最新金融业机构信息自查报告(优秀5篇)

在当下这个社会中，报告的使用成为日常生活的常态，报告具有成文事后性的特点。写报告的时候需要注意什么呢？有哪些格式需要注意呢？下面我就给大家讲一讲优秀的报告文章怎么写，我们一起来了解一下吧。

金融业机构信息自查报告篇一

我局信息系统运转以来，能严格按照上级部门要求，积极完善各项安全制度、充分加强信息化安全工作人员教育培训、全面落实安全防范措施、全力保障信息安全工作经费，信息安全风险得到有效降低，应急处置能力得到切实提高，保证了政府信息系统持续安全稳定运行。

我局高度重视信息系统安全工作，成立有由主要领导任组长、分管领导任副组长、各处室负责人为组员组成的局信息安全工作领导小组，明确了局办公室为主要职能部门，确定了一名兼职信息安全员，召开了由分管领导、信息安全工作职能部门和重点部门负责人参加的会议，对上级有关文件进行了认真学习，对自查工作进行了周密的部署，确定了自查任务和人员分工，真正做到领导到位、机构到位、人员到位、责任到位、措施到位。为确保我局网络信息安全工作有效顺利开展，我局要求以各处室、下属单位为单位认真组织学习相关法律、法规和网络信息安全的相关知识，使全体人员都能正确领会信息安全工作的重要性，都能掌握计算机安全使用的规定要求，都能正确的使用计算机网络和各类信息系统。

我局在以前建立一系列信息安全制度的基础上，针对信息安全工作的特点，结合我局实际，重新修订了一系列信息安全制度和程序，做到按制度办事，提高执行力。按照市政府和市经信委要求，我局与计算机维保单位重新签订了服务协议，增加了信息安全与保密协议内容。同时我局还与全局所有工

作人员签订了安全保密协议。我局对涉密计算机和涉密移动存储介质高度关注，对所有涉密计算机和涉密移动存储介质全部进行编号在册统一管理，明确责任人和保管人，对涉密信息系统的使用进行多次重点检查，强化涉密人员管理，严格执行涉密计算机和涉密移动存储介质的相关管理制度，专门为涉密人员配发了带有硬件锁的u盘，严禁在涉密和非涉密信息系统间混用移动存储介质等等。对非涉密计算机的保密系统和防火墙、杀毒软件等皆为国产产品，公文处理软件使用微软公司的正版office系统，信息系统的第三方服务外包均为国内公司。

我局网络系统的组成结构及其配置合理，并符合有关的安全规定;网络使用的各种硬件设备、软件和网络接口是也过安全检验、鉴定合格后才投入使用的，自安装以来运转基本正常。我局经常开展信息安全检查工作，主要对操作系统补丁安装、应用程序补丁安装、防病毒软件安装与升级、木马病毒检测、网页篡改情况等进行监管，认真做好系统安全日记。今年，我局在市政府办的指导下试运行协同办公系统，投入10多万元为所有局领导、各处室配置了内网计算机，为涉密处室另配备了涉密计算机，从硬件上加强了涉密信息系统管理。

我局认真做好各项准备工作，对可能发生的各类信息安全事件做到心中有数，进一步完善了信息安全应急预案，明确应急处置流程，落实了应急技术支撑队伍，把工作做深做细做在前面。

我局针对信息管理人员实际情况，每年开展信息化教育培训，以掌握信息化管理技能为目的进行实践操作能力培训。还组织有关工作人员参加了相关信息安全培训，职工信息安全意识得到有效提高。

目前我局在市行政中心大楼内办公，网络和信息系统便于统一管理，内外网完全物理隔离，内网计算机均在有效管理范围内。局信息安全工作领导小组针对我局的信息安全形势，

定期组织由专业技术人员组成的检查小组到各个办公室专项检查网络和信息安全情况，仔细排查信息系统的漏洞和安全隐患，用专用工具查杀木马、病毒，及时加强防范措施，为所有计算机安装了正版杀毒软件和防火墙，有效提高了计算机和网络防范、抵御风险的能力。此外，检查小组针对个别在市行政中心大楼外办公的处室进行了上门检查，不放过任何信息安全死角。在检查的同时，检查小组还就信息安全知识进行了上门培训。经多次检查，我局信息系统总体情况良好，运行正常，未发现重大隐患。

(一)存在的主要问题

一是专业技术人员较少，信息系统安全方面可投入的力量有限。

二是规章制度体系初步建立，但还不完善，未能覆盖到信息系统安全的所有方面。

三是遇到计算机病毒侵袭等突发事件处理不够及时。

(二)下一步工作打算

一是进一步扩大对计算机安全知识的培训面，组织信息员和干部职工进行培训。

二是要切实增强信息安全制度的落实工作，不定期的对安全制度执行情况进行检查，从而提高人员安全防护意识。

三是要以制度为根本，在进一步完善信息安全制度的同时，安排专人，完善设施，密切监测，随时随地解决可能发生的信息安全事故。

金融业机构信息自查报告篇二

一年来，我校办学条件大大改善，信息技术和实验教学工作得到进一步发展。实验室建设得到巩固和完善，教学仪器设备得到丰富。教学技术和设备逐步规范化、标准化。人员的专业素质通过培训不断提高，教师的教育观念也在逐步更新。实验教学和视听教学逐渐成为教师教学中不可或缺的教学手段。演示实验和小组实验可以根据教学大纲和教材的要求正常进行。

这次自我评估的结果非常好。

学校实验教学、电教、信息技术教育、远程教育由专人管理，纳入学校工作计划。学校规划和制度健全，管理到位，考核良好。学校对所有专职管理人员要求严格，教师有计划有总结，教学仪器设备保管到位，各种登记表填写详细、完整、规范。账目齐全，仪器分类，摆放有序，整洁干净(柜有柜卡，仪器有标签)，账目一致，有借阅和定期维护的证据。

学校充分发挥资源优势，充分利用各种资源。每学期组织教师和工作人员按要求学习远程教育资源和信息技术知识，纳入教师个人评价。远程教育管理员可以坚持每天接收资源并分类。阅览室和图书馆每天应该开放两个小时以上。一年来，我们密切关注相关人员的专业培训，提高实验技能和管理水平，积极选择教师参与各种活动，如潼南县实验教师专业培训、重庆信息技术环境下的教学论文写作活动等。

虽然我们做了很多工作，取得了可喜的成绩，但从高标准、严要求的角度来看，我们的工作与先进学校相比仍有一定的差距。

1、声、美、工、体、卫设备的配备仍有不足，今后应进一步努力加强配置。

2、小学自然实验教学有待进一步完善。

金融业机构信息自查报告篇三

20××年，在信息中心党委的正确领导下，积极参加党支部和党小组组织的各项政治学习，学习了党的基本理论、基本知识，贯彻落实十七大精神，联系建设中国特色社会主义的丰富实践，联系党的建设，认真学习党章，自觉遵守党章，切实贯彻党章，坚决维护党章，用三个代表”重要思想武装头脑，不断提高政治理论水平和党性修养。下面就按着党员评议的要求分六方面总结

一、在学习方面

一年来自己能够按照信息中心党委的安排和要求，认真学习党的十七大报告、党章等，注重自身党性修养，能够积极参加树立荣辱荣辱观的学习和讨论，通过学习，不断提高了自己的思想素质，坚定了自己对理想的追求，用优秀党员的标准来严格要求自己，为实现这个目标而做一名共产党人应尽的义务。

二、在政治思想方面

坚持四项基本原则，与党中央在政治上、思想上、行动上保持高度一致，拥护党的路线、方针、政策，坚定对共产主义的信仰，坚决抵制违背科学发展观的错误行为。自觉认真的学习马列主义、毛泽东思想、邓小平理论、“三个代表”重要思想和科学发展观，努力掌握基本原理，把握丰富内涵和精神实质，并结合实际学以致用，努力改造自己的世界观、人生观和价值观。认真学习和领会党的各项方针政策，进一步激发爱岗敬业的热情，在平凡的岗位上自觉为我局的发展贡献自己的力量。

三、作风建设方面

一年来，自己能够按照党章的标准，遵纪守法、廉洁自律，在各项工作中能够牢记自己是一名党员，自己的一言一行时时影响着身边工作的群众，工作中能够发挥党员模范作用，积极开展档案各项业务管理工作，认真履行岗位职责，服从领导，听从指挥，尽职尽责、较好地完成了各级领导交办的各项任务。

四、工作方面

（1）完成了局各类档案立卷、归档、整理，档案规章制度的修订工作；

（2）配合海委顺利完成了我局档案管理系统试运行工作，实现了档案检索、档案借阅、档案在线收集归档、档案数据库管理等功能；可以全面实现我局档案管理工作网络化、电子化、网络在线查询、利用、浏览、下载等；进一步推进了我局档案管理的现代化水平。

五、存在问题

回顾一年来工作，虽然取得了一定的成绩，这主要是和各级领导的帮助和全科人员的共同努力支持分不开的，工作中还存在一定不足，主要表现在理论学习不够深入，对新知识、新技术掌握不够全面，有待于今后加强并不断提高自身各方面素质。

六、整改措施

金融业机构信息自查报告篇四

**********中心：

一、总体情况

（一）信息科技治理组织架构

1.强化“三会一层”履职。成立了以高管层和主要业务部门参加的信息科技管理委员会，定期或不定期履行职责，审议信息科技相关重大事件，本年度共计召开信息科技管理会议2次。

2.加大专业人员配备。设立首席信息官。参与我行与信息科技运用有关的业务发展决策，确保信息科技发展战略符合本行的总体业务战略和信息科技风险管理策略。

3.明确部门职责分工。明晰信息科技实施、风险管理及审计职责。信息技术部负责信息科技实施、管理工作，各支行设立兼职或专职计算机管理员，配合信息技术部开展应用推广、故障处理、设备维护工作；合规与风险管理部负责协调制定有关信息科技风险管理策略，尤其是在涉及信息安全、业务连续性计划和合规性风险等方面； 内部审计部负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划。

（二）信息科技管理制度建设

1.安全管理方面。对安全管理活动中的各类管理内容建立安全管理制度，制定了由安全策略、管理制度等构成的全面的信息安全管理总则《********商业银行行计算机信息安全管理办法》，安全管理办法经信息科技管理委员会审定，审定周期为一年一次，并且及时发现缺漏或不足对制度进行修订。

2.应急管理方面。建立了较为完善的信息系统应急管理办法《********商业银行行计算机信息系统应急管理办法》，明确应急管理组织机构和职责，对突发事件进行分级，确定风险防范措施，制定了各信息系统突发事件应急处置方案。对突发事件报告和应急响应也做了规定。2019年1月开展了全辖范围内的业务连续性应急演练，并对应急演练发现的问题进行整改。

3. 岗位职责与分工方面。信息技术部员工9人，人员配置能够满足当前业务发展的需要。按照科技管理、运行维护等条线设立岗位，重要岗位均配备a/b角。《********商业银行行计算机岗位人员管理办法》对相关岗位职责进行了规定。

4. 安全操作规范及管理流程。具备完整的信息安全管理流程，包括介质管理、网络管理、维护及故障处理制度、软硬件变更流程、备份管理□atm安全管理、机房管理、监控管理、密钥管理、巡检制度等科技管理流程。

三、信息技术管理情况

（一）网络安全管理

对自身网络安全管理情况进行现场检查，检查内容主要包括：内控制度；人员管理与访问控制；网络机房安全；网络接入安全；网络变更管理；网络应急管理；网络设备管理；日志与文档管理；第三方管理等方面。

根据文件要求，我行对重要网络设施进行了检查，总体管理有效，网络系统的组成结构及其配置合理。内控制度方面，我行制定《计算机网络管理办法》和《互联网管理及违规处罚办法》，明确管理机构和人员职责，确认网络设备安装和运维的具体工作措施，健全互联网使用规范。

日常管理方面，依托机房人员出入登记、门禁管理以及巡检值班制度，确保网络设备物理安全、运行稳定，所有网络设备均设置密码，且仅由网络管理员保管并定期修改登记。网络系统拓扑图、机柜标签、网络地址规划等网络运行资料已形成技术档案严格保密。网络设备的日志和开机运行配置由省联社建设的imc管理平台实现每周离机备份并永久保存，所有网络设备均纳入imc管理，网络管理员定期查询设备运行情况并处理系统告警信息。网络设备的接入和外联配置的变更，我行实行需求申请、有权人审批、网络管理员实施的流程管

理。实现内网安全方面，每台内网终端均安装杀毒软件，另切实抓好生产网络与其他网络的物理隔离，对生产网络实行严格保护。

自查发现：所有机柜均安装标签，部分网络机柜内线缆标签不够完善，目前已完成整改。另外我行内网接入核心路由器的主备无法自行切换，因涉及辖内所有网点网络运行，安全隐患凸显。该隐患已在省信息技术中心组织的2019年上半年h3c网络巡检中反馈。

（二）机房安全管理

对我行机房运行管理情况进行细致自查，自查内容主要包括：机房管理制度；机房基础设施管理；机房设备管理；机房人员出入管理；机房消防管理；机房巡检和故障处理等方面。

我行机房根据 《关于印发的通知》、《安徽商业银行行系统计算机机房管理办法》的相关规定，整改建设完成，日常运维管理工作按照《********商业银行行机房管理办法》严格执行。

基础设施管理，机房通过门禁控制实现物理访问控制，严防外部人员未经允许进入机房。供电系统均采用双路ups供电，线路冗余性好，负载能力强，能够满足机房电力需求。

空调系统的有效性。机房均配套防盗窃、防雷、防火、防水、防静电、温湿度控制、电磁保护等措施，以确保机房正常运转。机房消防管理严格贯彻“严防为主，防治结合”的方针，消防管理由信息技术领导具体负责，建立防火安全责任制做到值班人员“三懂”即懂火灾危害性，懂火灾的预防措施，懂灭火方法、“三会”，即会报警、会用消防器材、会补救明火。机房消防器材定期维护配备足量，定期开展消防演练。机房巡检工作由信息技术部当日值班人员每天进行4次，登记网络、电力、空调、设备等运转情况。机房同时采用集中监

控，参数实行24小时不间断监控，确保第一时间发现问题，处理问题。

自查发现：机房管理制度健全，基础设备配置齐全，设备管理、出入人员和巡检记录完整，机房管理有一定的应对消防灾情和故障处理的能力。目前我行机房受制与空间狭小，基础配置过于拥挤，没有通风系统。

（三）数据安全管理

制度方面，我行制定了《********商业银行行计算机信息系统数据管理办法》，对数据的使用和管理等做了比较细致的规定。

我行数据下发平台在省联社云服务器，主要用于存放省联社下发的数据。平台的用户管理方面□root用户由专人负责，密码定期修改并用保密信封封存；普通用户由数据管理员负责。自助取数平台的用户由数据管理员负责，目前主要用于省联社的一些业务数据分析和查询参考，不对外提供数据。

系统运行管理方面我行自建报表平台对数据下发情况进行监控和对数据进行校验。并自建定时任务对下发数据每天传输到异地进行备份，保证了数据的容灾备份。

数据的使用管理目前主要依托我行自建的报表查询系统供业务条线人员使用。

数据的存储保管、备份策略和有效性验证、清理等方面也都按照制度制定了详细的策略台帐。

（四）终端安全管理 1.终端采购选型情况

我行使用终端按照省联社选型范围采购，使用终端为升腾n610□升腾945w和国光ut3019f+□

2.防病毒软件安装

我行制定了《********商业银行行计算机病毒防治管理规定》，对所有内网终端均安装病毒查杀软件，保证杀毒软件全覆盖，及时更新病毒库，对病毒、恶意代码进行安全防护，对系统的有效性和完整性时行监督检查，定期组织员工举办病毒防治知识培训，对新病毒的传播和破坏机制进行跟踪，发现病毒及时采取清除措施。

3.重要补丁更新

及时关注系统安全漏洞最新情况，及时对新发现的安全漏洞打上相关的安全补丁，经检查当前系统已是最新版本，已安装了最新补丁。

4.网信安全主题教育或培训方面

我行积极开展网络安全、信息安全方面的宣传和培训，****4日开展信息科技培训，培训内容包括网络安全、病毒防治、信息安全等培训；****至26日我行开展科技活动周宣传活动，积极宣传网络、信息科技安全；****19日开展信息安全意识培训及考试，全面提升员工安全意识。

自查发现：内网杀毒软件病毒库更新只能离线更新，要做到及时更新，存在一定困难，建议省科技中心在杀毒软件总结点做联网更新，农商行联机更新病毒库。

（五）外包管理

对我行信息科技外包管理开展情况进行自查，内容主要包括：外包管理职责；外包制度执行；外包策略执行；外包项目立项管理；外包项目过程管理；外包项目风险管理；开发类外包管理；运维类外包管理；外包供应商入场管理；供应商日常管理；供应商评价管理；外包供应商安全管理；外包供应

商应急管理；外包人员入场管理；外包人员日常管理；外包人员安全管理。

我行已下发《********商业银行行科技外包管理办法》、《********商业银行行外包管理实施细则》、《********商业银行行外包商异常退出应急预案》其中明确了外包管理的组织架构与部门职责、外包项目管理、供应商管理与评价、人员管理、合同、实施、应急管理等内容，并认真落实日常管理工作。我行外包业务类型结构简单，大部分为采购产品的售后服务类和设备维护类外包。我行通过建立健全外包管理系统实现外包项目、供应商档案以及外包人员登记、管理工作，有效的解决了外包项目跟进难、供应商档案乱、人员管理无序等问题。

自查发现：外包管理系统的功能还不健全。外包项目更新还不及时，供应商的档案信息登记不完整的问题，人员管理中的安全培训的频次不足、培训内容单一等问题。

（六）应急管理

1.制定预案，成立组织

为保障本行信息科技系统能够安全、可靠、稳定运行，提高应对各类信息系统突发事件的能力，有效防范信息科技系统风险，妥善处置和应对信息科技突发事件，制定《**********商业银行商业银行计算机信息系统应急管理办法》、《********商业银行行业务连续性管理办法》等制度。

根据《********商业银行行计算机信息系统应急管理办法》成立信息系统应急管理领导小组，负责辖内信息系统应急管理工作，组建应急团队，在发生信息系统突发事件时，能够做到及时实施应急处置工作，应急团队包括应急领导小组、应急执行小组、支持保障小组。由行长担任应急领导小组组长，副行长为副组长，各相关职能部门为应急领导小组成员，

应急执行小组由信息技术部和相关业务部门主要负责人及涉及支行负责人组成，对应急领导小组负责，支持保障小组由办公室、人力资源、财务会计、合规与风险、监察保卫、电子银行等部门负责人组成。

根据《********商业银行行业务连续性管理办法》，成立以董事长为组长，行长为副组长，副行长为成员的业务连续性工作领导小组成，成立以董事长为组长，行长、副行长为副组长，其他职能部门负责人为成员的业务连续性工作协调保障小组，成立以分管信息科技的副行长为组长，其他职能部门负责人为成员的业务连续性工作执行小组。

2.开展培训，组织演练

为保障应急预案妥善实施，我行在1月份组织开展信息系统应急演练培训和演练，培训内容包括解读和说明应急演练的背景、意义，让全体员工意识后备电力和网络的支持是业务持续高速发展的核心基础和重要保障,熟知电力和网络的结构;能认识其相关部件并能正确说出其连接路径;能够将演习培训经验应用到实际应急处置中，坚持把演习工作常态化。演练内容包括:网点ups系统应急演练；网点发电机应急切换演练；网点主/备网络线路应急切换演练；总行主/备网络线路应急切换演练；总行主/备电力切换演练。通过信息科技培训和演练梳理网点应急处置流程，提升网点应急处置能力，妥善保障信息系统未定运行。

3.健全机制，预防为主

按照“预防为主、积极处置”的原则对辖内网点终端安装防病毒软件，并定期检查处理终端安全健康情况，对中毒设备及时进行网络隔离并进行病毒查杀。对离行式自助网点布设电力监控系统，监控市电及ups运行情况，出现故障及时通知网点人员、科技及监保部门，及时防范各类系统风险。

（六）其他

根据《********商业银行行信息科技风险管理办法》中职责分工，合规与风险管理部负责信息科技风险管理工作。每年按季开展信息科技风险排查工作，排查结果直接向分管理领导汇报，并提交高级管理层审查、审批，信息技术部负责具体的问题整改落实工作。内部审计部负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计。

截至到8月底，信息技术部共组织3批信息安全与网络安全培训，培训内容涵盖网络安全、病毒防治、信息安全，通过培训和宣传提升了我行员工的信息安全意识和安全防护技能。

********银行信息科技部

二〇一九年*月*日

金融业机构信息自查报告篇五

一、设备间建设规范和管理规范

（1）设备间安装了温湿度仪表，以用来监控机房温度和湿度，并能够及时开启控温控湿设备来保证机房的温度和湿度。

（2）设备间每周由网点经理或支行行长来对设备间的环境状况进行检查，并登记成册，以确保设备间保持整洁和规范。

（3）设备间严格控制出入人员，并保证营业网点外来人员有相关证件登记。

（4）支行技术人员每年一次对设备间的主要设备进行巡检，确保设备能够正常使用，并在相关登记本上记录。

二、应急管理和终端安全

（1）支行会不定期对一些预案进行检查，确保这些预案是最新的，且告知网点人员张贴在需要的地方。

（2）支行每年会抽取一定的网点人员进行培训和演练，并书写心得和体会，确保网点人员能够正确的应对突发状况。

（3）支行每月会不定期的抽查相关电脑的软件安装情况，检查是否存在私自安装不必要的软件，以及是否私自开通adsl等违规的网络。