据安全事件定级判定标准和应急预案，规范应急演练、事件处置、风险评估和审计等工作。

具体来说，在风险监测方面，金融机构可参照监管文件中明确的监测内容，完善监测指标和告警规则，强化对数据安全风险和事件的发现能力。在数据安全事件管理方面，尤其强调时效性与各方协同，做好信息上报，确保信息透明；加强对风险扩散的阻断能力，多方协同，控制和减缓数据安全事件影响。每年开展全面的数据安全风险评估和针对特定场景的专项评估，如涉及敏感数据处理业务流程发生重大变化、将数据对外提供或跨境提供时，均应对其处理合理性和影响性进行评估，并制定相应的控制措施。定期进行数据安全审计，包括三年一次的全面审计和针对重大数据安全事件的专项审计，以确保持续改进和合规性。

通过这些措施，金融机构可以构建一个更加健全的数据安全风险管理框架，有效预防、识别、评估和应对数据安全风险，保障业务的稳定性和合规性。

第七章　数据安全技术保护

第二十一节　多元异构环境下的数据安全技术保护体系

第 14 题　贵公司是否建立了针对大数据、云计算、移动互联网、物联网等多元异构环境下的数据安全技术保护体系？ [单选题]

选项	小计	比例
已建立	19	43.18%
未建立	25	56.82%
本题有效填写人次	44	

根据调研情况，在大数据、云计算、移动互联网、物联网等多元异构的技术环境下，仅有约 43%的金融机构建立了数据安全技术保护体系。这一发现揭示了金融机构在数据安全技术保护体系建设方面存在的明显短板，现状远未达到预期的安全标准，这不仅增加了数据泄露和滥用的风险，也可能导致金融机构面临合规性和信誉方面的挑战。

在大数据、云计算、移动互联网和物联网等多元异构环境下，数据安全技术保护体系需要综合考虑多个方面的技术和策略。

大数据环境下的数据安全技术：

- 数据生命周期管理：包括采集、存储、处理、交换和销毁各阶段的安全框架与防护技术。
- 密码技术和网络安全协议：如身份认证、访问控制和数据加密技术，确保数据在传输和存储过程中的安全性。
- 平台安全机制：例如 Hadoop 平台的安全机制，以及基于大数据分析和威胁情报共享的协同安全防护体系。

云计算环境下的数据安全技术：

- 云身份认证和访问控制：确保只有授权用户可以访问云资源。
- 虚拟化安全技术：包括虚拟机逃逸防护、固件防篡改和端到端加密等措施，以降低虚拟机逃逸风险。
- 全链路加密：从云原生安全体系出发，对数据进行全链路加密，以保障数据在存储、传输和处理过程中的安全。
- 数据安全审计和隐私保护：通过完整性审计、密文数据去重、可靠数据删除以及高效密文检索等方法来增强云存储的安全性。

移动互联网环境下的数据安全技术：

- 移动应用的数据安全管理：包括数据安全管理要求和技术防范能力的全面梳理，以应对移动应用

在数据安全全周期面临的问题和挑战。

- 移动通信技术标准：需采取多路传输以缓解网络压力并抵御拒绝服务攻击，并采用加密机制确保传输层的安全。

物联网环境下的数据安全技术：

- 设备和数据的加密保护：利用 AES、RSA 等加密算法保护物联网设备间的数据传输和存储，防止数据被窃取或篡改。
- 端云协同防御体系：在云端对终端的安全状态进行感知、监测和升级，同时采取相应的安全防护措施。
- 物联网平台保护技术：包括 WAF（Web 应用防火墙）、防火墙、HIDS（主机入侵检测系统）等手段抵抗恶意攻击，并满足各国对于物联网数据隐私的相关要求。

第二十二节　同步规划、同步建设、同步使用

第 15 题　贵公司是否实现了数据安全保护措施与信息系统的同步规划、同步建设、同步使用？ [单选题]

选项	小计	比例
已实现	35	79.55%
未实现	9	20.45%
本题有效填写人次	44	

数据安全保护措施与信息系统的同步规划、同步建设、同步使用，通常被称为“三同步”原则，是确保信息系统在设计、开发和部署过程中，数据安全得到充分考虑和实施的一种方法。具体来说，它包含以下几个方面：

一、同步规划：在信息系统规划阶段，数据安全保护措施需要被纳入整体规划之中。在设计信息系统架构和功能时，必须同时考虑数据的安全性，包括数据的加密、访问控制、数据备份和恢复计划等。

二、同步建设：在信息系统的建设或开发阶段，数据安全保护措施需要与系统功能同步开发。包括实现数据加密技术、访问控制机制、安全审计和监控系统等，确保这些安全功能与业务功能同时构建并集成

到系统中。

三、同步使用：当信息系统投入运行时，数据安全保护措施也需要同步投入使用。这意味着在系统上线的同时，所有的数据安全措施都应该是激活状态，以保护数据在实际使用中不被未授权访问或泄露。

“三同步”原则的目的是确保数据安全不是事后考虑的事项，而是从信息系统开发的最开始就融入其中，贯穿整个生命周期。这样可以减少安全漏洞的风险，提高系统的安全性和可靠性，避免后期补救措施带来的额外成本和时间延误。

实施“三同步”原则有助于构建一个更加安全、可靠的信息系统环境，保护敏感数据不被泄露、滥用或遭受未授权访问，对于维护公司声誉、客户信任和业务连续性至关重要。在确保数据安全的前提下，金融机构可以更自信地推出新服务和产品，促进业务创新和增长。

调研结果显示，参与调研的金融机构中近 80%已经实现了数据安全保护措施与信息系统的同步规划、同步建设、同步使用，反映出这些机构对于数据安全保护的重视程度较高，他们认识到数据安全对于业务运营的重要性。另有约 20%的机构尚未实现数据安全保护措施与信息系统的同步，需要考虑将数据安全保护措施纳入信息系统的开发生命周期中。

金融机构在进行数据安全保护措施与信息系统的同步规划、同步建设、同步使用时，可能会遇到的难点包括：

一、技术复杂性：随着技术的发展，金融机构需要不断更新其安全技术和策略，以应对日益复杂的安全威胁。

二、资源分配：数据安全保护需要投入大量的人力、财力和时间资源，如何在有限的资源下实现有效的安全保护是一个挑战。

三、跨部门协作：数据安全保护措施的实施需要 IT、业务、合规等多个部门的协作，协调这些部门的工作可能会遇到困难。

四、遗留系统问题：许多金融机构有老旧的遗留系统，这些系统可能难以集成新的安全技术和措施。

五、第三方风险管理：金融机构常常依赖第三方服务提供商，管理这些第三方的安全性和合规性是一个挑战。

六、数据分类分级和访问控制：对数据进行准确分类分级并实施相应的访问控制策略是一项复杂的任务，需要精确的策略和高效的执行。

七、安全与便利性的平衡：在保护数据安全的同时，金融机构还需要确保服务的便利性和用户体验，这两者之间需要找到合适的平衡点。

为克服这些难点，做到数据安全保护措施与信息系统的同步规划、同步建设、同步使用，金融机构可

以采取以下步骤：

一、确立安全策略：制定全面的安全策略，确保所有信息系统的开发和使用都遵循数据保护的最佳实践。

二、风险评估：定期进行风险评估，识别潜在的安全威胁和漏洞，以便在规划阶段就加以考虑。

三、集成安全设计：在系统设计阶段，将安全措施作为核心组件，如数据加密、访问控制和安全审计功能。

四、安全编码实践：培训开发人员采用安全编码实践，减少软件中的安全漏洞。

五、资源优化：合理分配资源，确保有足够的人力和财力支持数据安全保护措施的实施。

六、跨部门协作：建立跨部门沟通机制，促进 IT、业务和合规等部门之间的协作，确保不同部门在数据安全保护方面的信息共享和任务协调。

七、更新遗留系统：对遗留系统进行逐步升级或替换，同时在过渡期间实施补充安全措施，如网络隔离和加强监控。

八、管理第三方风险：制定严格的第三方安全评估和审查流程，确保第三方服务提供商符合金融机构的安全标准，并建立持续的监控机制。

九、平衡安全与便利性：设计易于使用的安全措施，以确保用户在享受便利服务的同时，数据也得到保护。

十、持续监控和改进：实施持续的安全监控，快速响应新出现的威胁，并根据反馈不断改进安全措施。

通过实施数据安全保护措施与信息系统的同步规划、同步建设、同步使用，金融机构不仅能够保护客户和自身的利益，还能够在竞争激烈的市场中保持领先地位。

第二十三节　将数据纳入网络安全等级保护

第 16 题　贵公司是否将数据纳入网络安全等级保护？ [单选题]

选项	小计	比例
已纳入	36	81.82%
未纳入	7	15.91%
不适用	1	2.27%

本题有效填写人次	44	

“将数据纳入网络安全等级保护”是指根据国家相关法律法规和标准，对各类数据进行分类分级，并在此基础上划分网络逻辑安全域，建立分区域的数据安全保护基线，实施有效的安全控制措施。这一过程旨在确保不同级别的数据在存储、传输和处理过程中得到相应的保护，特别是对于存放或者传输敏感级及以上数据的机房和网络，需要实施重点防护。

《网络数据安全管理条例》（征求意见稿）中明确指出国家建立数据分类分级保护制度，并要求数据处理者根据网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等的安全防护。具体来说，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关规定从严保护。《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）中提到保存 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。《银行保险机构数据安全管理办法（征求意见稿）》也要求银行保险机构应当将数据纳入网络安全等级保护，根据数据安全级别，划分网络逻辑安全域，建立分区域数据安全保护基线，实施有效的安全控制。

调研结果显示，被调研的金融机构中约有 82%的机构已经将数据纳入了网络安全等级保护，说明网络安全等级保护已经被广泛接受和实施，成为一种行业标准或最佳实践。约 16%的金融机构表示未将数据纳入网络安全等级保护，意味着这些公司可能还没有意识到数据安全的重要性，或者由于资源、技术等限制尚未实施相应的保护措施。也有少部分公司由于业务特性或数据类型使得将数据纳入网络安全等级保护不适用或暂时没有必要。

金融机构作为数据处理和存储的重要实体，在将数据纳入网络安全等级保护时，可采取以下步骤和策略：

一、划分数据安全级别：根据数据的重要性和敏感程度，将其分为不同的安全等级，具体数据分类分级的方法可参照行业相关标准要求，如《证券期货业数据分类分级指引》《金融数据安全 数据安全分级指南》《银行保险机构数据安全管理办法（征求意见稿）》等。

二、映射数据等级到网络安全等级：将数据分级的结果与网络安全等级保护的要求相匹配。例如将处理重要数据的系统纳入三级以上网络安全等级保护、大数据的安全保护等级应不低于第三级，并参考《金融行业网络安全等级保护实施指引》（JRT 0071-2020）针对不同安全级别的保护能力中对于数据完整性、数据保密性、数据备份恢复、个人信息保护等方面的要求，对不同安全等级的信息系统制定相应的数据安全措施。

三、网络安全域划分：根据数据等级，将网络划分为不同的逻辑或物理安全域，以实现数据的隔离和

访问控制。每个安全域内部又可以进一步划分为多个子域，以确保不同级别的数据在各自的区域内受到相应的保护

四、建立分区域数据安全保护基线：在划分好网络逻辑安全域后，金融机构需要为每个安全域建立相应的数据安全保护基线。包括制定并实施内容过滤、访问控制和安全监控等措施，以确保各安全域内的数据能够得到充分的保护。

五、实施有效的安全控制：根据数据等级和用户角色，实施相应的安全控制措施，如数据加密、访问控制、入侵检测、安全审计等。对于存储或处理高等级数据的区域，实施物理安全措施，如访问控制、监控摄像头等。

通过将数据纳入网络安全等级保护，金融机构能够更好地管理和降低数据安全风险，保护关键信息资产不受威胁。

第二十四节　数据安全保护基线

第 17 题　　贵公司是否建立了数据安全保护基线？[多选题]

选项	小计	比例
将敏感级及以上数据纳入信息系统保护	31	70.45%
制定用户对数据的访问策略	38	86.36%
敏感级及以上数据传输采用安全的传输方式	36	81.82%
敏感级及以上数据采取安全存储措施	35	79.55%
敏感级及以上数据达到使用或者保存期限后，采取技术措施及时删除或者销毁	25	56.82%
以上都没有	3	6.82%
本题有效填写人次	44	

数据安全保护基线是组织在数据安全方面制定的最低标准或要求，通常包括一系列政策、程序和技术措施，旨在保护组织的数据不受未授权访问、泄露、篡改或丢失。数据安全保护基线是组织数据安全保护策略的基础，有助于指导和规范组织内的数据安全管理活动。

金融机构建立数据安全保护基线出于多方面的考虑：

一、合规性要求：数据安全相关的法律法规要求金融机构必须保护客户数据和敏感信息，建立数据安全保护基线有助于满足这些合规性要求。例如，在《银行保险机构数据安全管理办法（征求意见稿）》中提出了根据数据安全级别划分网络逻辑安全域，建立分区域数据安全保护基线的要求。

二、风险管理：金融机构处理大量敏感数据，包括个人身份信息、交易信息、财务信息等，这些数据的泄露或滥用可能导致重大的法律后果和声誉损失。

三、客户信任：保护客户数据安全是建立和维护客户信任的关键。客户更倾向于选择那些能够提供安全数据保护的金融机构。

四、业务连续性：数据安全保护基线有助于确保金融机构在面对数据安全事件时能够快速响应，减少业务中断，保障业务连续性。

五、技术进步：随着技术的发展，数据安全威胁也在不断演变。建立基线可以帮助金融机构及时更新安全措施，应对新的安全挑战。

数据安全保护基线通常包括以下几个关键方面：

一、信息系统保护：将敏感级及以上数据纳入信息系统保护。

二、数据访问控制：制定用户对数据的访问策略，严格实施对敏感级及以上数据的管理。

三、数据传输保护：敏感级及以上数据传输应当采用安全的传输方式。

四、数据存储保护：对敏感级及以上数据采取安全存储措施。定期备份数据，确保在数据丢失或损坏时能够恢复。

五、数据销毁保护：对不再需要的数据进行安全销毁，防止数据泄露。

调研结果揭示了金融机构在数据安全保护基线建设上的进展与挑战：约 70%的机构将敏感数据纳入信息系统保护，显示出对数据保护重要性的认识；在数据删除和销毁方面的措施仅有 56%的机构得以实施，体现了数据生命周期安全管理的不足。80%左右的机构已制定了数据访问、安全传输和安全存储策略，说明大多数公司在控制数据访问、传输和存储方面做得比较好，有助于防止未授权访问和数据泄露。然而，仍有近 7%的机构未制定任何数据安全保护策略，暴露出明显的数据安全风险。

虽然大多数公司在数据安全保护方面采取了一定的措施，但仍有改进空间。特别是在将敏感数据纳入信息系统保护、数据销毁等方面，需要更多的关注和改进，对于那些没有采取任何措施的机构，需要立即开始制定和实施数据安全保护基线，以降低潜在的风险。

数据安全保护基线是保障数据安全的重要手段，金融机构在建立数据安全保护基线时可以参考以下几

个关键步骤：

一、遵循法律法规：金融机构需要遵守数据安全相关的法律法规和行业监管要求，如《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等。

二、评估现有状况：金融机构需要对现有的数据安全状况进行全面评估，包括数据分类分级、数据生命周期各个环节的安全管控措施。

三、建立治理体系：建立一个多层级的治理架构，涵盖董事会、高管层以及相关部门，并明确各自的数据安全责任。

四、数据分类和分级：对数据进行分类和分级，根据数据的敏感性和重要性，确定不同的保护级别和相应的安全措施。

五、制定数据安全策略：制定全面的数据安全策略和制度，包括数据的收集、存储、使用、加工、传输、提供和公开等方面的安全管理。

六、技术保护措施：建立数据安全技术保护体系，包括数据访问控制、数据传输和存储的加密、数据备份与恢复机制以及数据销毁管理等。其中数据存储期限、加密方式、销毁策略应遵循法律法规规定、监管机构的有关要求。

七、持续改进：随着技术进步和业务需求的演进，金融机构应持续评估并优化其数据安全保护基线。通过实施计划－执行－检查－行动（PDCA）循环，机构能够系统地识别改进点，实施解决方案，并不断迭代其数据安全管理策略。在每个 PDCA 循环中，积极查找潜在问题，迅速采取行动进行修正，并记录改进措施以供未来参考。

八、定期安全检查：金融机构应定期对数据安全保护基线的制定和执行情况进行彻底的审查，包括确保所有安全措施不仅遵循最新的法律法规和行业最佳实践，而且确实达到了基线设定的标准。审查过程中，应评估安全措施的有效性，识别合规性差距，并采取必要的纠正措施，以确保数据安全基线得到严格执行和维护。

通过这些优化措施，金融机构能够确保其数据安全保护基线始终保持最新状态，同时满足监管要求并适应不断变化的业务环境。

第二十五节　数据安全技术基础设施

第 18 题　　贵公司是否开展了数据安全的技术基础设施建设？ [多选题]

选项	小计	比例
用户身份管理	39	88.64%
数据匿名化	17	38.64%
行为监测	30	68.18%
日志审计	41	93.18%
数据虚拟化	7	15.91%
以上都没有	2	4.55%
本题有效填写人次	44	

数据安全技术基础设施是指一系列技术和工具的集合，它们共同工作以保护组织内的数据资产免受未授权访问、泄露、篡改或其他安全威胁。这些技术和工具通常包括但不限于：

一、用户身份管理：确保只有授权用户才能访问系统和数据，包括身份验证和访问控制机制。

二、数据匿名化：对敏感数据进行处理，以去除或替换可识别个人身份的信息，以保护隐私。

三、行为监测：监控用户和系统的行为，以便检测和响应可疑或恶意活动。

四、日志审计：记录和分析系统活动日志，用于安全监控和事后分析。

五、数据虚拟化：创建数据的虚拟表示，以便更安全、更灵活地访问和管理数据。

金融机构建设数据安全技术基础设施是为了确保其在快速变化的网络环境中能够有效地保护客户数据和机构资产，同时满足严格的法律法规要求，增强客户信任，降低运营风险，并支持业务的持续创新和发展。通过实施先进的身份管理、数据匿名化、行为监测、日志审计和数据虚拟化等技术措施，金融机构能够实现对敏感信息的全面保护，确保业务操作的安全性和数据管理的一致性，从而在竞争激烈的市场中保持其业务的稳健和信誉。

调研结果揭示了金融机构在数据安全技术基础设施建设上的不同进展。参与调研的金融机构中约有89%的机构已经实施了用户身份管理措施，这反映出业界普遍认识到了强化用户身份验证和访问控制的重要性。此外，高达 93%的机构已经建立了日志审计机制，这一环节对于追踪系统内发生的事件、进行事后分析以及满足合规性要求至关重要。

尽管如此，调研也显示出一些领域尚有提升空间。仅有 68%的机构开展了行为监测，而这项措施对于预防和检测潜在的不当行为或安全威胁至关重要。数据匿名化和数据虚拟化技术的采用率相对较低，分别只有约 39%和 16%的机构实施，这可能与这些技术需要特定的技术环境或业务需求有关。

令人关注的是，有约 4.5%的机构表示尚未建立任何上述数据安全技术基础设施，暗示这些公司可能

面临较高的数据安全风险。

总体来看，尽管参与调研的金融机构在数据安全技术基础设施建设方面取得了一定的进展，特别是在日志审计和用户身份管理方面，但仍需在行为监测、数据匿名化和数据虚拟化等关键领域加大投入和推广力度，以确保数据安全无虞。

金融机构在构建数据安全技术基础设施的过程中面临诸多挑战，包括在众多解决方案中进行正确的技术选型、防范日益复杂的数据泄露风险、适应不断演变的数据保护法规、应对技术更新换代的快速节奏以及克服预算限制。同时，专业人才短缺、内部对变化的抵抗、跨部门协作的困难、员工安全意识的提升以及高级持续性威胁的防范，都是金融机构需要重点关注的问题。此外，全球化运营的金融机构还需应对不同国家和地区法规的合规性挑战，以及第三方服务提供商带来的依赖风险。解决这些问题要求金融机构采取全面策略，包括投资先进技术、培养专业人才、加强内部教育、增强员工安全意识、建立灵活的治理结构，并在全球化背景下进行有效的合规性管理。

金融机构构建数据安全技术基础设施是一项全面而系统的工程。鉴于多数机构已在用户身份管理和日志审计方面取得进展，对于尚未采纳数据匿名化与数据虚拟化技术的机构，以下是一些建议和解决方案：

一、评估需求与风险：首先，公司需要评估自身对数据匿名化和数据虚拟化的需求，分析可能面临的数据泄露风险和合规性要求。

二、技术研究与培训：对数据匿名化和数据虚拟化技术进行深入研究，为技术人员提供相关培训，以便他们能够理解并有效实施这些技术。

三、制定实施计划：制定详细的实施计划，包括技术选型、资源分配、时间表和预算等。

四、引入专家和顾问：考虑引入外部专家或顾问，利用他们的专业知识和经验来指导数据匿名化和数据虚拟化项目的实施。

五、试点项目实施：在小范围内启动试点项目，测试数据匿名化和数据虚拟化技术的有效性和适用性，然后根据试点结果进行调整和优化。

六、逐步推广：在确认试点项目成功后，逐步扩大数据匿名化和数据虚拟化技术的实施范围。

七、建立跨部门协作：促进 IT、法务、业务等部门之间的协作，确保数据安全措施与业务需求和合规要求相一致。

八、持续监控与评估：实施后，建立持续的监控和评估机制，确保数据匿名化和数据虚拟化措施的有效性，并根据技术发展和业务变化进行调整。

九、强化数据访问控制：即便实施了数据匿名化，也要确保对敏感数据的访问进行严格控制，防止未经授权的访问。

遵循这些步骤，有助于金融机构稳健地构建起强大的数据安全技术基础设施，不仅提升数据保护水平，

也满足日益严格的监管标准和业务需求。

第二十六节　大数据平台安全

第 19 题　　贵公司是否采取措施保障了大数据平台安全？[多选题]

选项	小计	比例
高可用设计	37	84.09%
安全加固	28	63.64%
数据备份	37	84.09%
大数据服务访问授权机制	35	79.55%
动态监测与审计大数据访问行为	22	50%
以上都没有	2	4.55%
不适用	3	6.82%
本题有效填写人次	44	

大数据平台，是指以处理海量数据存储、计算、分析等为目的的基础设施，包括数据统计分析类的平台和大数据处理类平台（如数据湖、数据仓库等）。大数据平台的安全是保障数据在整个生命周期中安全的关键。

根据调研结果，目前约 90%的金融机构采取了不同的技术手段来保障其大数据平台的安全性。在这些措施中，实现系统的高可用性和数据备份是主要手段，均占到了 84%。为了满足信息安全中的机密性和完整性要求，金融机构主要通过安全加固和访问控制手段来提供保障。然而，在技术措施方面，仍存在一定的不足。

金融机构的大数据平台普遍具有数据量巨大、数据类型多元，以及响应时效要求高的特点，其在金融场景的应用主要集中在以下几个方面：

一、风险管理：金融机构可以利用大数据平台对客户数据、交易数据等进行分析，以识别风险，提高

风险管理能力。

二、市场分析：金融机构可以利用大数据平台对市场数据进行分析，以了解市场趋势和变化，提高投资决策的准确性。

三、客户关系管理：金融机构可以利用大数据平台对客户数据进行分析，以了解客户需求和行为，提高客户满意度和忠诚度。

四、反欺诈：金融机构可以利用大数据平台对客户数据、交易数据等进行分析，以识别欺诈行为，提高反欺诈能力。

五、合规管理：金融机构可以利用大数据平台对合规数据进行分析，以了解合规风险，提高合规管理能力。

目前，金融机构传统业务系统在数据安全风险主要集中于未经授权访问、业务逻辑漏洞、单点故障，数据共享接口等风险。目前金融机构主流使用的大数据平台应用技术为 Hadoop、Spark、Kafka、HBase、Flink、Storm、MongoDB 等，其数据安全风险除需关注常规业务系统的数据安全风险外，还存在以下新的风险：

一、海量数据处理：大数据平台通常处理海量数据，数据规模巨大，使得数据的分类、标记和管理变得复杂，容易出现数据遗漏或错误分类，导致敏感数据暴露。例如，大量的客户交易数据如果没有准确分类和保护，可能被误用于不当用途

二、数据融合风险：大数据平台可能整合来自多个业务系统的数据，不同来源的数据安全级别和保护要求可能不同，融合过程中容易出现安全漏洞。比如，将低安全级别的数据与高安全级别的数据混合处理，可能降低整体数据安全性

三、新技术应用风险：大数据平台常采用新的技术架构和算法，如分布式存储、云计算等，这些新技术可能存在未知的安全漏洞。例如，使用的某个云服务提供商存在安全漏洞，导致数据泄露。

为应对上述新的风险，我们建议从以下几方面加强大数据平台安全技术保障：

一、建立完善的数据分类和标记体系。制定明确的数据分类标准和标记规则，确保数据能够被准确分类和标记。可利用数据治理和数据管理的自动化工具，如数据血缘分析工具以及数据分类和标记引擎辅助进行数据的分类、标记和管理，减少人工操作带来的错误。

二、建立数据风险评估与监控机制。实时监控数据安全风险，包括数据的机密性、完整性和可用性，及时发现问题并解决。可通过人工智能和机器学习算法检测异常数据访问模式和潜在的数据安全威胁。同时，可引入专业第三方评估，定期对大数据平台的数据安全管理现状进行风险评估和专项审计，及时发现风险问题并解决。

三、加强数据隔离安全与权限管理。在物理或逻辑上对不同安全级别的数据进行隔离存储和处理，建立严格的访问控制机制，确保只有授权人员能够访问特定安全级别的数据。通过对数据仓库和数据湖合理的架构设计和数据存储方式，优化对不同安全级别数据隔离与访问控制。必要时可通过数据脱敏与加密技术，对敏感分级数据进行脱敏、加密存储和传输，在不影响数据使用的前提下确保数据融合下高安全级别数据的保密性。

四、基于角色配置细粒度的数据访问控制安全策略，确保只有经过授权的用户才能访问特定的数据，从而有效防止不同敏感等级的数据融合而造成数据泄露和滥用。如通过 Kerberos、OAuth 等身份验证机制，确保用户身份的真实性；通过访问控制列表（ACL）和基于角色的访问控制（RBAC）来定义用户和组对资源的访问权限。控制不同服务之间的访问和交互权限。记录系统中的各种操作和事件，以便进行安全审计和追踪。

在引入大数据平台的新技术之前，金融机构应进行全面的风险评估，包括分析新技术是否符合金融行业的相关法规和监管要求、可能引入的安全漏洞，以及数据隐私风险，并制定相应的应对策略。在新技术上线前，应进行严格的安全测试，包括漏洞扫描和渗透测试，以确保技术在投入使用前满足既定的安全标准。

应用新技术的过程中，应建立实时监控系统，对大数据平台的运行状态和数据访问进行监控，以便及时发现并预警异常情况。同时，与技术供应商建立紧密的合作关系，确保能够及时获取安全补丁和技术支持。

此外，金融机构应加强对技术人员和业务人员的培训，提高他们对新技术特点的理解，以及对可能存在风险的认识，从而提升整体的安全意识和应急处理能力。制定完善的应急预案，定期进行数据备份，并测试数据恢复流程，以准备应对可能的安全事件。

第二十七节　人工智能安全管理

第 20 题　　贵公司是否建立了人工智能管理机制？[多选题]

选项	小计	比例
对人工智能模型开发应用进行统一管理	16	36.36%
建立模型算法产品外部引入的准入机制	10	22.73%
对模型研发过程进行主动管理，实现模型算法可验	15	34.09%

证、可审核、可追溯		
模型算法投入使用时，开展数据安全审查	12	27.27%
使用人工智能技术开展业务时就数据对决策结果影响进行解释说明和信息披露	9	20.45%
实时监测自动化处理与系统运行结果	7	15.91%
建立人工智能应用的风险缓释措施	7	15.91%
以上都没有	15	34.09%
不适用	9	20.45%
本题有效填写人次	44	

随着人工智能技术的快速发展和广泛应用，金融机构正逐步将 AI 技术融入其业务流程中，以提高效率、优化决策。然而，人工智能的安全管理已成为监管部门和金融机构共同关注的焦点。目前，金融机构在人工智能方面的应用领域主要有：

一、客户服务：利用 AI 模型结合客户服务具体会话状态与金融服务场景，代替人工作业，实时定制回复话术，节约时间成本。

二、客户营销：利用 AI 模型进行语义分析和线索挖掘帮助提升潜在客户线索识别与转化。

三、个性化投资策略：利用 AI 模型，收集大量的宏观经济、金融市场、风险偏好等数据进行训练，为客户生成投资策略建议。

四、智能办公：基于大模型的 AI 应用工具，大幅提高员工办公效率。

五、辅助研发：辅助需求分析、UI 设计、代码生成、系统测试等研发全流程，促进端到端研发效率提升。

监管部门对人工智能的安全要求主要集中在数据处理透明度、模型的公平合理性、可验证性、可审核性和可追溯性等方面。具体要求包括：

一、对人工智能模型开发应用进行统一管理。

二、建立模型算法产品外部引入的准入机制。

三、对模型研发过程进行主动管理。

四、在模型算法投入使用时开展数据安全审查。

五、使用人工智能技术开展业务时进行数据对决策结果影响的解释说明和信息披露。

六、实时监测自动化处理与系统运行结果。

七、建立人工智能应用的风险缓释措施。

调研结果显示，金融机构在人工智能安全管理的实施上存在不足：

- 仅有 36%的机构对人工智能模型开发应用进行了统一管理。
- 23%的机构建立了模型算法产品外部引入的准入机制。
- 34%的机构实现了对模型研发过程的主动管理。
- 27%的机构在模型投入使用时开展了数据安全审查。
- 20%的机构在使用人工智能技术时提供了数据影响的解释说明和信息披露。
- 实时监测自动化处理与系统运行结果的机构占比仅为 16%。
- 风险缓释措施的建立同样只有 16%的机构满足。

金融机构在人工智能安全管理方面面临的挑战主要包括：

一、技术复杂性：人工智能技术的复杂性给统一管理和审查带来了难度。缺少专业性模型安全认证体系与独立审计，安全性能验证成本高。

二、人才短缺：缺乏足够的专业人才来支持复杂的 AI 安全管理体系。

三、监管适应性：随着技术的发展，现有监管要求可能需要更新以适应新情况。利用 AI 大模型处理数据时，获取合法的用户授权，确保数据的收集、使用和存储均符合法律要求

四、风险识别与管理：实时监测和风险缓释措施的缺乏增加了安全威胁的风险。难以从供应商处获取模型架构、训练算法和数据使用的详细说明，无法充分理解模型内在逻辑，可能存在理解偏差来源。

五、供应商合作：审慎评估 AI 供应商安全策略和技术方案，避免潜在风险传染

六、为了提高金融机构的人工智能安全管理水平，建议采取以下措施：

七、加强顶层设计：制定全面的数据安全战略，与业务战略紧密结合，确保人工智能应用的安全性。

八、提升技术能力：投资于人工智能安全技术的研发和部署，提高数据处理和模型监控的能力。

九、人才培养与引进：加强数据科学家和安全专家的培养与引进，建立跨学科团队。

十、合规性监控：建立持续的合规性监控机制，确保人工智能应用符合监管要求。

十一、风险管理：建立动态的风险评估和管理机制，及时识别和响应安全威胁。

十二、透明度和问责制：提高人工智能决策过程的透明度，确保决策结果的可解释性和问责制。

十三、应急响应计划：制定和测试人工智能应用的应急预案，提高对安全事件的响应能力。

十四、行业合作与共享：与同行业机构和监管机构建立合作机制，共享安全信息和最佳实践。

十五、安全测试：在人工智能模型投放运行前，对其进行全面安全测试，保证面对常见安全攻击（如

数据注入、恶意软件感染等）时的防护能力和恢复机制。

金融机构在人工智能安全管理方面虽有进展，但与监管要求和最佳实践相比仍有较大差距。通过加强管理、技术投入、人才培养和风险管理，可以提高人工智能应用的安全性和合规性，从而保护客户利益，维护金融系统的稳定。

第二十八节　与外部机构的数据交互

第 21 题　贵公司是否实施了与外部交互数据的安全技术措施？ [多选题]

选项	小计	比例
建设了与外部交互数据的专用平台	23	52.27%
采用了 API 安全的技术措施	25	56.82%
采用了其他安全技术措施	21	47.73%
以上都没有	0	0%
不适用	7	15.91%
本题有效填写人次	44	

《银行保险机构数据安全管理办法（征求意见稿）》第五十三条 （外部交互数据安全） 银行保险机构在建设开放银行、金融生态或者与第三方数据合作时，要实现自身与外部的安全风险隔离，与外部机构的数据交互应当通过集中管理的外联平台或者应用程序接口实施，依据“业务必需、最小权限”原则，采取有效措施对接口设计、开发、服务、运行等进行集中安全保护管理。

金融机构与外部交互数据的场景广泛，涉及多个方面和领域，主要包括：

- 客户数据收集：金融机构在为客户提供服务时，需要收集客户的个人信息、财务状况、交易记录等数据。
- 风险评估与信用评分：金融机构利用外部数据进行风险评估，包括信用评分、欺诈检测等。
- 合规性检查：与监管机构共享数据，确保业务符合法律法规要求，如反洗钱（AML）和客户身份识别（KYC）程序。

- 支付和结算服务：在进行国内和国际支付时，金融机构需要与其他银行或支付网络共享交易数据。
- 信贷服务：在提供贷款和信贷服务时，金融机构会与信用评级机构、征信机构等外部实体交换数据。
- 投资银行业务：在证券发行、并购咨询等业务中，金融机构需要与潜在投资者、目标公司等交换信息。
- 资产管理：金融机构在管理基金、投资组合时，会与外部资产管理公司、顾问公司等交换市场数据和投资策略。
- 保险业务：在承保和理赔过程中，保险公司需要与医疗、汽车维修等第三方服务提供商交换数据。
- 供应链金融：金融机构在提供供应链融资时，需要与供应商、购买方、物流公司等交换交易和物流数据。
- 数字化服务：通过 APIs 和合作伙伴关系，金融机构将服务嵌入到第三方平台和应用程序中，实现数据交换。
- 市场数据服务：金融机构订阅外部市场数据提供商的服务，获取股票、债券、外汇等市场数据。
- 监管报告：定期向监管机构提交业务报告、财务报表和其他监管要求的数据。
- 技术外包：金融机构可能会将部分技术基础设施、软件开发、数据分析等外包给外部技术服务提供商。
- 客户服务和支持：在提供客户服务时，可能会与外部呼叫中心、客户关系管理系统等进行数据交互。
- 研究和分析：金融机构可能会与市场研究机构、经济咨询公司等合作，获取宏观经济数据和行业分析报告。

金融机构与外部交互数据的方式主要包括：

- U 盘复制传输：使用 U 盘等移动存储设备进行数据的物理复制和传输，适用于没有网络连接或需要离线传输的场景。
- 电子邮件传输：通过电子邮件发送数据文件或链接，适用于小到中等规模的数据传输，方便快捷，但安全性较低。
- API 接口传输：通过应用程序编程接口进行数据的实时交互，适用于系统间的集成和自动化数据交换。
- 网络专线传输：通过专用网络连接进行数据传输，提供高安全性和稳定性。
- 云服务传输：使用云存储和云计算服务进行数据的存储、处理和传输。
- 移动设备传输：通过智能手机、平板电脑等移动设备的连接进行数据传输。

- FTP/SFTP 文件传输：使用 FTP 或 SFTP 协议进行文件的上传和下载。
- 数据交换平台：通过数据交换平台实现不同系统间的数据传输和集成。
- 在线表单和数据导入导出：通过在线表单收集数据或使用数据导入导出工具在系统间传输数据。
- 即时通讯工具：使用即时通讯软件或协作平台传输数据。
- 数据同步工具：使用数据同步软件或服务实现不同系统之间的数据实时同步。
- Web 服务：通过 Web 服务进行数据交互，如 SOAP 和 RESTful API。
- 数据湖和数据仓库：在数据湖或数据仓库中存储大量数据，并通过网络进行数据的访问和分析。
- 区块链技术：利用区块链的分布式账本技术进行数据的传输和存储。
- 隐私计算平台：通过隐私计算平台实现数据的安全共享和计算。
- 数据室（Data Room）：在商业活动中，通过安全的在线数据室共享敏感数据。

API 接口的安全传输是确保数据在 API 请求和响应之间的传输过程中不被截获、篡改或泄露的重要步骤。以下是一些用于增强 API 接口安全传输的常见技术和最佳实践：

- 使用 HTTPS 协议：HTTPS（超文本传输安全协议）通过 TLS/SSL 协议对数据进行加密，从而保护数据在传输过程中的机密性和完整性。
- 数据加密：选择合适的加密算法是关键的一步。常用的加密算法包括 AES（高级加密标准）、RSA（Rivest-Shamir-Adleman）和 HMAC（基于哈希的消息认证码）。这些算法可以有效地保护数据的机密性和完整性。
- API 密钥和令牌：使用 API 密钥进行身份验证和授权，可以有效防止未经授权的访问。此外，还可以使用基于令牌的身份验证机制，以确保每次请求都经过验证和授权。
- 输入验证和过滤：对输入数据进行严格的验证和过滤，可以防止 SQL 注入、跨站脚本攻击等常见攻击手段。这包括对所有输入参数进行类型检查和长度限制，并使用白名单而非黑名单来定义可接受的输入值。
- 访问控制和权限管理：实现细粒度的访问控制，确保每个用户或客户端只能访问其有权访问的资源。此外，还应定期评估和更新 API 的风险等级，以应对新的威胁和漏洞。
- 日志记录和监控：详细记录 API 的访问日志，并实施实时监控，以便及时发现和响应异常行为或潜在的安全威胁。这有助于追踪攻击源并采取相应的防护措施。
- 防范拒绝服务攻击（DDoS）：通过实施速率限制和其他防护措施，可以有效防止 DDoS 攻击对 API 造成的影响。

调研数据显示，约有 52%的金融机构已经建立了专用平台以实现与外部的数据交互，57%的机构实施了 API 安全技术措施，另有 48%的机构采取了其他类型的安全技术手段。然而，有近 16%的机构对该项

标记了“不适用”，可能反映出某些金融领域对外部数据交互有严格的限制或特殊规定。

这些统计结果揭示了金融机构在实现监管要求——即与外部机构的数据交互应当通过集中管理的外联平台或者应用程序接口实施——方面还存在差距。为了缩短这一差距，金融机构，特别是银行保险机构，需进一步强化其数据交互的安全管理措施，并优化现有系统，以确保能够有效控制数据安全风险，满足监管标准。这可能包括提升技术防护能力、加强数据治理，以及增强对数据交互活动的监控和审计等方面。

第二十九节　数据安全防护技术或工具

第 24 题　贵公司部署了哪些数据安全防护技术或工具 [多选题]

选项	小计	比例
数据分类分级自动化工具	15	34.09%
数据防泄漏 DLP	38	86.36%
数据库审计	32	72.73%
数据库防火墙（网关）	19	43.18%
API 安全	24	54.55%
数据库加密存储	14	31.82%
文档加密	24	54.55%
数据脱敏	39	88.64%
网间摆渡	26	59.09%
运维人员管理系统	28	63.64%
用户行为分析	19	43.18%
以上都没有	0	0%
本题有效填写人次	44	

调研结果显示，金融机构普遍部署了多种数据安全防护技术与工具，主要包括数据防泄露（DLP）、

数据库脱敏、数据库审计、运维管理、API 接口安全、文件传输安全以及文件加密等。这些技术与工具之所以受到青睐，是因为它们在技术成熟度上较高，产品选择性多样，能够满足多样化的安全需求。

然而，相对而言，数据库加密和用户行为分析等技术与工具的部署受到了业务流程、部署环境的复杂性以及系统兼容性问题等因素的影响，导致其整体覆盖率不高，显示出这些领域仍有较大的发展空间。

从数据生命周期管理的角度来看，金融机构在数据处理的各个阶段都面临着众多安全风险。为了应对这些风险，我们需要综合运用管理手段和技术手段来解决或降低它们的影响。

一、在数据采集阶段：

可能存在的风险有：

1. 数据来源不可靠可能导致采集到错误或虚假的数据，这会影响后续的数据分析和决策，可能造成金融机构投资决策失误、客户信用评估错误，进而导致经济损失。

2. 数据采集方式不合规可能引发法律纠纷，面临监管部门的罚款和声誉损害，导致客户信任度下降和业务量减少。

管理层面建议：

1. 制定明确的数据采集政策和流程，明确数据来源的合法性和可靠性。

2. 对数据采集人员进行培训，增强其合规意识和数据质量意识。

技术层面解决措施：

1. 采用数据验证技术，如格式检查、数据清洗和重复数据检测，确保采集数据的准确性和完整性。可以使用 Apache NiFi、Talend、Trifacta 等工具对不同数据源的数据处理操作

2. 利用 HTTPS、SFTP 等加密传输协议对采集的数据进行加密传输，防止数据在传输过程中被窃取或篡改。

二、在数据存储阶段：

可能存在的风险有：

1. 数据存储设备故障可能导致数据丢失，使金融机构无法正常开展业务，如无法为客户提供准确的账户信息，可能引发客户投诉和赔偿要求。

2. 数据被非法访问或篡改可能导致客户的账户信息被窃取或资金被转移，造成直接的经济损失，同时损害金融机构的声誉，引发客户流失。

管理层面建议：

1. 建立数据存储管理制度，明确数据存储的位置、期限和安全要求。

2. 定期进行数据存储的安全审计，发现和解决潜在的安全隐患。

技术层面解决措施：

1. 采用冗余存储和备份技术，定期进行数据备份，并测试恢复流程，以防止数据丢失。
2. 部署访问控制技术，如身份认证、授权和访问权限管理，限制对数据的非法访问。
3. 运用数据加密技术对存储的数据进行加密，保护数据的机密性。

三、在数据处理阶段：

可能存在的风险有：

1. 数据处理算法错误可能导致数据分析结果不准确，影响金融机构对市场趋势的判断和风险评估，进而导致投资损失和业务决策失误。
2. 数据处理过程中泄露敏感信息可能被竞争对手获取，影响市场竞争优势，或者被不法分子利用进行欺诈活动，给金融机构和客户带来巨大损失。

管理层面建议：

1. 制定数据处理的规范和流程，明确数据处理的目的、方法和责任。
2. 对数据处理人员进行培训，增强其数据安全和合规意识。

技术层面解决措施：

1. 采用 Elasticsearch、Flink、Spark 等较为先进、可靠的数据分析工具和算法，并进行充分的测试和验证，确保处理结果的准确性。
2. 运用数据脱敏技术，对敏感数据进行处理，降低数据泄露风险。而数据脱敏算法较为关键，需要根据不同的需求和场景，确定脱敏数据类型。

四、在数据传输阶段：

可能存在的风险有：

1. 数据在网络传输中被拦截可能导致客户交易信息被窃取，造成客户资金损失，金融机构需要承担赔偿责任。
2. 数据被篡改可能导致交易指令错误，引发金融交易混乱和经济纠纷。

管理层面建议：

1. 制定数据传输的安全策略，明确传输的方式、加密要求和授权流程。
2. 对数据传输进行监控和审计，及时发现异常传输行为。

技术层面解决措施：

1. 采用虚拟专用网络（VPN）等加密传输技术，保障数据传输的安全性。
2. 使用哈希算法（MD5、SHA-1、SHA-256 等）、循环冗余校验（CRC）实施数据传输的完整性校

验，确保数据在传输过程中未被篡改。

五、在数据共享阶段：

可能存在的风险有：

1. 数据共享范围不当可能导致敏感信息扩散，违反法律法规，面临巨额罚款。
2. 共享对象不可信可能导致数据被滥用，如用于非法营销或欺诈活动，损害金融机构和客户的利益。

管理层面建议：

1. 制定严格的数据共享审批流程，明确共享的范围、目的和期限。
2. 与合作方签订数据共享协议，明确双方的权利和义务以及数据安全责任。

技术层面解决措施：

1. 采用数据匿名化和去标识化技术，在共享数据时保护个人隐私。
2. 建立数据共享平台，通过隐私保护技术如全同固态加密、函数加密、差分隐私、安全多方计算等或者数据沙箱方式来实现数据的安全交换和共享。

六、在数据销毁阶段：

可能存在的风险有：

1. 若未彻底销毁数据，残留数据被恢复和利用可能导致客户隐私泄露，引发法律责任和声誉损失。
2. 残留的重要业务数据被竞争对手获取，可能影响金融机构的市场竞争力。

管理层面建议：

1. 制定数据销毁的政策和流程，明确销毁的条件和方式。
2. 记录数据销毁的操作和相关信息，以备审计和追溯。

技术层面解决措施：

1. 使用安全的数据销毁技术和工具，确保数据无法被恢复。

第八章　数据安全认证

第三十节　数据安全认证

目前，数据安全领域的相关认证主要包括 DSMM（数据安全能力成熟度模型）认证、DSM（数据安全

管理）认证以及 ISO 27701（隐私信息管理体系）认证等。DSMM 认证与 DSM 认证是专注于数据安全领域的两个认证标准，它们通常用于评估和增强组织的数据安全管理能力。

一、DSMM 认证

DSMM（Data Security Capability Maturity Model）认证是中国首个依据国家标准《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）开展的数据安全认证。该标准由中国电子技术标准化研究院、国家信息安全工程技术研究中心、中国信息安全测评中心等业内权威机构，联合阿里巴巴共同编写。作为国内首个数据安全标准认证，它于 2019 年 8 月 30 日发布，并自 2020 年 3 月 1 日起正式实施。

DSMM 评估以组织为单位，以数据为中心，依据四个安全能力维度、七个安全过程维度和五个安全能力等级来评价组织的数据安全能力：

- 四个能力维度：包括组织建设、制度流程、技术工具、人员能力。
- 七个安全过程维度：涵盖数据生存周期安全过程，具体包括数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全，以及通用安全，共计 30 个数据安全能力过程域。
- 五个安全能力等级：从低到高依次为 1 至 5 级。

DSMM 认证的推出，旨在通过系统化的评价方法，帮助组织全面提升数据安全管理水平，确保数据全生命周期的安全与合规。在 30 个数据安全能力过程域中，有一些领域需要重点关注，如 PA01 数据分类分级、PA12 数据正当使用、PA20 数据安全策略规划、PA29 需求分析、PA30 安全事件应急等，需要加强在这些领域的建设工作。

二、DSM 认证

2022 年 6 月 9 日，国家市场监督管理总局与国家互联网信息办公室联合发布了《关于开展数据安全管理认证工作的公告》（简称 18 号文）。该公告标志着国家主管部门将加强对数据安全的规范化管理，并启动了统一的认证工作。同时，还发布了《数据安全管理认证实施规则》，明确了对网络运营者在网络数据收集、存储、使用、加工、传输、提供、公开等处理活动中进行认证的基本原则和要求。

数据安全管理认证（DSM）的认证依据是国家标准 GB/T 41479《信息安全技术 网络数据处理安全要求》及相关标准规范。《信息安全技术 网络数据处理安全要求》标准结合了《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》以及《信息安全技术 个人信息安全规范》（GB/T 35273-2020）等法律法规，从数据处理安全的总体要求、技术要求和管理要求三个方面，为网络运营者开展数据处理活动提供了全面的安全要求指导。

认证标准通常反映了当前最佳的安全实践和标准，如果组织未能符合这些标准，可能存在安全漏洞和风险，使其易受攻击和数据泄露的威胁，并可能降低组织在客户和合作伙伴眼中的信任度。

组织可对照以上标准对自身数据安全体系进行差距分析，识别目前的数据安全控制措施与标准要求之间存在的差距，对发现的问题进行风险评估，并制定改进措施，以确保数据安全和合规性，提升组织的竞争力和信任度。

组织按照以上标准规范建立数据安全体系并运行一段时间后，可以向数据安全管理认证的专业机构提出认证申请。认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

获得数据安全认证是金融机构向其他企业展示其对数据安全重视程度的一种方式，同时也是实现持续改进和保持行业竞争力的重要步骤。

获得数据安全认证对金融机构来说具有多重重要意义：

- 增强信任：数据安全认证表明机构遵守了严格的数据保护标准，能够增强客户、合作伙伴及投资者的信任。
- 合规性保证：许多行业和地区都有数据保护法规要求，获得认证有助于确保机构符合这些法律法规的要求。
- 风险管理：通过认证过程，机构能够识别和评估数据安全风险，并采取措施进行有效管理。
- 保护资产：数据是现代企业的重要资产，数据安全认证有助于保护这些资产免受未授权访问、泄露和其他安全威胁。
- 提升品牌形象：展示对数据安全的承诺和实践能够提升机构的品牌形象和市场竞争力。
- 内部管理优化：认证过程通常涉及对内部流程和政策的审查，有助于优化数据管理实践。
- 应对保险要求：某些保险政策可能要求企业持有数据安全认证，以降低保险风险和成本。
- 技术进步的适应：随着技术的不断进步，数据安全认证可以帮助机构适应新的安全挑战和最佳实践。
- 客户和市场要求：客户和市场越来越重视数据安全，认证成为满足这些要求的一种证明。
- 防范法律诉讼：在数据泄露或其他安全事件发生时，数据安全认证可以作为机构已经采取合理预防措施的证据。
- 员工培训和意识：认证过程通常包括员工培训，有助于提高员工对数据安全的认识和责任感。

调研结果显示，在参与调研的金融机构中：

- 9%的机构获得了 DSMM（数据安全能力成熟度认证）。
- 4%的机构获得了 DSM（数据安全管理认证）。
- 13%的机构获得了 ISO 27701（隐私信息管理体系）认证。
- 18%的机构获得了其他类型的数据安全认证。
- 而将近 66%的机构尚未获得任何数据安全相关认证。

调研结果表明，金融机构在数据安全认证方面面临诸多挑战：

- 认证意识不足：部分机构对数据安全认证的重要性认识不足。
- 资源投入有限：缺乏足够的人力、财力和技术支持。
- 缺乏专业知识：缺少对数据安全认证标准和流程的深入了解。
- 监管环境变化：法规的不断更新要求机构持续适应新的合规要求。

为提升金融机构的数据安全认证水平，建议采取以下措施：

- 加强认证宣传和教育：提高机构对数据安全认证的认识和重视。
- 制定认证计划：根据机构的实际情况，制定合理的认证获取计划。
- 加大资源投入：在人力、技术和资金上为数据安全认证提供支持。
- 培养专业人才：加强员工对数据安全认证相关知识的培训。
- 建立合作伙伴关系：与专业机构合作，获取认证过程中的专业指导。
- 持续监控和改进：获得认证后，持续监控数据安全状况并进行改进。

第九章　数据安全合规建设典型案例研究

A 某银行数据安全合规评估项目案例（翰纬科技提供）

一、案例背景

随着数字化转型的不断深入，银行业务对信息技术和数据处理的依赖日益增强。数据已成为银行的核心资产，其安全性直接关联到银行的稳定运营和客户信任。面对网络攻击、数据泄露、非法访问等日益增长的数据安全挑战，国家金融监督管理总局发布了《银行保险机构数据安全管理办法（公开征求意见稿）》（以下简称《办法》），旨在规范银行保险机构的数据处理活动，保障数据安全，促进数据合理开发利用，

保护个人和组织的合法权益。

本次数据安全合规评估项目是为响应《办法》的要求，对某银行现有的数据安全管理体系进行全面评估，识别该银行现有体系与《办法》规定之间的差距，并评估潜在的数据安全风险。通过这一过程，为该银行提供一个清晰的数据安全现状，指出需要改进的领域，并提出切实可行的改进建议。

二、解决方案

通过现状调研、差距分析等评估过程，对某银行进行数据安全现状分析，识别与《办法》要求之间的差距，并提出针对性的改进建议，以促进该银行数据安全管理的持续优化和提升。

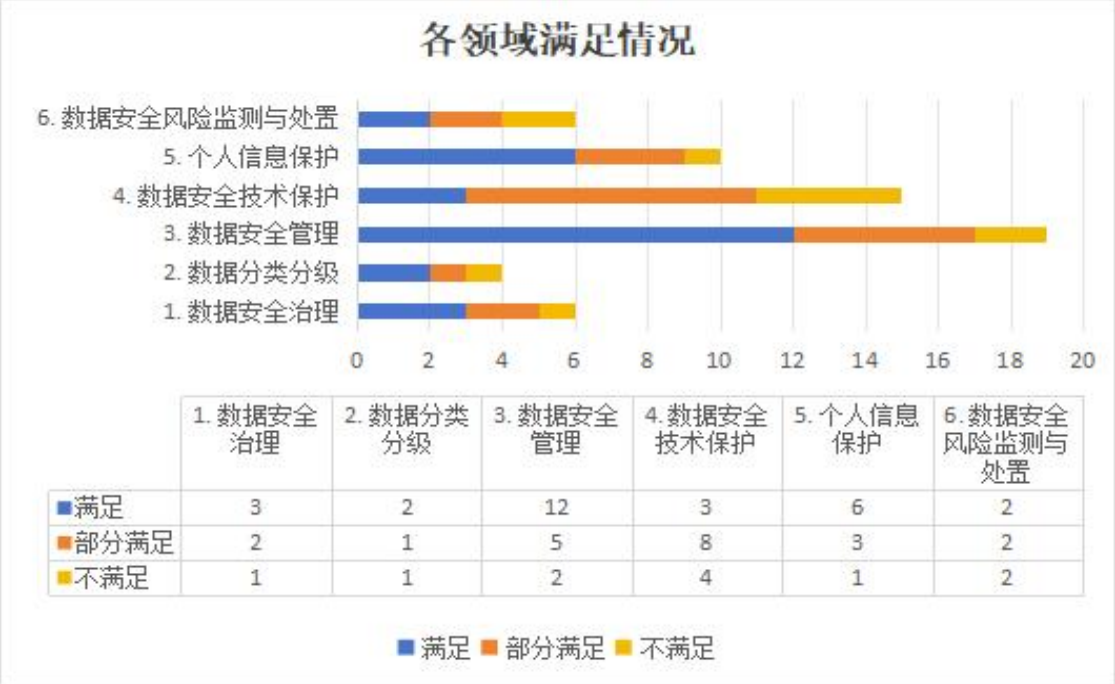
1.现状调研：通过文档查阅、人员访谈、系统和流程分析、技术评估等方式对该银行数据安全现状进行调研，了解现行的数据安全管控措施；

2.差距分析：根据《银行保险机构数据安全管理办法（公开征求意见稿）》，对 61 项要求条款进行拆分解读，逐项对比该银行现有的数据安全管理措施，识别差距和不足。

3.风险评估：对识别的差距和不足进行风险评估，确定其可能对该银行运营和声誉造成的影响以及发生的可能性。

4.制定改进措施：基于差距分析和风险评估的结果，制定针对性的改进措施和建议。

图：数据安全合规评估结果示例



	1. 数据安全治理	2. 数据分类分级	3. 数据安全管理	4. 数据安全技术保护	5. 个人信息保护	6. 数据安全风险监测与处置
满足	3	2	12	3	6	2
部分满足	2	1	5	8	3	2
不满足	1	1	2	4	1	2

图：数据安全合规评估结果示例

评估项	合规结果	评分	合规风险等级
第九条　数据安全治理架构			
第十条　数据安全责任制			
第十一条　数据安全归口管理部门			
第十二条　业务部门			
第十三条　风险合规与审计部门			
第十四条　数据安全技术保护部门			
第十五条　数据安全文化建设			
第十六条　总体要求			
第十七条　数据分类			
第十八条　数据分级			
第十九条　动态调整			
第二十条　管理体系			
第二十一条　数据资产管理			
第二十二条　数据安全评估			
第二十三条　数据服务管理			
第二十四条　数据收集			
第二十五条　数据收集			
第二十六条　外部数据采购			
第二十七条　数据加工			
第二十八条　数据使用			

图：数据安全合规评估结果示例

评估发现的问题主要体现在以下几个方面：

1.数据安全治理架构不完善，未明确数据安全主体责任、数据安全第一责任人、直接责任人以及各层级负责人的责任等内容；

2.数据分类分级标准与《办法》的规定存在不一致，未建立数据分类分级动态调整审批机制；

3.数据安全管理办法覆盖内容不全，制度流程不成体系；

4.未建立起多元异构环境下的数据安全技术保护体系；

5.对人工智能模型开发应用未进行统一管理；

6.未将数据安全纳入全面风险管理体系和内控评价体系，定期开展数据安全评估和审计；

7.未建立体系化的数据安全风险监测机制。

将以上问题及整改方案归纳为三类：

1.已有的管理实践尚未完全体现在正式的制度中，需要将这些实践明确地纳入制度中，以形成一套完整的、书面化的管理制度，如通过优化现有数据安全组织架构，在制度中明确数据安全责任等内容，完善数据安全治理架构，提升“数据安全治理”领域的合规水平。

2.现有管理体系不足导致的问题，需要依据《办法》要求进行体系建设和完善。具体包括优化数据分类分级策略；建立企业级数据服务管理体系；建立多元异构环境下的数据安全技术保护体系；对人工智能模型开发应用进行统一管理；将数据安全纳入全面风险管理体系和内控评价体系，定期开展数据安全风险评估和审计，建立体系化的数据安全风险监测机制等。

3.在对现有的制度流程进行重新设计和优化的基础上，配套技术工具来实现安全管控，如数据分类分级自动化标识、数据安全风险监测和事件处置。

三、案例优势

1.咨询公司对最新的数据安全监管要求进行了深入解读，确保评估项目与当前监管要求保持一致。

2.咨询公司采用经过验证的科学方法论进行合规评估，包括风险评估框架、合规性检查清单等，确保评估的全面性和系统性。

3.咨询公司服务过多个同业客户，在整改方案方面可提供行业较佳实践和创新解决方案，帮助客户在数据安全方面取得竞争优势。

4.咨询公司拥有数据安全方面的专家，能够评估和推荐最新的数据保护技术，如数据脱敏、访问控制、风险监测等。

四、案例效果

1.通过数据安全合规评估，有助于银行提高对监管政策变化的敏感度和应对能力，能够快速适应监管要求，降低合规风险。

2.通过评估，银行能够识别数据安全管理中存在的潜在风险，并采取相应的控制措施以降低数据泄露、滥用等安全风险。

3.在合规评估过程中，对银行内部数据安全管理流程进行了梳理，并提出了优化改进方案以提高管理效率。

4.银行员工的数据安全意识得到加强，能够在日常业务中更好地遵守数据安全管理规定。

五、案例评价

实施数据安全合规评估项目不仅有助于银行应对当前的监管要求，还能够在长远中提升银行的整体竞争力和市场地位。

B 某银行 DSMM 认证咨询项目案例（翰纬科技提供）

一、案例背景

DSMM（Data Security capability Maturity Model）认证是我国首个依据国家标准《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）开展的数据安全认证。标准给出了组织数据安全能力的成熟度模型架构，规定了数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全的成熟度等级要求。

某公司经过持续不断的努力，在数据安全建设方面已经取得了大量工作成果，包括成立了数据安全团队、建立了基本的数据安全管理制度、对业务数据进行了梳理、对敏感数据制定了管控措施，以及加强了对员工数据安全意识的培训等，但仍需在一些方面进行加强和完善，包括更新数据分类分级策略、全面评估数据安全风险、优化数据安全技术工具、强化数据安全监测机制等。

基于上述背景和现状，该公司决定启动数据安全 DSMM 认证项目，基于科学的方法论，对公司当前的数据安全能力成熟度进行检验，体系化地构建更加高效的数据安全管理体系，获得 DSMM 三级认证，保障公司在数字化时代的可持续发展。

二、解决方案

1.评估现有数据安全状态：通过问卷调查、访谈、文档审查和系统扫描等方法，全面评估公司当前的数据安全状况。

2.数据安全成熟度模型对标：将公司的数据安全管理实践与 DSMM 模型的标准进行对标，识别差距和改进领域。

图：DSMM3 级对标自评估结果

3.风险评估和管理：识别数据安全风险，评估风险等级，并制定相应的风险管理和缓解策略。

4.数据安全政策和流程优化：制定或更新数据安全政策和流程，确保它们与 DSMM 标准一致，并满足公司的具体需求。

5.技术控制措施实施：推荐和实施必要的技术措施，如数据加密、访问控制、数据脱敏、网络安全等。

6.认证准备和申请：帮助公司准备 DSMM 认证所需的文件和证据，并支持认证申请过程。

三、案例优势

1.咨询公司拥有数据安全领域的专业知识，能够提供符合 DSMM 标准的定制化解决方案。

2.咨询公司具有在不同行业和领域实施 DSMM 项目的经验，能够借鉴最佳实践并避免常见陷阱。

3.作为外部咨询顾问，能够提供客观的评估和建议。

4.咨询公司拥有先进的评估工具和方法，提高评估效率和准确性。

5.在项目过程中提供持续的咨询和支持服务，与认证机构保持良好的沟通，协助公司顺利通过认证审核。

四、案例效果

1.帮助公司了解其当前的数据安全能力现状，识别存在的不足和薄弱环节，明确改进方向和重点。

2.DSMM 为公司提供了一组标准化的关键过程和实践，有助于公司构建一套完整的数据安全管理体系，提高数据安全保障水平。

3.提升数据安全管理人员的技能，增强全体员工的数据安全意识。

4.向客户及合作伙伴表明公司保障数据安全的能力，有助于增加公司在同行业内的竞争优势，稳固市场地位。

五、案例评价

1.随着国家和行业监管部门对数据安全要求的不断提高，公司有义务满足监管要求，而通过 DSMM 认证等手段能够证明公司的数据安全能力符合国家标准，有助于提高公司在监管方面的合规性。

2.公司通过提升数据安全能力，不仅满足监管要求，还能够向客户和合作伙伴展示其在数据安全方面的卓越实力，从而在市场上树立良好声誉。

DSMM 认证在一些领先企业中得到了广泛应用，有许多专业的咨询机构和认证机构提供数据安全能力成熟度认证服务，可以为公司提供专业的认证咨询和支持，确保认证项目的顺利实施和有效达成。

C 某银行数据安全审计案例（谷安天下提供）

一、案例背景

《数据安全法》《个人信息保护法》发布后，国家高度重视数据安全法的落实，金融监管机构也对数据安全领域重点关注，由于某银行近些年重要信息系统持续建设和数据安全能力持续提升，加速实现“信息科技支撑业务开展”向“金融科技赋能数字化转型”演进，完善的数据安全体系成为持续推进全行业务高质量发展的基础。伴随科技支撑业务发展能力的不断提升，数据安全领域风险隐患日益凸显，其中数据泄露、数据丢失等已成为主要痛点。为全面防控数据安全风险，全力支撑业务创新发展，发起本次数据安全专项审计项目，旨在发现数据安全体系存在的风险及不足，提供可落地的管理建议和控制措施。

二、解决方案

咨询公司经过多年的理论与实践研究，提出了数据安全治理体系成熟度评价模型，如下图所示。

成熟度级别	安全状况	性质描述	赋值范围	备注
持续管理级	极低风险	数据安全治理已形成体系，组织架构及职责落实效果好，制度体系健全，应急管理及演练管理已基本形成体系化，能够主动开展业务连续性体系自评估及管理审计活动，能够通过应急演练对应急预案、资源建设、人员配备进行持续改进及优化。	>=90	保持
量化管理级	低风险	数据安全治理已形成体系，组织架构及职责明确，职责及制度体系执行效果好，战略方向和目标清晰，应急预案建设已覆盖重点业务和系统，演练执行力较好，业务影响分析和业务连续性风险评估可量化分析与评价，灾备中心建设满足合规要求，可主动管理和监控业务连续性各项活动的有序开展。	>=80 且<90	列入长期规划
主动管理级	中等风险	数据安全治理已基本形成体系，组织架构及职责明确，制度体系较为完善，战略方向清晰，各项应急预案较全面，应急演练执行效果较好，已建立同城及异地灾备中心。	>=70 且<80	部分要点需列入短期规划，其它列入长期规划
基本管理级	高风险	数据安全治理未成体系，组织架构和职责已明确，战略及策略不明确，业务连续性制度部分缺失，应急预案不全面，开展过应急演练，已有初步灾备环境。	>=60且 <70	体系建设列入短期规划，其他列入长期规划
初始管理级	极高风险	数据安全治理尚未形成体系化，业务连续性组织架构及职责有待完善，管理制度严重缺失，应急预案不全面、执行效果差，应急演练执行效果仍需提高，灾备建设不完善，需要立即对数据安全治理体系开展规范化建设	<60	体系建设列入短期规划

图：数据安全体系成熟度评价模型

咨询公司将数据安全治理组织架构、数据安全体系建设、数据采集、传输、存储、使用、删除、销毁、访问控制、运行安全等方面建立详细的指标分解，统计并提炼了 16 个评分项、80 个评价指标，能够对数据安全治理体系进行全方位的审计评价。

序号	评分项	标准分	权重	评估得分	综合得分
1	数据安全治理组织架构	100	0.05		
2	数据安全管理职责	100	0.05		
3	数据安全管理制度体系	100	0.08		
4	数据采集管理	100	0.08		
5	数据传输管理	100	0.08		
6	数据存储管理	100	0.08		
7	数据使用管理	100	0.08		
8	数据删除管理	100	0.08		
9	数据销毁管理	100	0.08		
10	数据安全运行管理	100	0.05		

11	数据安全策略	100	0.03		
12	数据安全访问控制	100	0.05		
13	数据监控与审计	100	0.05		
14	数据安全检查和评估	100	0.05		
15	数据安全事件处置	100	0.03		
16	数据安全治理工具	100	0.08		
总计			1	——	

表： 数据安全体系成熟度评分表

三、案例优势

1. 专业——自研的方法论、丰富的行业经验

结合国际和国内数据安全治理标准和方法论，全面指导数据安全审计项目有序实施，对数据安全治理方法论、审计指标、数据安全类行业产品等均有一定的研究，通过深入解读数据安全相关国家法律法规，并将最新的研究成果及时转化为审计方法论。

2. 全面——治理、管理、技术、工具全方位审计

咨询公司以国际国内标准和行业规范为参照，以客户的业务需求为导向，以大众化的信息安全意识普及和专业培训为铺垫，以管理咨询为过程，以数智化审计赋能平台为工具，以技术服务为手段，为企业提供一体化、多层次、全方位、以人为本的服务，解决数据安全治理体系不健全、风险隐藏深、数据工具难检查等痛点，为客户提供专业、深入、细致的审计服务，实现 IT 审计服务的精细化落地。

3. 服务能力——专业的数据安全审计团队

咨询公司拥有在国际咨询机构从业或在大型金融机构从事信息科技风险管理、数据库管理、数据安全管理、IT 审计的专业团队，具有 CISA、CISSP、PMP、CDGA、CDGP、CISP-DSG 等多项专业资质，实施过众多的数据安全审计项目，具有丰富的行业经验和专业的理论知识。

四、案例效果

该银行经过本次数据安全审计后，得到如下收益和提升：

1. 对比了与《数据安全法》《个人信息保护法》《金融数据安全 数据生命周期安全规范》《金融数据安全 数据安全分级指南》等法规与行业监管的差距及不足。

2. 本次共发现问题项 20 个，发现主要问题如下：数据安全治理体系不健全、数据安全岗位能力较弱、缺少数据防泄露、数据脱敏等管理制度、科技外包环节存在敏感信息泄露风险、安全管控桌面程序可

被绕开、数据安全负责人未正式发文、未落实数据安全风险评估与监测要求、数据未实现有效分类分级等。

3. 咨询公司从顶层建设、流程优化、能力提升、风险修复等四个层面为客户提出了系统化、专业化的管理建议，助力客户数据安全管理的全面提升。

4. 对客户的审计部门、数据安全部门分别提供了数据安全审计、数据安全意识等两个层面的知识转移及培训，进行了有效的知识赋能。

五、案例评价

国内银行的数据安全治理体系建设工作已快速起步，如何有效的进行体系建设和应用成为银行关注的主要问题，通过审计评价，可以帮助银行更全面的了解与法规与监管的差距，通过管理建议，帮助银行更全面和系统化的了解行业实践，为银行数据安全管理提升进行了有效的助力，帮助客户发现问题，解决问题，为客户实现了有效的赋能。

D 某银行数据分类分级技术工具案例（绿盟提供）

一、案例背景

自 2018 年《银行业金融机构数据治理指引》发布，数据治理工作成为全国商业银行信息科技工作的核心与重点，经过数年发展，到 2021 年全国商业银行已基本构建完成数据治理架构，随之成立了数据管理部门，建立了数据仓库、数据中台、大数据平台等数据应用架构，均基本具备对业务数据的综合分析与利用能力。因此银行业较高的数据治理水平催生出明确的数据安全需求，识别、保护上述融入数据治理架构的业务数据是银行业数据安全建设的主要特征。

数据安全工作的落地，在于做管理流程管控和技术工具的管控，只有进行此两部分落地工作的开展，才能有效实现数据管控的目的。然而数据的重要程度不同，决定了数据的级别差异，不同级别的数据也必将对应不同的管控措施。所以，针对数据级别的识别确认，是管控措施能落地有效的基础。

为提高某国有银行敏感数据识别效率，需要采用敏感数据识别产品，对数据库中与客户相关的业务数据进行抽样扫描和识别，并且将经产品扫描识别到的敏感信息，对接某国有银行数据管理系统完成敏感信息标记和视图展现。

二、解决方案

图：绿盟数据分类分级方案流程

目标：在实际开始数据分类分级之前，对目标范围内所有数据表、数据项、数据文件进行全面的梳理，形成数据资产表作为分类分级的输入。

依据：参考行业标准《金融数据安全 数据安全分级指南》《个人金融信息保护技术规范》《金融数据安全 数据生命周期安全规范》，构建数据分类分级的整体框架，而后将数据资产逐层代入框架，形成基于标准的数据分类分级规则库。

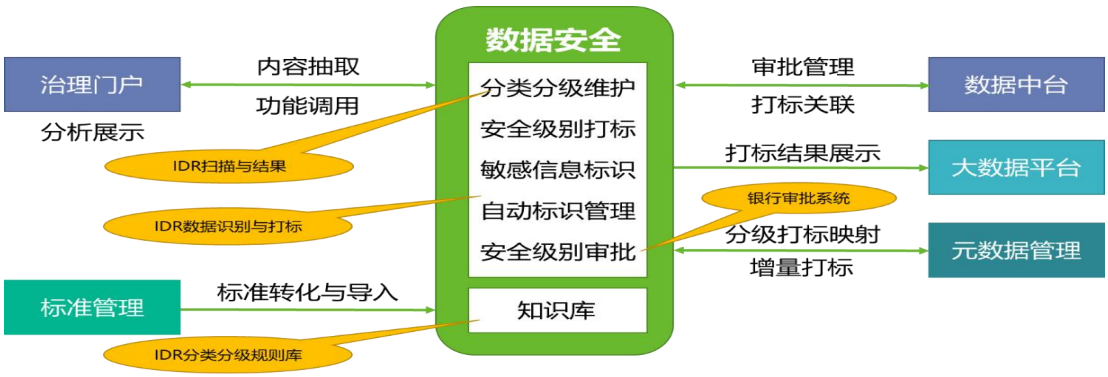
流程：

针对某国有银行业务中发现的标准中未明确的数据内容，根据数据的属性或管理归属，对数据资产进行归类；同时，根据业务需求和安全能力，定义数据分级的级数，以及各级别的判断依据。形成树形的分类层次结构，并为最低一级的数据子类逐一分配安全级别。最终将自定义规则融入基于标准的数据分类分级规则库中。

某国有银行数据分类分级标签的识别可以分为两个步骤，第一步先进行敏感信息的识别，第二步进行自动化的分类分级套入。敏感信息的识别需要进行实际数据的规则匹配，规则匹配维度包括字段名、字段备注、字段内容、表备注等；为保证规则匹配的准确度，前期需要进行数据字典及相关元数据的识别，更新优化匹配规则。针对每条匹配规则会对应一个数据标签，标签对应的类别和级别是根据分类分级字典表内置的，可实现自动化映射。

RSAS-IDR 产品实现自动化的数据识别和映射，产品具有实用、易用、适用、高效的数据资产测绘能力，具有丰富的敏感数据发现算法和智能的数据分类分级算法，帮助某国有银行梳理全行敏感数据全景图，将数据分类分级结果推送到生产、业务和安全部门，为数据的合理应用和安全防护奠定了坚实的基础。

三、案例优势



图：RSAS-IDR 数据分类分级与业务对接融合

1. 分布式部署，实现产品高可用；
2. 融入数据使用安全审批流程，为不同级别数据的安全使用提供决策支撑；
3. 内置行业分类分级模板规则共计 10 万余条，数据识别准确率达到 98%以上；
4. 内置机器学习+神经网络算法，比传统算法产品在内容识别与打标率上提高 83%；
5. 提供多种扫描机制，包括断点扫描、定时扫描、周期扫描、增量扫描，帮助数据管理者快速发现数据变化。

四、案例效果

1. 对数据资产的分类可进行新增、合并、拆分、删除等操作；
2. 对数据资产的类别、级别进行变更审批（对接业务系统）；
3. 对数据资产进行自动化的分类标识、分级标识；
4. 对数据资产分类分级标识实现人工校验；
5. 对个人金融信息进行自动化的区分与标识；
6. 对数据资产自动标识规则可创建、可修改、可变更等管理；
7. 以数据安全视角对数据业务进行基于分类分级的审批管理（对接业务系统）；
8. 形成全量数据分类分级标识知识库，供其他系统调用（对接业务系统）。

五、案例评价

国有银行通常已经做过数据治理工作，在此之上进行数据分类分级工作具有较好的效果，并且可以更好地进行一些智能化技术的应用。同时，数据分类分级工作结束后，结果可反馈给数据中台，为用户使用数据提供帮助。

E 某金融机构数据分类分级技术工具案例（明朝万达提供）

一、案例背景

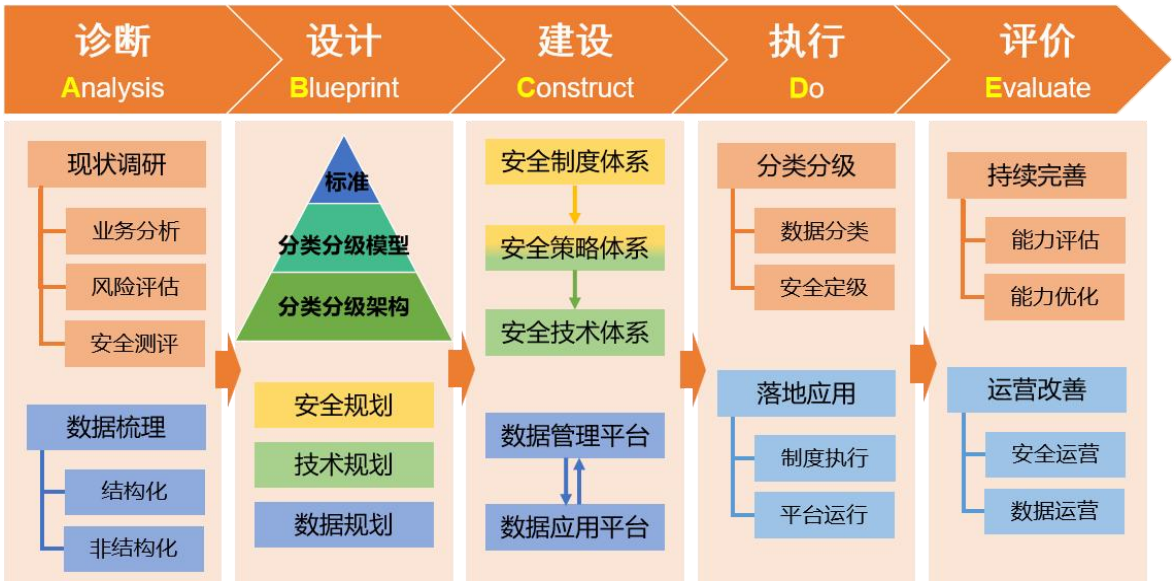
目前，银行、证券、保险等金融机构的业务数据规模大、价值高、应用场景复杂，面向投资者提供着众多金融产品和服务，对数据安全治理有着天然的诉求。然而金融机构在开展数据安全和敏感数据保护政策落地时，往往面临着一系列痛点和挑战：比如多数金融机构在开展数据分类分级的工作中，由于业务场景复杂、数据类型多样，以致传统自动化识别技术覆盖率和准确率不高。特别是非结构化数据，检测率低，

开发和应用不足，难以开展深度的数据挖掘与分析工作，导致规则难以制定。大部分仍依赖个人的工作经验和主观判断，评价过程十分简单，缺乏科学的指导。

如何结合金融机构业务特性，满足相关政策法规、监管要求，建立健全数据分类分级体系，保护数据在业务中的合规使用及流转，提升数据价值就显得尤为迫切。针对以上痛点问题，公司以数据分类分级自动化建设为切入点，围绕敏感数据特征，从数据资产盘点、分类分级、数据安全运营等不同维度，建设完善健全的数据分类分级体系，提升数据安全运营保障能力，为数字化转型赋力、赋能。

二、解决方案

针对某金融机构数据体量大、存储分散、数据质量不高、应用人数众多等特点，公司为某金融机构提供分类分级自动化解决方案。从数据资产自动嗅探、数据资产自动化采集、数据资产梳理、数据分类分级、数据安全运营等方面开展数据安全体系建设，减少金融机构在分类分级过程中的大量人员投入，提升分类分级效率，最大化释放数据的价值和潜力。



图：某金融机构数据安全分类分级解决方案

1. 资产自动嗅探

金融机构内部业务多元化，各类 IT 支撑平台、业务系统信息化管理平台增多产生海量数据，安全管理人员无法清楚有效的掌握当前网络空间内海量数据资产，同时无法对数据资产进行安全有效的管理。为解决上述问题，公司智能数据治理平台支持主动嗅探网内数据库，可指定 IP 段和端口的范围进行搜索。

2. 数据资产自动化采集

数据治理平台可对关系型数据库、非关系型数据库以及大数据等 30 种不同类型的数据库，通过导入不同类型的模板文件对金融机构内部敏感数据库进行梳理。平台对梳理完成的资产抽取数据库表、字段等信息，支持对数据样本进行随机抽取，同时支持手动、周期、定时等方式更新对资产进行增量数据获取。

平台支持资产归属配置，可将数据库资产从部门、系统、区域、业务标签四个维度进行归类管理。资产配置用户后该用户方可查看该资产信息，包括任务扫描结果、分类分级任务、数据资产梳理、资产全景等与资产相关的信息。

金融机构梳理内部文件资产时，可将非结构化资产通过挂载服务器的方式配置协议信息，读取文件目录及对应文件基础信息。结合自然语言处理（NLP）技术对文本数据进行分析，从中提取关键信息，有效提升非结构化文件的识别率。

3. 数据分类分级

公司通过多年的实践经验以及行业积累，已总结归纳了不同行业的分类分级模板，开箱即用，减少用户现场的规则调优工作，并且通过指定分类分级模板，从业务条线出发，对业务细分，细化数据管理颗粒度。遵从系统性、规范性、稳定性、明确性等原则，形成从总到分的树形逻辑体系结构，对分类后的数据确定级别。

4. 安全运营

依据咨询结果，平台可向第三方系统提供梳理的资产信息以及对应的分类分级结果。并提供标准的 API 接口，供外部系统从资产、分类分级树目录逐级获取信息，实现动态安全管理。对于自研产品，可将分类分级结果进行推送。生成的安全规则、策略模板，可为第三方系统、自研产品提供标准依据规范，形成深度融合与多方联动，同时可采用多种防护能力进行数据安全管控，比如：终端安全防护、网络防泄漏、数据脱敏、数据库审计等。结合 AI 引擎、UEBA 等新兴技术应用，可实现智能告警，数据流转溯源，安全态势感知等一体化数据安全解决方案，帮助金融机构从根本上解决了数据安全治理规划面临的难题，为金融机构开展数据分类分级、风险评估、数据安全运营防护、数据安全管控提供合理依据，真正让数据安全建设变得简单易行。

三、案例优势

1. 技术创新

全公司 IT 资产“数字化”；动态安全“智能化”；事件处置“智能化”；管理协同“一体化”。

2. 成果先进

内置规则模板采用主动嗅探技术和 nlp 技术大幅提升识别率，根据制定的分类分级规则进行识别，自动匹配和数据打标，快速输出数据资产分类分级结果，形成最终的数据分类分级清单，将敏感数据识别精

确率提升至 95%，显著解决了行业内部分数据需要人工进行数据分类分级和打标的现状。

3. 成果可复制

在整个数据分类分级过程内置分类分级模板结合了数据安全法律法规和金融行业监管要求，从管理、技术和运营三个方面均开展了数据安全治理工作，具备可推广性。

四、案例效果

1. 为企业提供专业、快速的数据分级技术支撑
2. 利用数据分类分级的结果指导数据安全策略的部署与实施，实行数据安全治理。
3. 帮助某金融机构对数据资产进行全面的清查和摸排，为某金融机构后续的数据资产管理和数据安全体系建设打好基础。

五、案例评价

大型机构的数据较为复杂，因此使用智能化的手段进行大规模数据的识别、扫描、分类分级建设。在其中，对自动化要求较高，且需要有较为准确的输出。金融行业的业务数据特征有一定的相似性，因此可以将项目中的模板、成果纵向下发或横向移植。

附件：数据安全合规建设调查问卷

第 4 题　贵公司是否建立了清晰的数据安全治理组织架构?　[多选题]

选项	小计	比例
建立了覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构	32	72.73%
建立了数据安全责任制	33	75%
明确了党委（党组）、董（理）事会对本单位数据安全工作负主体责任	24	54.55%
明确了公司主要负责人为数据安全第一责任人	30	68.18%
明确了公司分管数据安全的领导为直接责任人	29	65.91%
以上都没有	3	6.82%
本题有效填写人次	44	

第 5 题　贵公司是否建立了完善的数据分类分级管理机制?　[多选题]

选项	小计	比例
已制定数据分类分级保护制度	38	86.36%
建立了数据目录	26	59.09%
建立了数据分类分级规范	32	72.73%
以上都没有	1	2.27%
本题有效填写人次	44	

第 6 题　贵公司是否开展了数据分类分级工作?　[多选题]

选项	小计	比例
依据人行的《金融数据 数据安全分级指南》对数据进行了分类分级	23	52.27%
依据证监会的《证券期货业数据分类分级指引》对数据进行了分类分级	17	38.64%
依据金融监督管理总局的《银行保险机构数据安全管理办法（征求意见稿）》对数据进行了分类分级	14	31.82%
对全部数据进行了分类分级	13	29.55%
对个人金融信息进行了分类分级	17	38.64%
以上都没有	4	9.09%
本题有效填写人次	44	

第 7 题　贵公司使用自动化分类分级工具的效果如何?　[单选题]

选项	小计	比例
自动化程度较高、准确率较高，能够自动识别 50%以上的数据	10	22.73%
自动化程度一般、准确率一般，大部分工作需要人工介入	11	25%
没有采用自动化分类分级工具	23	52.27%
本题有效填写人次	44	

第 8 题　贵公司是否制定了数据安全管理办法?　[单选题]

选项	小计	比例
已制定了数据安全管理办法，但是没有参照金融监督管理总局的《银行保险机构数据安全管理办法（征求意见稿）》	28	63.64%
已参照金融监督管理总局的《银行保险机构数据安全管理办法（征求意见稿）》制定了数据安全管理办法	14	31.82%
未制定数据安全管理办法	2	4.55%
本题有效填写人次	44	

第 9 题　贵公司是否建立了企业级的数据架构?　[多选题]

选项	小计	比例
已依据监管要求开展了数据治理，建立了企业级的数据架构	27	61.36%
已根据公司业务发展需要，建立了企业级的数据架构	22	50%
已采用信息系统支持，实现了数据地图	11	25%
以上都没有	5	11.36%
本题有效填写人次	44	

第 10 题　贵公司是否在处理敏感级及以上数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，事先开展了数据安全评估?　[单选题]

选项	小计	比例
已开展了数据安全评估	19	43.18%

只针对个人金融信息开展了安全评估	16	36.36%
未开展数据安全评估	9	20.45%
本题有效填写人次	44	

第 11 题　贵公司是否建立了企业级数据服务管理体系?　[多选题]

选项	小计	比例
制定了数据服务规范	24	54.55%
建立了专职数据服务团队	36	81.82%
统筹了内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动	27	61.36%
以上都没有	4	9.09%
本题有效填写人次	44	

第 12 题　贵公司是否制定了以下数据安全管理机制?　[多选题]

选项	小计	比例
数据收集	40	90.91%
外部数据采购	27	61.36%
数据加工	38	86.36%
数据使用	40	90.91%
数据共享及集团内部共享	30	68.18%
委托处理数据	23	52.27%
数据共同处理	21	47.73%

数据转移	20	45.45%
数据公开	25	56.82%
数据跨境	24	54.55%
数据删除与销毁	31	70.45%
以上都没有	1	2.27%
本题有效填写人次	44	

第 13 题　贵公司是否制定了从生产环境提取数据的管理流程?　[多选题]

选项	小计	比例
已制定管理流程	42	95.45%
审批环节中包含数据安全岗位	26	59.09%
审批环节中包含数据所有者	27	61.36%
明确了数据使用或者保存期限	26	59.09%
明确了数据脱敏要求	32	72.73%
以上都没有	0	0%
本题有效填写人次	44	

第 14 题　贵公司是否建立了针对大数据、云计算、移动互联网、物联网等多元异构环境下的数据安全技术保护体系?　[单选题]

选项	小计	比例
已建立	19	43.18%
未建立	25	56.82%

本题有效填写人次	44	

第 15 题　贵公司是否实现了数据安全保护措施与信息系统的同步规划、同步建设、同步使用？ [单选题]

选项	小计	比例
已实现	35	79.55%
未实现	9	20.45%
本题有效填写人次	44	

第 16 题　贵公司是否将数据纳入网络安全等级保护？ [单选题]

选项	小计	比例
已纳入	36	81.82%
未纳入	7	15.91%
不适用	1	2.27%
本题有效填写人次	44	

第 17 题　贵公司是否建立了数据安全保护基线？ [多选题]

选项	小计	比例
将敏感级及以上数据纳入信息系统保护	31	70.45%
制定用户对数据的访问策略	38	86.36%
敏感级及以上数据传输采用安全的传输方式	36	81.82%
敏感级及以上数据采取安全存储措施	35	79.55%

敏感级及以上数据达到使用或者保存期限后，采取技术措施及时删除或者销毁	25	56.82%
以上都没有	3	6.82%
本题有效填写人次	44	

第 18 题　贵公司是否开展了数据安全的技术基础设施建设？ [多选题]

选项	小计	比例
用户身份管理	39	88.64%
数据匿名化	17	38.64%
行为监测	30	68.18%
日志审计	41	93.18%
数据虚拟化	7	15.91%
以上都没有	2	4.55%
本题有效填写人次	44	

第 19 题　贵公司是否采取措施保障了大数据平台安全？ [多选题]

选项	小计	比例
高可用设计	37	84.09%
安全加固	28	63.64%
数据备份	37	84.09%
大数据服务访问授权机制	35	79.55%
动态监测与审计大数据访问行为	22	50%

以上都没有	2	4.55%
不适用	3	6.82%
本题有效填写人次	44	

第 20 题　贵公司是否建立了人工智能管理机制？ [多选题]

选项	小计	比例
对人工智能模型开发应用进行统一管理	16	36.36%
建立模型算法产品外部引入的准入机制	10	22.73%
对模型研发过程进行主动管理，实现模型算法可验证、可审核、可追溯	15	34.09%
模型算法投入使用时，开展数据安全审查	12	27.27%
使用人工智能技术开展业务时就数据对决策结果影响进行解释说明和信息披露	9	20.45%
实时监测自动化处理与系统运行结果	7	15.91%
建立人工智能应用的风险缓释措施	7	15.91%
以上都没有	15	34.09%
不适用	9	20.45%
本题有效填写人次	44	

第 21 题　贵公司是否实施了与外部交互数据的安全技术措施？ [多选题]

选项	小计	比例
建设了与外部交互数据的专用平台	23	52.27%
采用了 API 安全的技术措施	25	56.82%

采用了其他安全技术措施	21	47.73%
以上都没有	0	0%
不适用	7	15.91%
本题有效填写人次	44	

第 22 题　贵公司是否建立了个人信息保护管理体系？ [单选题]

选项	小计	比例
已建立	39	88.64%
未建立	5	11.36%
本题有效填写人次	44	

第 23 题　贵公司是否对以下领域开展了数据安全风险监测？ [多选题]

选项	小计	比例
超范围授权或者使用系统特权账号	29	65.91%
内部人员异常访问、使用数据	31	70.45%
对数据集中共享的系统或者平台的网络安全、数据安全威胁	24	54.55%
敏感级及以上数据在不同区域的异常流动	16	36.36%
移动存储介质的异常使用	22	50%
外包、第三方合作中的数据处理异常或者数据泄露、丢失和篡改	24	54.55%
客户有关数据安全的投诉	32	72.73%
数据泄露、仿冒欺诈等负面舆情	32	72.73%

以上都没有	3	6.82%
本题有效填写人次	44	

第 24 题　贵公司部署了哪些数据安全防护技术或工具　[多选题]

选项	小计	比例
数据分类分级自动化工具	15	34.09%
数据防泄漏 DLP	38	86.36%
数据库审计	32	72.73%
数据库防火墙（网关）	19	43.18%
API 安全	24	54.55%
数据库加密存储	14	31.82%
文档加密	24	54.55%
数据脱敏	39	88.64%
网间摆渡	26	59.09%
运维人员管理系统	28	63.64%
用户行为分析	19	43.18%
以上都没有	0	0%
本题有效填写人次	44	

第 25 题　贵公司是否获得了数据安全相关认证？　[多选题]

选项	小计	比例
DSMM - 数据安全能力成熟度认证	4	9.09%

DSM - 数据安全管理认证	2	4.55%
ISO 27701	6	13.64%
其他认证	8	18.18%
以上都没有	29	65.91%
本题有效填写人次	44	

扫一扫，添加编审组组长微信
咨询了解更多本报告相关内容

版权声明