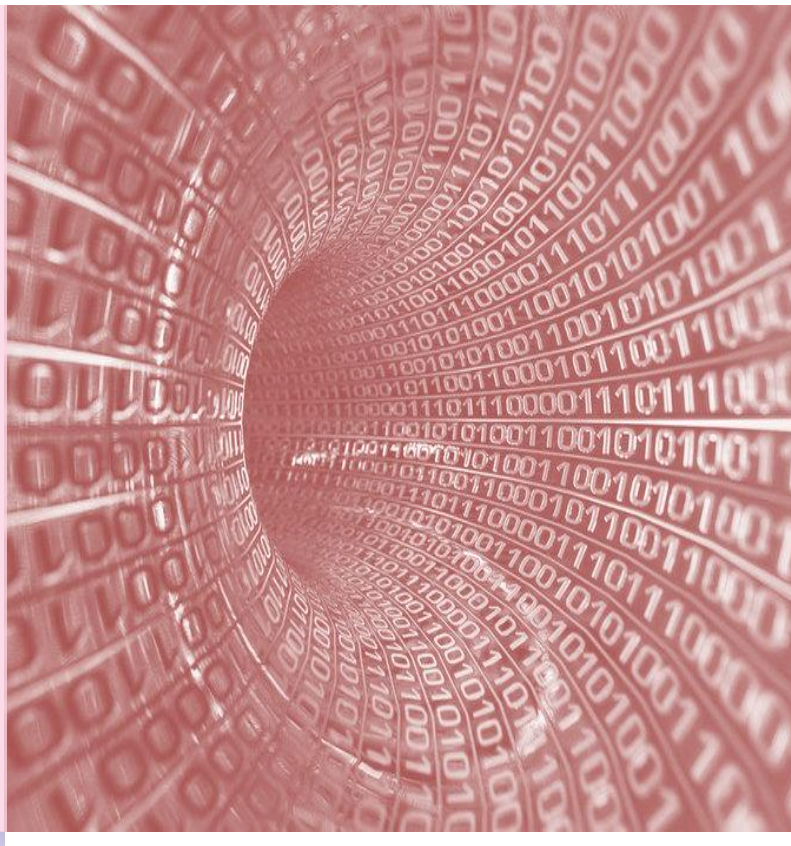
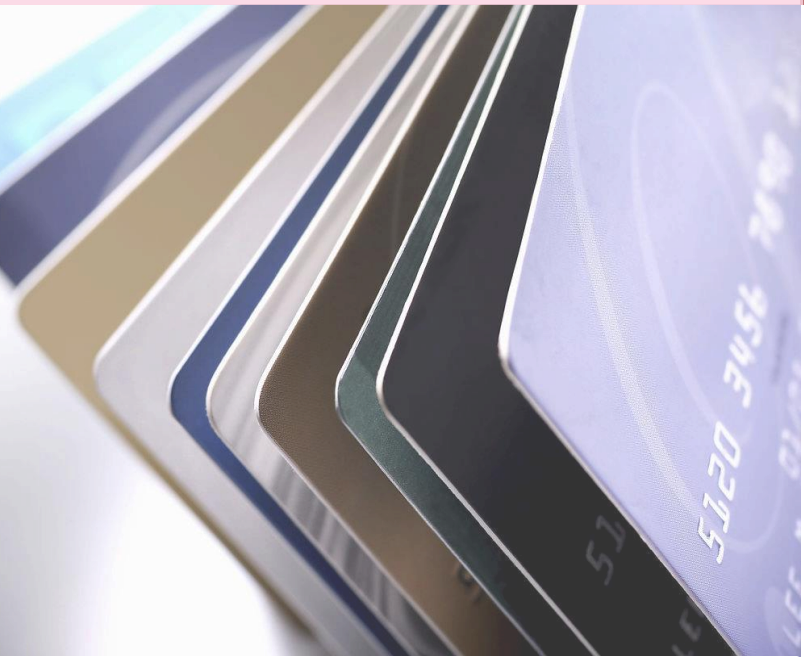




信用卡中心
信息安全现状
调研报告

ANY. 安言咨询

目录

前言

进入 2014 年以来，信息安全事件层出不穷，信用卡行业的信息安全管理工作面临着前所未有的挑战。应浦发银行股份有限公司信用卡中心要求，于 2014 年 1 月至 2014 年 2 月开展上海地区信用卡中心调研活动并在当年 4 月 25 日特别召开了一次成果分享研讨会，邀来参与此次调研的卡中心等相关人员参与会议。

在此特别感谢浦发银行信用卡中心、建设银行信用卡中心、兴业银行信用卡中心、招商银行信用卡中心、农业银行信用卡中心、广发银行信用卡中心等相关人员对本次调研的大力支持和帮助！

声明

本次调研活动受到时间及资源的限制，主要关注安全管理组织架构、安全技术应用情况、业务支撑相关情况的相关内容，其范围及内容可能还不完整。此外， 由于本次是初次尝试开展此类卡中心间的调研活动，故其过程和整个展现形式并非十分成熟，若存在不当之处还请见谅。

报告中所提到的“卡中心”均指参与到本次调研活动的信用卡中

一、 调研目的

为了给浦东发展银行股份有限公司信用卡中心在信息安全技术中远期规划的制定上提供参考，针对卡中心较为关注的技术发展的方向，以同业间采用的技术方法作为依据，特开展此次上海地区各银行信用卡中心信息安全管理现状的调研，以最终达到信息系统安全、持续、稳健地运行，增强卡中心竞争力和可持续发展能力。

同时，通过开展此次调研工作，编写此份卡中心信息安全调研报告，该报告将免费提供给参与调研的各家银行信用卡中心，希望借此调研结果分享的机会，搭建专业的交流平台，增加信用卡中心之间的互相交流。

二、 调研对象

浦发银行 信用卡 SPD BANK Credit Card

上海浦东发展银行 1993 年正式开业，其信用卡于 2004 年正式发行。截止到 2013 年，浦发卡中心共发行信用卡 653 万张。

中国建设银行 China Construction Bank

中国建设银行成立于 1954 年，是国有五大商业银行之一，其信用卡中心成立于 2004 年。截止到 2013 年，建行卡中心共发行信用卡 5201 万张。

兴业银行 INDUSTRIAL BANK CO.,LTD. 信用卡 Credit Card

兴业银行成立于 1988 年，是经中国人民银行批准成立的首批股份制商业银行之一，其信用卡中心成立于 2004 年正式发行。截止到 2013 年，兴业卡中心共发行信用卡 1195 万张

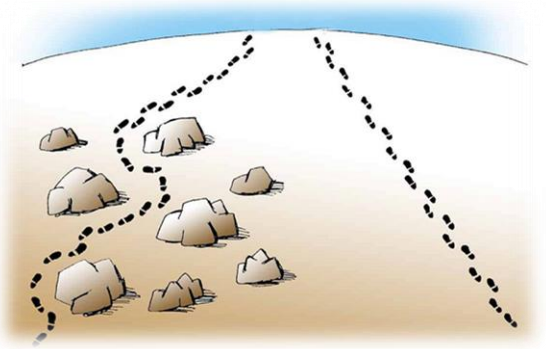
二、调研对象

招商银行成立于 1987 年，是中国第一家完全由企业法人持股的股份制商业银行，其信用卡于 2002 年正式发行。截止到 2013 年，招行卡中心共发行信用卡 5121 万张。

农业银行成立于 1951 年，是新中国成立的第一家国有商业银行。截止到 2013 年，农行卡中心共发行信用卡 4438.81 万张

广东发展银行 1988 年经人民银行批准成立，是国内最早组建的股份制商业银行之一， 于 1995 年发行国内第一张真正意义上的信用卡。截止到 2013 年，广发卡中心共发行信用卡 2793 万张。

（以下简称建行卡中心、兴业卡中心、农行卡中心、招行卡中心、浦发卡中心、广发卡中心）



三、 调研方法

上海安言信息技术有限公司会针对信用卡中心较为关心的问题制定此次调研的范围及内容，通过与卡中心科技部相关人员当面访谈、交流的形式就制定的问题展开讨论，随后会将调研的记录整理汇总并发送给受调研的人员确认，以电话或邮件的形式对调研的记录进行修改、完善，得到最终的调研结果。最终会对所有的调研结果进行统计分析，以图表表的形式在交流会中呈现，并形成一份完整的调研报告。

其中广发卡中心相关人员在广州办公，因此其采用远程调研的方式，通过邮件及电话交互。

四、 调研内容

此次卡中心间的调研工作主要针对较为关注的三个层面、十二个方面的问题展开讨论。

具体内容见下表所示：

调研内容	安全管理组织架构	信息安全团队职责归属
		因为连续性职责归属
		合规工作事项牵头归属
		信息安全资源配备
	安全技术应用情况	邮件外发监控与审计
		终端安全管控
		打印审计
		数据脱敏处理
		数据库操作审计
		虚拟桌面部署
	业务支撑相关情况	SAS 系统安全管控
		智能终端安全管控
		信用卡申请环节电子签名技术应用

五、 调研结果

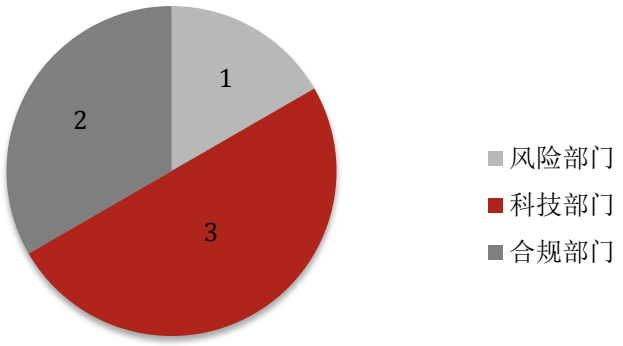
1. 卡中心安全团队现状

1.1 信息安全团队职责归属

信息安全团队所属部门	
调研对象	归属部门
浦发卡	技术运营部信息安全组
建行卡	开发协调处
兴业卡	信息技术部
招行卡	信息技术部综合室
农行卡	信息技术部综合管理与信息安全组
广发卡	合规处信息安全组

1.2 业务连续性职责归属

目前各家卡中心的业务连续性工作牵头部门各不相同，但其一般都与总行业务连续性工作牵头部门保持一致。主要包括以下几类：合规部门、风险部门和科技部门。具体情况如图表 1 所示：

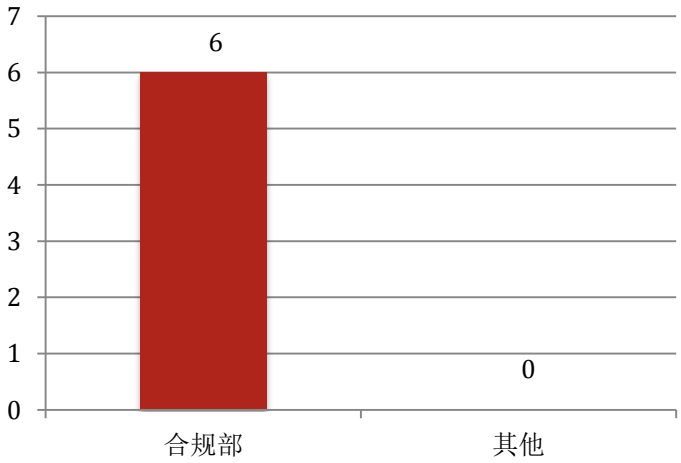


图表1 业务连续性牵头部门统计图

1.3 合规工作事项牵头归属

合规工作的牵头部门无一例外均为合规部门（法律合规部、合规处等），主要工作职责是识别各类合规要求（法律法规、合规要求），但是合规部门仅是负责合规的牵头，落实对比等工作依然由客户部门负责完成。

具体情况如图表 2 所示：



图表 2 合规工作牵头部门统计图

1.4 信息安全资源配备

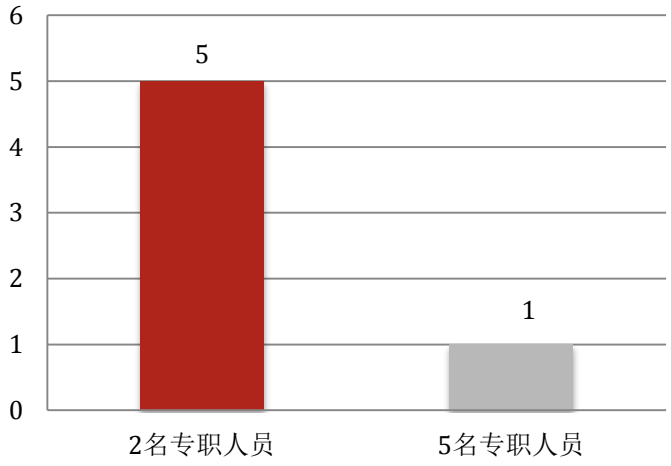
（1） 现状

各家卡中心基本都有信息安全管理团队，其中广发卡中心的安全团队有 5 人且均为专职，规模最大；其余卡中心安全团队目前均为 2 人。

具体情况如图表 3 所示：

关注点：

各家卡中心信息安全团队的规模以及安全团队的工作量和发展趋势。



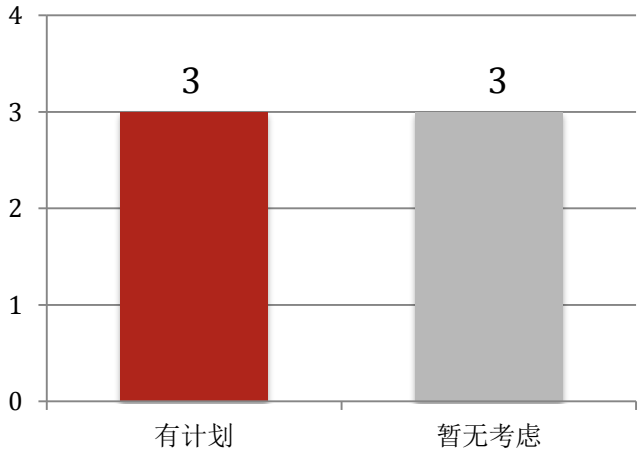
图表 3 安全团队资源配备统计图

（2） 分析

绝大部分卡中心的信息安全管理人员均为专职人员，且均有较为丰富的 IT 相关工作经验，但是仍有部分卡中心的信息安全工作由兼职人员负责，且信息安全工作仅为实际工作的一小部分工作内容。

安全团队除了传统的工作如制定管理策略、制定/实现技术需求、进行技术方面的安全评估，体系日常管理上的压力日渐加大，风险评估及文件维护的相关事项都是每年必须的。另外，随着监管要求不断深化、外部环境不断复杂化、管理体系不断落实，信息安全部门承担的工作职责越来越多，各家卡中心均表示目进行团队扩充的占到受访卡中心的 50%。

具体情况如图表 4 所示：



图表 4 安全团队扩充计划统计图

（3） 建议

各家卡中心应根据自身的工作情况适当进行团队的扩充，并尽可能招聘一些有 IT 相关经验、熟悉安全工作的人员。另外，在招聘时可以考虑逐步向信息安全管理人员提出持证上岗的要求。工作中，还应鼓励信息安全从业人员获得相关资质证书，同时也可以制定一些激励政策以带动安全团队不断学习、不断提升的积极性。

针对持证上岗的要求，现有如下证书可供参考：

序号	名称	介绍
1	上海地区的人员信息安全素养提升及信息安全保障从业人员等相关资质	通过信息安全保障从业人员（CISAW）考试和其他评价方式证明获证人员具备了在一定的专业方向上从事信息安全保障工作的个人素质和相应的技术知识与应用能力，以供用人单位选用具备能力资格的信息安全工作人员。
2	信息安全师认证	信息安全师低到高分为三个等级：助理信息安全师（国家职业资格三级）；信息安全师（国家职业资格二级）；高级信息安全师（国家职业资格一级）。其要求人员具备丰富的信息安全专业知识；掌握较为全面的信息安全保障技能；具有较强的学习能力、信息处理能力和应变能力；能够准确判断问题和解决问题；善于沟通与协调，合作意识强；语言表达清楚。
3	国际信息系统审计师（CISA）证书	CISA 全称：“Certified Information Systems Auditor”。拥有 CISA 资格证书说明持证人具备的实践能力和专业程度。随着对信息系统审计、控制与安全专业人士需求的增长，CISA 已成为全球范围内个人与公司机构不可或缺的认证。CISA 资格证书代表持证人有卓越的能力服务于公司的信息系统审计、控制与安全领域。此外，获得任何职业资格证书的持证人必须参与继续教育计划来维持其资格证书。
4	注册信息系统安全师（CISSP）的证书	CISSP 全称：“Certified Information Systems Security Professional”。是一种反映信息系统安全专业人员水平的证书，可以证明证书持有者具备了符合国际标准要求的信息安全知识和经验能力，已经得到了全球范围的广泛认可。

2. 安全技术应用情况

2.1 邮件外发监控与审计

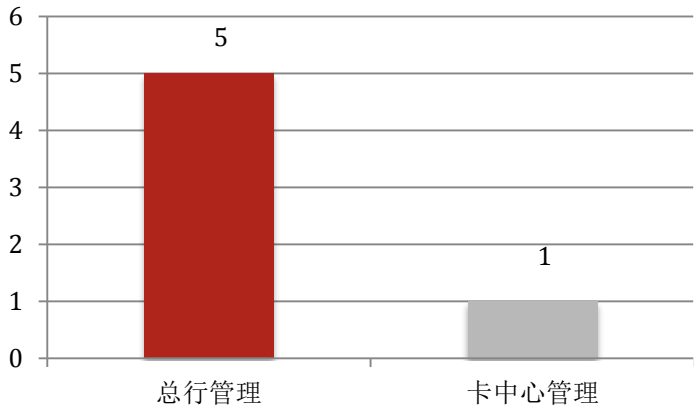
2.1.1 邮件外发监控

（1） 现状

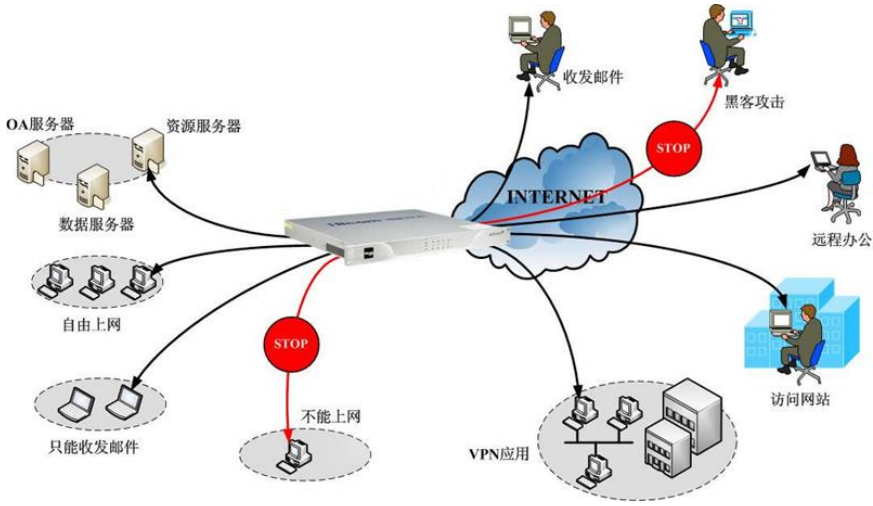
层面的相关技术措施。现对于邮件外发的监控主要涵盖以下内容：邮件主题、正文、附件名称及未加密的附件。具体情况如图表 5 所示：

关注点：

分析各家卡中心对于邮件外发的监控实施情况及监控的内容。



图表 5 邮件外发监控管理情况统计图



（2） 分析

各家卡中心现都已对邮件外发监控制定了相关策略，但是在监控过程中依然存在有待改进的地方，一是无法实现对于已加密附件的检查，包括加密的 office 文件、PDF 文件、加密压缩包等；二是对于发现敏感词的邮件仅仅是进行告警而已，并不会直接拦截它的发送，这样只能达到事后追责的效果，不能完全杜绝敏感信息的外泄，存在一定的安全隐患。

（3） 建议

- 部署信息防泄漏相关产品或统一的文档加密系统，在外发前对邮件实现自动加密，然后发件人通过其它可靠途径告知收件人密码。这样可以自动实现邮件加密、邮件与密码分开发送的过程，但需要采购相关产品。
- 控制外发邮件的邮箱权限，把邮件发送的权限细分为对卡中心内部、外部等，并且仅赋予级别相对较高的人外发邮件的权限，例如业务部门组长以上、客服主管以上的人员。
- 在邮件发送时一旦监控到邮件中包含涉及敏感信息的相关内容即对其进行“临时阻断”，即将邮件暂时隔离，由具有权限的人审核无误后方可继续发送。这类做法可以极大程度的避免带有敏感信息的邮件外泄，但是工作量较大，需要大量的人力配备来支撑。

2.1.2 邮件外发量审计分析

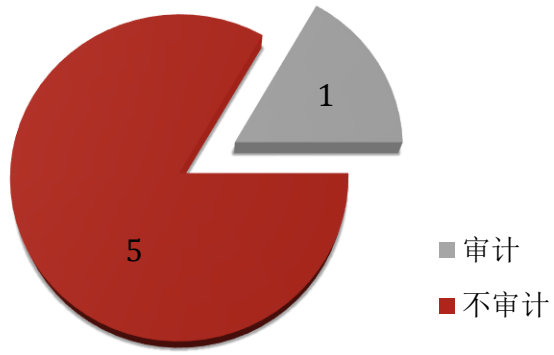
（1） 现状

所有参与到调研中的卡中心中，除了对邮件进行敏感词的监控之外，有部分卡中心还会对邮件外发量进行审计，包括外发邮件的数量和容量。通过采集数据之后，评估每个岗位的人员在一段时间内可能产生的邮件量，设定一个基准值，若有员工突然发生邮件数量剧增或邮件容量总值过大的情况，就会对其邮件进行审核，包括其加密的附件，以检测是否存在数据泄露的情况。

具体情况如图表 6 所示：

关注点：

各家卡中心对于各个岗位人员阶段内的邮件外发量是否进行对比、审计。



图表 6 邮件外发量审计情况统计图

（2） 分析

通过对邮件量进行监控，确实是解决加密附件无法监控的手段之一，但是其需要大量的资源来支持，需要对所有岗位的情况进行评估及审计，其工作量相对较大、工作效率相对较低，并且针对不同岗位设定一个合理的阀值来界定外发量是否过大在实施过程中存在一定难度。另外，这种做法难以根据业务的实时变化情况对制定的策略进行灵活调整。

（3） 建议

邮件外发量的审计分析是邮件外发监控的进阶控制，各家卡中心可以根据自身的实际况结合资源配备，选用此方法。

定义说明：数据泄密（泄露）防护（Data leakage prevention，DLP），又称为“数据丢失防护”（Data Loss prevention，DLP），有时也称为“信息泄漏防护”（Information leakage prevention，ILP）。DLP 是通过一定的技术手段，防止企业的指定数据或信息资产以违反安全策略规定的形式流出企业的一种策略。DLP 这一概念来源于国外，是目前国际上最主流的信息安全和数据防护手段。

2.2 终端安全管控

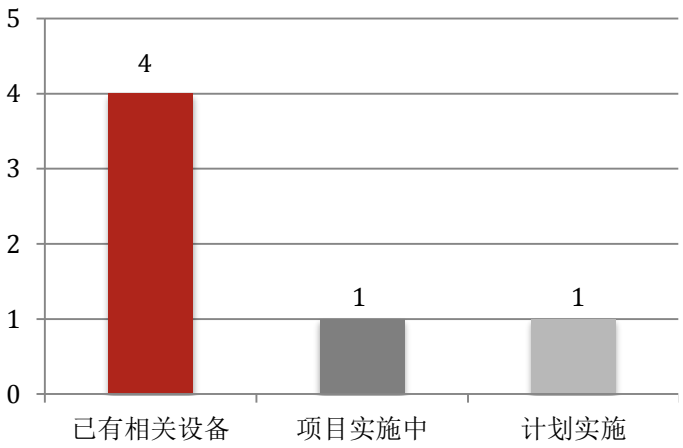
2.2.1 DLP 产品部署及应用情况

关注点：

各家卡中心 DLP 的部署、实施情况、选用产品的品牌及应用范围。

（1） 现状

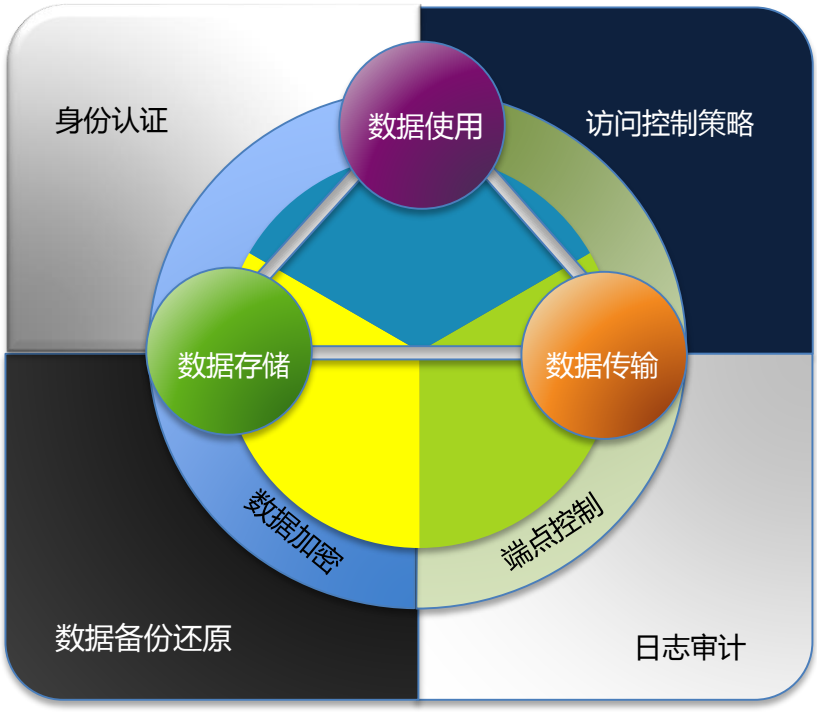
参与本次调研个卡中心中，大部分都已部署了 DLP 产品，个别正在实施或已计划实施（具体情况如图表 7 所示）。在已部署了 DLP 产品的卡中心中基本都选用的是赛门铁克（Symantec）的相关产品。



图表 7 DLP 产品部署情况统计图

（2） 分析

DLP 产品基本都已被部署，但是仅有一小部分卡中心会对全卡中心范围部署，大部分还是只针对邮件网关的管控。



DLP 原理图

（3） 建议

DLP 系统主要从终端准入控制、数据保护、主机审计、安全管理、桌面管理等多个角度构建一套完整的终端安全防护体系，通过技术手段全面贯彻落实用户的安全管理策略。DLP 形态上与终端安全管理系统比较相似，都是安装在终端电脑，根据安全策略上报数据、接受管理。两者的区别在于 DLP 产品能够对文件的内容进行内容分析，自动识别敏感文件并识别处用户对敏感文件所进行的敏感操作。

各家卡中心可以根据自身实际的安全需求考虑实施 DLP 产品部署，同时再部署 DLP 的同时要充分考虑卡中心业务需求，在保障安全的同时应充分考虑业务开展的便利性。

2.2.2 USB 端口管控情况

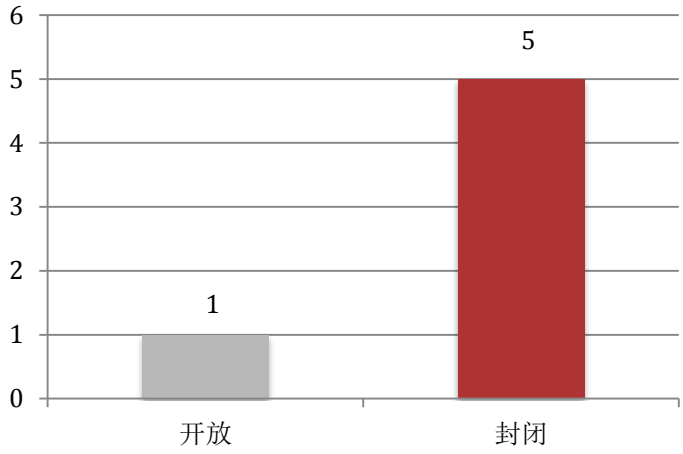
关注点：

在卡中心实施部署 DLP 相关产品前，邮件外发管控已经降低了敏感信息通过邮件泄露的可能性，因此利用移动存储介质拷贝文件就成了卡中心关注的重点。USB 端口管控情况主要关注各家卡中心对于终端 USB 接口的控制情况及控制措施。

（1） 现状

参与本次调研的卡中心大部分都已关闭 USB 端口，但仍有个别卡中心在部署 DLP 产品后仍未关闭 USB 端口。

具体情况如图表 8 所示：



图表 8 USB 端口管控情况统计图

（2） 分析

USB 端口的控制主要采用加密或制定移动存数介质（针对办公及生产网络分别采用不同的移动存数介质，并对介质统一进行编号登记，且要求不得将其带离工作环境）、部署相关的 DLP 策略或给特定部门开放权限等。

（3） 建议

对于 USB 端口的管控措施目前已经较为成熟和灵活，在采用 DLP 或桌面安全管理软件后，可以允许鼠标、键盘等常规设备使用，但对于存储介质、通信设备（如 USB 无线网卡、USB 3G 上网卡等）可以阻止其正常工作。

关注点；

在卡中心实施
DLP 相关产品前，邮
发管控已经降低了
信息通过邮件泄露
能性，因此通过文件
泄密就成了卡中心
的重点。打印审计主
注各家卡中心对于
的管控情况，包括打
控的内容。

2.3 打印审计

2.3.1 打印审计实施情况

（1） 现状

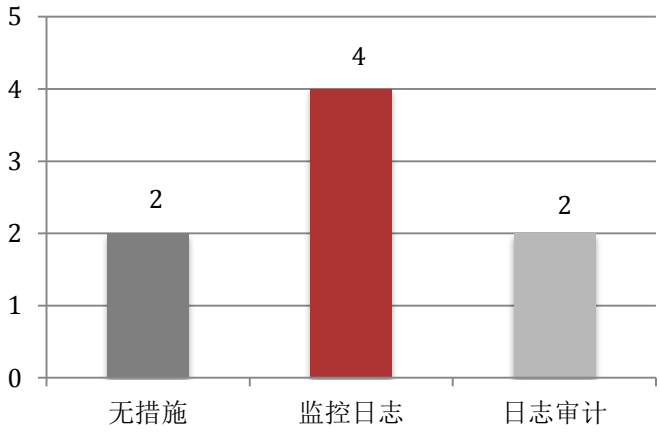
参与本次调研的卡中心中，对于打印方面的控制主要包含以下几类：

①不采取任何措施；

②采取监控措施，监控打印用户和打印文件名并记录成日志，但不会对日志进行审计；

③采取监控措施，监控打印用户和打印文件名并记录成日志，并且会对日志做审计。

具体实施情况见图表 9 所示：



图表 9 打印审计措施统计图

（2） 分析

已进行打印控制的卡中心都对打印的人和物进行了监控，区别在于是否定期对日志进行审计。缺失审计这一环节，就不能及时的发现打印过程中对于机密文件的复制，难以对所有文件进行管控，导致敏感信息泄露的可能性大大增加，但是打印审计的工作量较大，且职责归属目前暂不明确，究竟由合规部还是安全团队管理难以清晰定义。

（3） 建议

还未部署打印审计的卡中心可以逐步开展打印审计的实施，先对打印文件的中心的资源配备不足以支持大量的打印审计工作，可以先将打印的内容记录成表单的形式而后对表单进行审计，能相对减少工作量。

2.3.2 打印输出控制

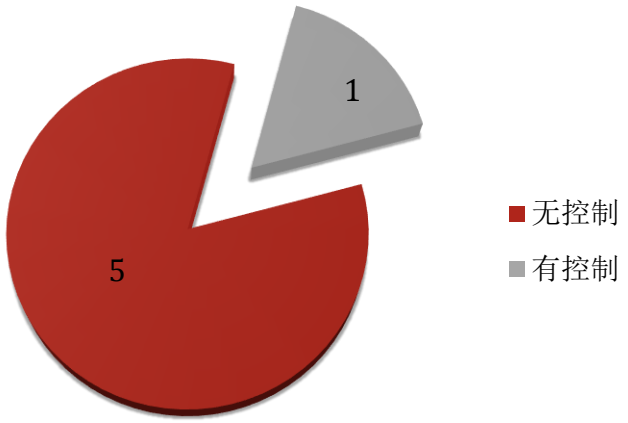
（1） 现状

所有参与本次调研的卡中心中，部分已严格限制打印权限的分配，如仅对业务部门组长或客服主管以上级别开放打印权限；但是绝大部分卡中心对于输出方面还未加以控制，仅有一家通过技术手段实现打印输出控制，进行打印操作后，扫描工牌验证身份后打印机方可输出相关纸质文档。

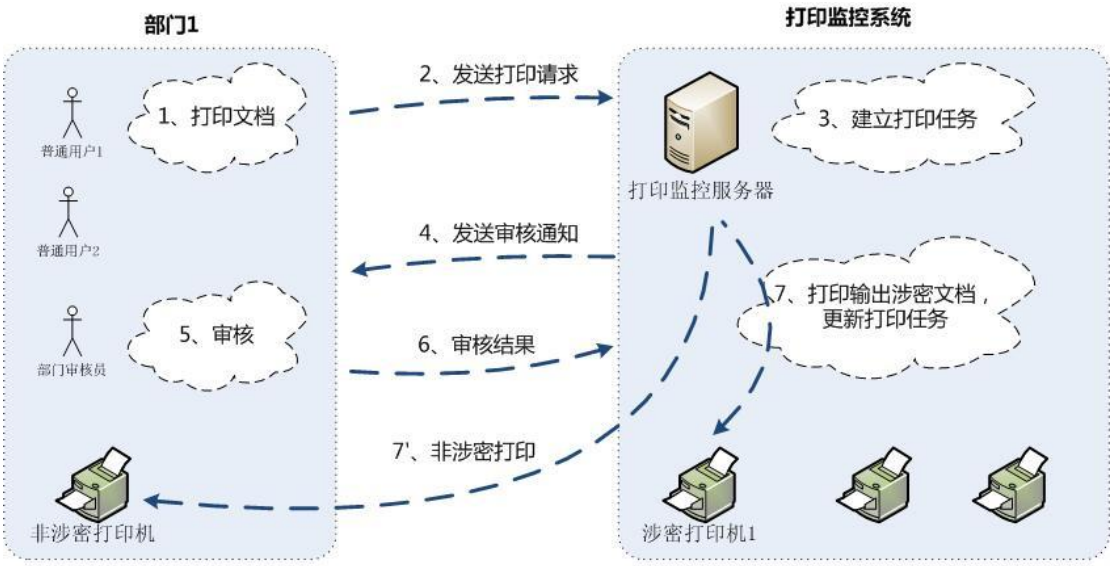
具体实施情况如图表 10 所示：

（1） 关注点

各家卡中心对于打印输出端的控制情况，是否通过技术手段实现目标。



图表 10 打印输出控制情况统计图



打印控制原理图

（2） 分析

通过打印权限的控制可以有效的限制打印文件的人数和级别，从而达到减少数据外泄的可能性；在打印输出端，通过扫描工牌进行打印输出端的控制可以很好的限制打印文件的领取，使只有拥有权限的人员才可以进行文件的打印，并且避免了打印文件漏拿或错拿的现象。

（3） 建议

目前尚未对文件打印进行控制的卡中心可以先从权限控制开始执行，仅赋予一定级别以上的员工以权限，如业务部门组长、客服主管等，并且可以定期进行打印权限的复核，以确保权限发放无误。

而打印输出控制作为对打印的进阶控制，在卡中心资源配备允许的条件下，可以采用技术手段对打印的输出端作限制，进一步减少敏感信息外泄的风险。

定义说明：数据脱敏，指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。这样，就可以在开发、测试和其它非生产环境以及外包环境中安全地使用脱敏后的真实数据集。

2.4 数据脱敏处理

关注点：

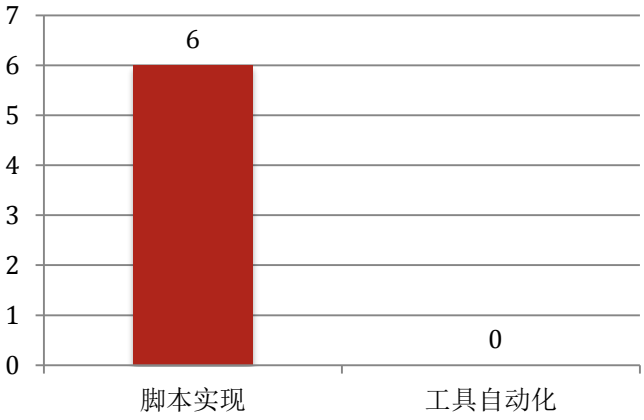
各家卡中心在数据脱敏方面的实现方式，是否有通过工具实现。

（1）现状

所有参与本次调研的卡中心均采用脚本的方式实现数据的脱敏，暂未采用相关的工具。具体实施情况如图表 11 所示：

（2）分析

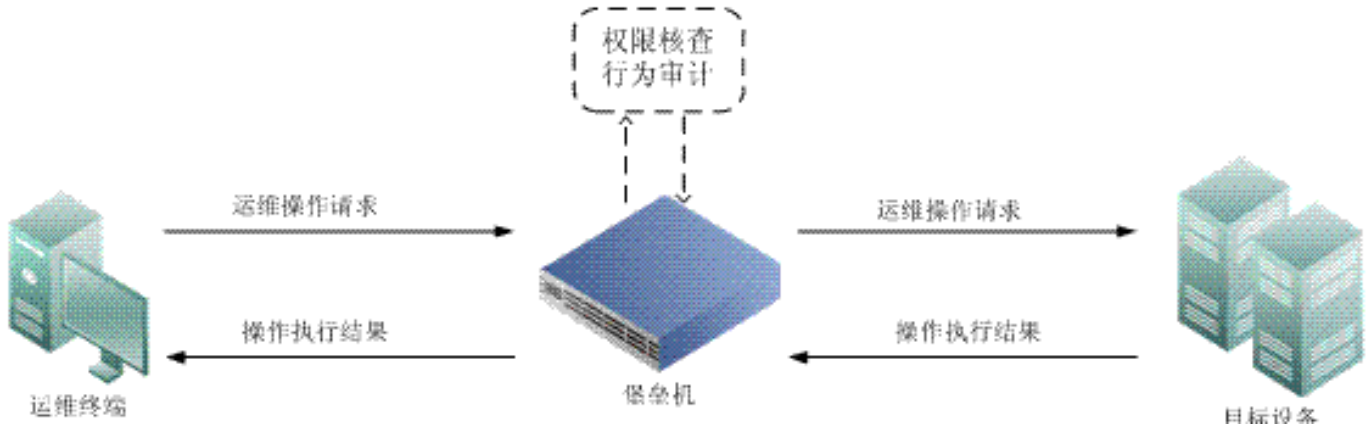
卡中心在测试环境运行的数据有时候必须使用真实的数据以确保数据测试的真实性，那么数据从生产环境导入到测试环境的这段过程就可能直接造成客户数据的泄露，因此需要对生产环境导出的数据进行变形。目前数据的变形主要通过工具自动化实现或脚本实现。两者相比较脚本的优势在于可以通过卡中心实际的需求去编写或修改脚本的内容，包括脱敏的字段、位置等等，操作便捷。而通过工具实现则可以批量的定制完成数据变形的过程，但是采购工具需要耗费一定的资金，存在成本问题。



图表 11 数据脱敏实现方式统计图

（3）建议

由于数据脱敏的操作仅在数据导出生产环境时需要采用，考虑到脱敏的个性化及成本问题，各家卡中心可以沿用脚本实现的方式。



数据库操作审计原理图

2.5 数据库操作审计

（1） 现状

关注点：

各家卡中心对数据库操作的审计方式。

参与本次调研的卡中心对数据库操作的审计方式主要包括以下三种：①基于堡垒机技术实现对数据库操作的屏幕录像

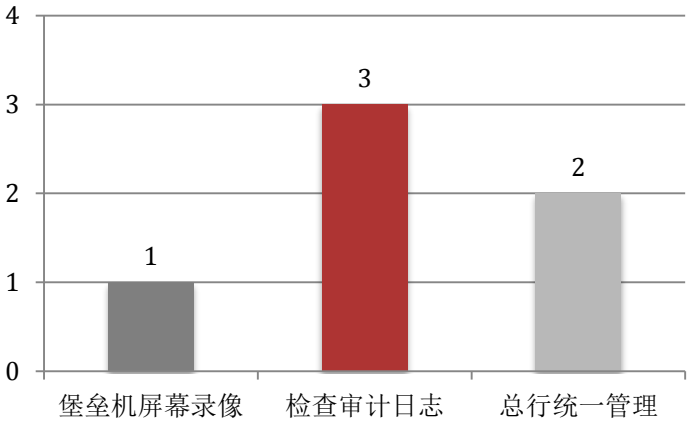
②采用人工抽查审计日志的方式

③由总行负责系统运维，卡中心不承担数据库操作审计工作

具体情况如图表 12 所示：

（2） 分析

基于堡垒机实现对数据库的屏幕录像可以完全记录下操作的过程但是其易造成容量过大，审查效率低下；而日志审计需要数据库记录更多的日志信息，对数据库的性能会产生影响，并且日志本身又被篡改的风险。



图表 12 数据库审计措施统计图

（3） 建议

目前尚无数据库审计工具的卡中心可以通过权限控制来限制访问数据库人员的数量，从而减少数据库产生的日志达到减轻审计工作量的目的；也可以通过限制数据库相关操作来减少日志的产生。

定义说明：简单的来说，虚拟桌面是指支持企业级实现桌面系统的远程动态访问与数据中心统一托管的技术。一个形象的类比，就是今天，我们可以通过任何设备、在任何地点，任何时间访问在网络上的我们的邮件系统，或者网盘；而未来我们可以通过任何设备，在任何地点、任何时间访问在网络上的属于我们个人的桌面系统。

2.6 虚拟桌面部署

关注点：

各家卡中心虚拟桌面的部署情况及主要产品。

（1） 现状

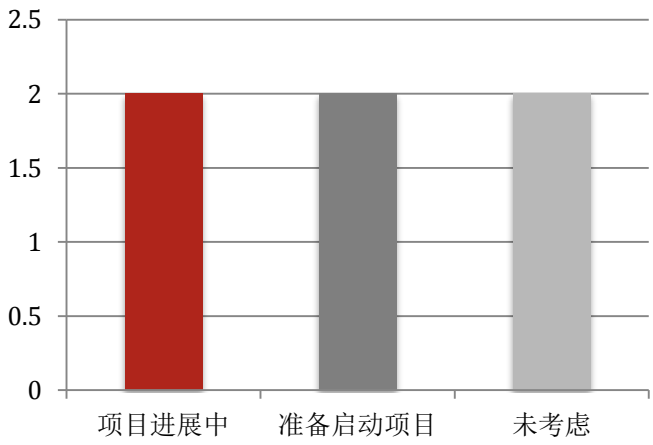
参与本次调研的卡中心有一部分已开展虚拟桌面的实施，同时还有一些仍未将此项列进考虑范围内。

具体情况如图表 13 所示：

（2） 分析

采用虚拟桌面技术可以实现跨网段的安全管控，降低数据落地的风险，同时更易于对系统和软件进行维护、控制。目前已有卡中心整体采用了桌面虚拟化技术，目的是实现办公网访问生产网，办公网访问互联网以及第三方驻场人员访问生产网的管控。

现在的虚拟桌面主要有两种类型：桌面虚拟化、应用虚拟化。前者将所有内容都放在远程桌面只存在数据上的交互，而后者的程序安装在本地交互的知识操作的过程。但是两者都依赖于网址的质量，一旦网络受阻用户体验度将会下降。



图表 13 虚拟桌面部署情况统计图

（3） 建议

现在虚拟桌面的使用主要集中在 Citrix 和 Vmware 两个产品，但是它们的部署及后期维护成本略高，在实际使用时，卡中心可以根据自身需求，灵活选择应用范围。

3. 业务支撑相关情况

3.1 SAS 系统安全管控

关注点：

各家卡中心对于SAS系统操作的管控方式。

（1） 现状

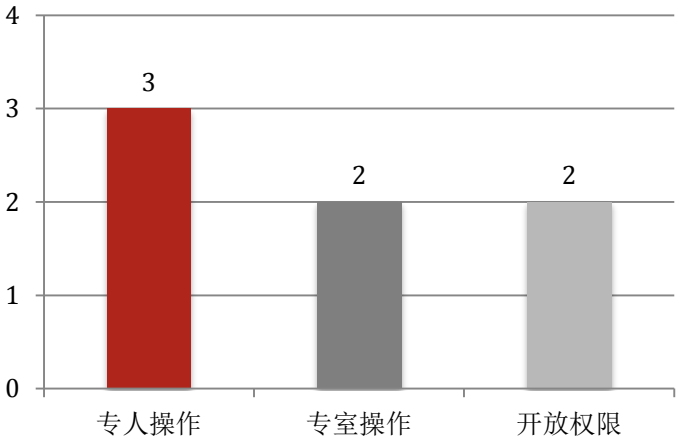
参与本次调研的卡中心对于 SAS 系统的使用管理模式主要包含三类：集中式管理、分布式管理、混合式管理。

集中式管理：SAS 系统由数据挖掘团队专职操作，业务部门只提供需求，并且有独立的环境进行数据挖掘处理。

分布式管理：业务部门及 IT 部门均有 SAS 系统的操作权限，安全管控通过权限控制及终端安全控制实现。

混合式管理：集中式管理与分布式管理的混用，既有专职的团队负责特定需求的处理，各部门特定人员也有 SAS 系统的操作权限，并且会设置独立的环境进行操作。

具体情况如图表 14 所示：



图表 14 SAS 系统安全管控情况统计图

（2） 分析

SAS 系统全称“Statistical Analysis System”，主要功能是数据访问和管理、数据展现以及数据分析。是用于数据分析与决策支持的大型集成信息系统。

现卡中心的数据挖掘分析都是基于 SAS 系统实现的，大部分业务都依赖于 SAS 提取的数据，但是 SAS 系统内的客户数据对于卡中心而言也是绝密的，因此如何进行 SAS 系统的安全管控就是我们关注的重点。

集中式管理：采取专人专室的操作方式，其安全性相较于其他管控手段而言是最高的，但是如何确保从数据挖掘分析团队处以安全可靠的方式提供给业务部门是目前存在的问题；另外，这些数据与业务部门有一个较长的交互部门，工作效率上会有所降低。

分布式管理：向有工作需要的员工开放 SAS 系统的权限，大大方便了业务部门对于 SAS 数据的提取利用，但同时这种做法在安全方面的管控力度是相当低的。如果办公终端可以访问 SAS 系统，同时办又能访问互联网，那么没有部署 DLP 或者桌面安全管理软件，其数据落地后的外发难以监控。

混合式管理：集合了“集中式管理”与“分布式管理”的特点，在采取专人专室操作的同时又赋予一个部门或一个团队的人员以权限。

（3） 建议

各家卡中心在进行 SAS 系统的管控时，应充分考虑到业务部门对 SAS 数据需求的个性化程度及数据传输过程中的安全控制，以选用合适的管控方式。

3.2 智能终端安全管控

关注点：

各家卡中心在信用卡申请环节，对于智能终端的安全管控措施。

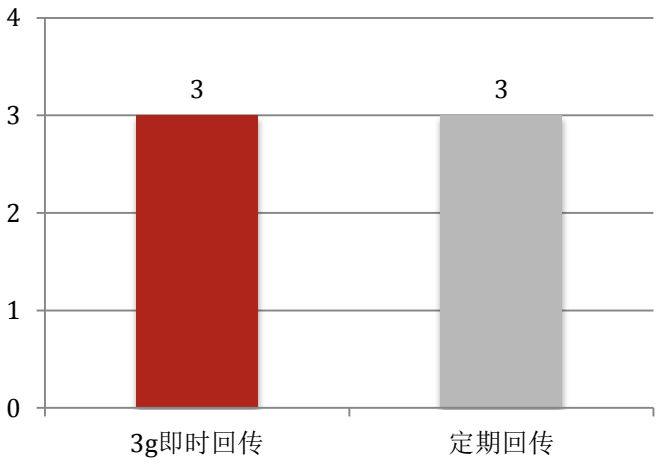
（1） 现状

参与本次调研的各家卡中心在信用卡申请环节时采取的管控措施各不相同，主要有利用 3g 网络即时回传和定期去网点进行回传。

具体回传模式如图表 15 所示：

（2） 分析

✧ 数据回传的模式主要分为“定期回传”和“即时回传”。前者通过业务员在指定时间将智能终端内的数据在网点经过专线的方式回传到本地，但是在数据录入直到回传的这段时间内，存在数据泄露的风险。后者采用 3g 网络传输，使智能终端不留痕。但是传输时采用的是 3g 加密方式。



图表 15 智能终端数据回传模式统计图

✧ 智能终端的安全管控主要由以下几种方式：设备与账号绑定、密码验证机制、超时锁定、远程数据清空、端口的安全控制、信息加密、芯片控制等，但是这些做法都无法避免系统自身存在的问题。

（3） 建议

各家卡中心应根据安全需求制定智能终端的安全策略，选择适合自身的措施。并且可以结合虚拟桌面技术的使用。

定义说明：电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。通俗点说，电子签名就是通过密码技术对电子文档的电子形式的签名，并非是书面签名的数字图像化，它类似于手写签名或印章，也可以说它就是电子印章。

3.3 信用卡申请环节电子签名技术应用

（1） 现状

所有参与本次调研的卡中心均未实施电子签名的技术。

（2） 分析

《中华人民共和国电子签名法》于中华人民共和国第十届全国人民代表大会常务委员会第十一次会议正式通过，银监会对电子签名也持开放态度，但是大部分卡中心的合规部门依旧觉得在技术实施上存在合规风险，因此电子签名技术在信用卡的申请环节迟迟未推广。

（1） 关注点

各家卡中心在信用卡申请环节电子签名技术的使用情况。

（3） 建议

随着技术的发展进步，电子签名技术终将被使用到信用卡的申请环节，但是在网点验证申请人信息的时候信息表上的“阅读声明”（本人已阅读全部申请材料，充分了解并知晓该信用卡产品的相关信息，愿意遵守领用协议的各项规则。）还应当保留是手写的方式，以防止电子签名带来的字体辨别不清的情况。

六、 小结

随着信息技术的发展，网络攻击手段也在不断的升级，新型的攻击渠道和恶意攻击者对卡中心讲构成连续、持续的威胁，因此需要管理层深层次的认识到信息安全的重要性并逐步确立新的思维模式。与此同时，伴随着移动设备技术的巨大进步，从上世纪九十年代到如今的智能终端（pad），我们的生活和工作得到了极大的便利，但它同时带来了新一轮的风险，这些可以通过技术设备控制、制度政策加以弥补，但是却不能完全将其杜绝，所以当我们考虑引入新技术的时候需要谨慎选择和测试。

除了加强对外界风险的控制，对于卡中心内部的安全隐患也需加强管控。应逐步加强对企业内部设备、流程的管理和技术手段，避免安全事件由内部爆发。