ICS 35.240
L 67

SZJG

深 圳 经 济 特 区 技 术 规 范

SZJG 47-2014

金融机构信息技术外包风险管理规范

2014-01-06 发布　　2014-06-01 实施

深圳市市场监督管理局　发布

目　　次

前　言

本规范依据 GB/T 1.1－2009 给出的规则起草。

本规范由金融服务业标准联盟提出。

本规范由深圳市市场监督管理局归口。

本规范起草单位：深圳市金融信息服务协会、平安银行股份有限公司、中国平安保险(集团)股份有限公司。

本规范主要起草人：李绅、邹伟、张志远、董锐、韩梅、雷波。

本规范为首次发布。

引　言

随着信息技术的进步和信息技术外包环境的发展，外包逐渐成为各金融机构对内提供信息技术服务的一种重要形式，外包范围更是从简单的设备维护外包、人力外包到相对复杂的灾备中心及数据中心整体外包、整体项目开发外包，再到全面的信息技术服务外包。信息技术外包风险已是金融机构信息技术风险的重要组成部分，因此信息技术外包风险的管控也应纳入金融机构风险管控之中。

为引导深圳市金融服务机构以及为其提供信息技术服务的供应商规范信息技术外包活动，防范金融业信息技术外包风险，依照中国银行业监督管理委员会印发的《商业银行信息科技风险管理指引》（银监发[2009]19 号）、《银行业金融机构外包风险管理指引》（银监发[2010]44 号）、《银行业金融机构信息科技外包监管指引》(银监发[2013]5 号)、中国保险监督管理委员会印发的《保险公司信息系统安全管理指引（试行）》（保监发[2011]68 号）、中国证券监督管理委员会印发的《证券期货业信息安全保障管理办法》(中国证券监督管理委员会令第 82 号)等有关监管规定，制定本规范。

金融机构信息技术外包风险管理规范

1 范围

本规范规定了金融机构信息技术外包风险管理的总体要求、管理职责、管理制度、评估与决策、服务提供商选择、外包合同管理、持续监控管理、跨境外包与审计。

本规范适用于深圳市金融服务机构以及为其提供信息技术服务的供应商。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19000-2008 质量管理体系 基础和术语 (ISO9000:2005，IDT)

GB/T 19001—2008 质量管理体系 要求 (ISO9001:2008，IDT)

GB/T 22080-2008信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2005，IDT)

GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则 (ISO/IEC 27002:2005，IDT)

SZDB/78-2013 金融机构信息技术服务外包质量管理规范

3 术语和定义

下列术语和定义适用于本规范。

3.1

金融机构信息技术外包

金融机构将价值链中原本由自身提供的信息技术业务剥离出来，委托给信息技术服务提供商来完成的经济活动，包括开发、应用信息技术的服务，以及以信息技术为手段支持金融机构业务活动的服务。

注：常见的外包服务形态有信息技术咨询服务、设计与开发服务、信息系统集成服务、数据处理和运营服务及其他信息技术服务。

3.2

信息技术外包服务提供商

向一个或多个金融机构提供信息技术服务的组织，包括独立第三方、金融机构母公司或其所属集团设立在中国境内外的子公司、关联公司或附属机构。

注：为描述方便，本标准中简称为“服务提供商”。

3.3

信息技术外包风险

在信息技术外包活动中因信息对称、道德、管理等方面的不确定性而对金融机构相关信息技术外包活动造成的战略、声誉、合规、操作等方面的影响。

3.4

跨境外包

在境外其他国家或地区实施的信息技术外包活动。

4 总体要求

4.1 金融机构应根据内外部的环境和市场状况拟定其信息技术外包的发展规划、策略，明确信息技术外包的范围，确定信息技术外包风险的可接受水平。

4.2 金融机构可按照服务外包的性质和重要程度对信息技术外包服务提供商进行分级管理，对不同级别的服务提供商采取差异化的管控措施，在有效管理重要风险的前提下降低管理成本。

4.3 金融机构在实施信息技术外包时，不得将信息科技管理责任外包。

5 管理组织与职责

信息技术外包风险的管理组织架构包括董事会（或对应的最高决策层）、高级管理层、信息科技外包管理团队及内部审计部门。

5.1 董事会（或对应的最高决策层）的职责：

a） 审议批准信息技术外包的战略发展规划；
b） 审议批准信息技术外包风险管理的政策、操作流程和内控制度；
c） 审议批准本机构的外包范围及相关安排；
d） 定期审阅本机构外包活动的有关报告；
e） 定期安排内部审计，确保审计范围涵盖所有的外包安排。

5.2 高级管理层的职责

高级管理层的职责主要包括以下方面：

a） 制定信息技术外包战略发展规划；
b） 制定信息技术外包风险管理的政策、操作流程和内控制度；
c） 确定信息技术外包业务的范围及相关安排；
d） 确定信息技术外包管理团队职责，并对其行为进行有效指导、管理和监督。

5.3 管理团队职责

信息技术外包管理团队通常包括来自信息技术外包需求、信息技术管理、信息技术风险管理及法律等部门或单位，金融机构应根据实际情况明确外包管理团队中各单位的具体职责分工，外包管理团队职责主要包括以下方面：

a） 执行外包风险管理的政策、操作流程和内控制度；
b） 负责外包活动的日常管理，包括外包需求分析、尽职调查、合同执行情况监督及风险状况的监控等；
c） 向高级管理层提出有关外包活动发展和风险管控的意见和建议；
d） 发现服务提供商业务活动存在缺陷时，采取及时有效的措施；
e） 高级管理层确定的其他职责。

6 管理制度

6.1 金融机构应根据其信息技术外包策略制定信息技术外包管理制度、流程，建立信息技术评估与决策、服务商选择、合同管理、外包服务监控、外包服务中断与终止管理的机制。

6.2 金融机构应定期对信息技术外包工作的实施成效进行全面评价和总结，并据此对信息技术外包策略、制度、流程进行检视和完善，确保其有效性和可行性。

6.3 金融机构应建立全面的外包风险评估、控制机制，将信息技术外包风险纳入金融机构的风险管理体系进行全面管理。信息技术外包风险的管理组织架构包括高级管理层、信息技术外包管理团队及内部审计部门，高级管理层承担外包活动的最终管理责任。

7 评估与决策

金融机构应有明确的信息技术外包需求形成、信息技术外包评估决策的流程，并建立适当的信息技术外包项目风险评估程序、标准以及对应的风险级别，对于持续性的重要信息技术外包项目，金融机构应定期对其进行风险评估，以确保考虑到信息技术外包项目的风险变化情况。

7.1 外包前调研

在开展信息技术外包前，金融机构应对外包项目的可行性、风险情况等进行调研,并根据调研结果及收集到的信息进行评估确定相应的风险级别。

7.2 评估阶段的风险控制

7.2.1 金融机构应确保评估阶段所发现的风险在实施外包前已得到妥善的处理或采取了相应的风险控制措施。

7.2.2 金融机构在实施外包管理时，应根据信息技术外包项目的风险级别及所涉及业务的重要性进行考虑，对于不同风险级别的信息技术外包项目，采取不同的风险规避及外包管理措施。

7.2.3 金融机构信息技术外包相关决策人员应根据评估结果及相应风险级别对拟外包的工作进行明确的审批，高级管理层应格外关注重要信息技术外包项目。

7.3 风险评估所要考虑的因素

在进行信息技术外包项目风险评估时，应考虑但不限于以下因素：

a) 拟外包工作的交易量以及对于金融机构的重要性、关键性；
b) 拟外包工作涉及数据的敏感性及是否涉及到客户信息处理的转移；
c) 潜在服务提供商的专业水平、风险管理水平及可持续服务能力；
d) 金融机构对于拟外包工作的评价和监控能力；
e) 服务提供商未能按要求完成外包工作时对金融机构的财务、声誉、经营造成的影响；
f) 外包服务意外中止时对于金融机构的影响以及可能的应急处理措施；
g) 其他认为需要关注的重要事项。

7.4 重要信息技术外包项目

对于重要的信息技术外包，金融机构应谨慎处理，并加以特别的关注和管理，重要信息技术外包包括但不限于以下项目：

a) 信息技术工作整体外包；
b) 数据中心、灾备中心整体外包；

c) 涉及将金融机构客户资料、交易数据等敏感信息交由服务提供商进行分析或处理的信息技术外包；
d) 以非驻场服务形式实施的、涉及集中存储客户数据的业务交易系统外包；
e) 信息安全审计；
f) 跨境外包；
g) 其他一旦外包服务意外终止，短时间内就有可能对金融机构的业务运营、管理、声誉或者安全产生严重、显著影响的外包安排；
h) 其他在评估阶段被金融机构认为是高风险级别的信息技术外包项目；
i) 其他金融监管机构认为是重要信息技术的外包项目。

7.5 外包需求涉及要素

在建立信息技术外包需求时，应考虑但不限于以下要素：

a) 拟外包工作的范围；
b) 外包服务水平的要求以及外包工作的标准；
c) 服务提供商的最低要求；
d) 外包监控和报告要求；
e) 服务开始及服务中止时过渡安排；
f) 合同的期限、终止和转让；
g) 赔偿、保险等合同责任条款方面的要求。

7.6 外包需求的形成

在实施信息技术外包前，金融机构应形成明确、清晰、正式的信息技术外包需求文档。信息技术外包需求应由金融机构内与信息技术外包相关的各方参与形成，并应考虑到风险评估阶段的风险控制需求。

8 服务提供商选择

8.1 在进行信息技术外包项目风险评估以及外包决策后，金融机构应对待选的服务提供商进行适当的调查，评估服务提供商业务及财务等能力是否满足金融机构外包的要求。

8.2 在对服务提供商进行尽职调查时，应考虑但不限于以下因素：

a) 在满足金融机构需求所需的服务及支持技术方面的经验和能力；
b) 在金融机构拟外包工作领域上的行业地位以及经验；
c) 经营声誉及企业文化；
d) 其指派的为机构提供服务的主要岗位人员的技能、经验、稳定性等情况；
e) 对于服务中断的应急处理能力；
f) 在拟外包工作方面的内部控制情况；
g) 在拟外包工作方面信息安全管理情况；
h) 对金融行业的熟悉程度；
i) 对其他金融机构提供服务的情况；
j) 财务状况。

8.3 对于重要的信息技术外包，必要时金融机构可考虑采取以下措施了解服务提供商如何运营及支持拟外包的业务，调查其与外包业务相关的内部控制和信息安全管理能力：

a) 指派内部人员开展现场调查；
b) 要求服务提供商提供相关独立的专业第三方机构完成的信息安全审查、内部控制审查、财务审计报告；

c） 邀请独立的专业第三方机构对服务提供商就信息技术外包领域的相关情况进行调查。

8.4 对于服务提供商为金融机构的母公司或其所属集团设立在中国境内、外的子公司、关联公司或附属机构的关联外包，金融机构不得因关联关系而降低对服务提供商的要求，应当在服务提供商选择阶段详细分析服务提供商技术、内控和管理水平，确认其有足够能力实施外包服务、处理突发事件等。

8.5 对于持续性信息技术外包项目，金融机构应定期对服务提供商进行调查，确保在服务期内服务提供商均能达到其要求。

9 外包合同要求

9.1 金融机构应建立正式的信息技术外包合同草拟、审定及审批流程，确保信息技术外包合同描述清晰、覆盖全面、权责明确，并经过正式的审定、批准。

9.2 金融机构开展信息技术外包活动时应当与服务提供商签订书面合同或协议，并根据外包服务需求、风险评估及尽职调查结果确定其详细程度和重点，以明确双方的权利义务，在签订合同或协议时应考虑但不限于以下范围：

a） 信息技术外包服务的内容和方式。包括但不限于金融机构要求服务提供商实施的具体工作及时限，交付物要求、配套服务要求，变更服务内容的权力及途径等；

b） 绩效标准。包括但不限于最低服务级别要求以及当不能满足合同要求时的处理措施；

c） 信息技术外包服务的安全性及保密性的安排。包括但不限于要求服务提供商按照“必须知道”和“最小授权”原则对相关人员授权、与服务提供商签署保密协议或保密条款、禁止服务提供商非授权披露或使用金融机构及其客户的信息、及时向金融机构报告安全漏洞或安全事件、要求服务提供商督促包括其员工、临时工、代理等在内的相关人员遵守保密规定等；

d） 对服务提供商的控制要求。包括但不限于法律法规的遵从要求、监管制度的通报贯彻机制、对服务提供商内部控制的基本要求、金融机构访问服务提供商工作记录的要求、对服务提供商技术及管理上重要变动的通知及审批要求、沟通及报告机制的要求等；

e） 外包服务的审计和检查要求。包括但不限于金融机构有权收到的审查报告的种类、对服务提供商审计或检查的开展频率和方式、对服务提供商日常外包服务工作检查的权力及方式、金融机构及其监管机构开展相关审查及获得审查结果的权力和基本流程等；

f） 信息技术外包的费用安排。

g） 信息技术外包服务的报告要求；

h） 知识产权及信息所有权的约定；

i） 外包服务的业务连续性安排；

j） 包括通知、审批在内的分包相关约束要求及转包的限制条款；

k） 合同的期限、合同终止的条件以及合同终止或变更时的过渡安排；

l） 争端的解决机制；

m） 罚则及充分的赔偿要求。

9.3 金融机构应在外包合同或协议中明确要求服务提供商承诺以下事项：

a） 定期通报外包活动的有关事项，及时通报外包活动的突发性事件；

b） 配合金融机构接受相关监督管理机构的检查；

c） 及时根据金融机构要求以认可的方式改正及改进检查中发现的问题及不足；

d) 保障客户信息的安全性，当客户信息不安全或客户权利受到影响时，金融机构有权随时终止外包合同；
e) 不得以金融机构的名义开展活动；
f) 不得将外包服务转包或变相转包，不将外包服务主要业务分包。对于存在分包情况的，主服务提供商需对服务水平负总责，承诺对分包商进行监控，并对分包商的变更履行通知或报告审批义务，以确保分包服务提供商能够严格遵守外包合同或协议。

9.4 金融机构在进行信息技术外包时应当根据其预先确认的服务要求与服务提供商签订服务水平协议，签订服务水平协议时应考虑但不限于以下因素：

a) 外包服务的关键要素；
b) 服务时效以及可用性；
c) 数据的机密性和完整性；
d) 变更的控制；
e) 安全标准的遵守情况；
f) 业务连续性的遵守情况；
g) 技术支持水平。

9.5 金融机构应注意监管法律、法规、规章和规范性文件的规定等对外包工作产生影响的外部环境和市场的变化情况，并视其必要性及时对外包合同及相关协议进行调整。

10 持续监控管理

金融机构应建立适当的信息技术外包监控程序，以确保金融机构能够了解到外包相关的风险变化情况并确保服务提供商按照合同要求提供相符合的信息技术服务。

10.1 外包监控程序内容

在建立信息技术外包监控程序时，金融机构可考虑但不限于以下因素：

a) 服务水平协议的有关要求；
b) 合同中的一些关键要素；
c) 外包监控开展的方式和频率；
d) 监控结果的报告流程；
e) 出现问题时的升级流程；
f) 实施外包监控时与服务提供商的争议解决程序；
g) 跟踪服务提供商对外包服务进行改进的措施；
h) 服务终止程序。

10.2 外包监控管理

10.2.1 信息技术外包的监控可根据所外包服务的重要性、复杂性和风险情况有所不同，但金融机构应确保外包监控覆盖了信息技术外包合同中的一些关键要素，对于重要的信息技术外包项目，金融机构应格外关注，并采取更严格的监控措施。

10.2.2 金融机构应根据外包需求、外包合同、服务水平协议等建立明确的信息技术外包服务质量监控指标，监控指标根据所外包的服务内容的不同而有所差异，但应通过这些监控指标能够监控到服务提供商外包服务的情况，以下是一些常见的服务监控指标：

a) 信息系统或设备及基础设施的可用率、设备的开机率；
b) 故障次数、故障解决率、故障响应时间；

c) 服务的次数、服务的客户满意度；
d) 业务需求的及时完成率、程序的缺陷数；
e) 外包服务的总人时、外包人员的考核质量、外包人员的离职率。

10.2.3 金融机构应对服务提供商的财务状况进行监控，监控的形式以及水平可根据信息技术外包项目的重要程度及风险级别有所不同，但应能够了解到服务提供商财务状况的严重下降以及恶化的情况，并根据其严重程度采取相应的措施，以避免重要的信息技术外包项目因服务提供商破产、兼并、关键人员流失、投入不足等而意外中断或服务质量急剧下降。

10.2.4 金融机构应采取措施对服务提供商的分包或转包情况进行持续的监控，应要求服务提供商就信息技术外包工作中存在的分包或转包实施情况进行定期报告。对于重要的信息技术外包项目，必要时，金融机构应根据事先约定的外包合同要求对服务提供商的相关分包或者转包行为进行审批和监控。

10.2.5 金融机构应对相关服务提供商就其所提供外包服务领域的信息安全及内部控制情况进行检查或审计，确保其符合机构在安全性及保密性上的要求。根据信息技术外包项目的重要程度及风险情况，检查或审计工作可选择但不限于以下形式：

a) 要求服务提供商定期向金融机构就外包工作相关的信息安全及内控情况做出报告，并要求其承诺对报告的真实性负责；
b) 要求服务提供商指派符合资质的内部人员开展相关审查工作，并及时向金融机构提供有关报告。采取这一形式时，金融机构关注服务提供商内部审查人员的技术水平、专业经验、履职能力及审查的独立性；
c) 要求服务提供商邀请专业第三方机构开展相关审查工作，并及时向金融机构提供有关报告；
d) 金融机构指派内部专业人员或邀请外部专业第三方对服务提供商就信息技术外包相关领域的信息安全及内部控制情况进行审查。

10.2.6 对于关联外包，金融机构最高决策层应当推动母公司或所属集团将外包服务质量纳入对服务提供商的业绩评价范围，建立外包服务重大事件问责机制。同时，应要求服务提供商在其内部建立与外包服务水平相关的绩效考核。

10.3 外包监控问题的处理

10.3.1 金融机构应建立适当的机制确保能够与服务提供商就外包监控中发现的问题进行讨论、升级及处理，对于信息技术外包监控中发现的问题，金融机构应根据问题对外包服务的影响采取必要措施，以确保其得到适当的处理。

10.3.2 金融机构对于信息技术外包监控中发现的问题，应采取措施通常包括但不限于：

a) 与服务提供商进行定期的沟通，就问题进行讨论，协助及督促服务提供商进行问题整改；
b) 视问题的重大程度，根据有关监管要求向监管部门进行报告；
c) 根据问题的性质依据预案启动外包应急处理措施；
d) 根据合同规定实施罚则；
e) 根据合同规定终止外包服务，并做好过渡期的安排。

10.4 外包的中断与终止

10.4.1 为降低外包突发事件的可能性及影响，对于会对业务连续性管理造成重大影响的外包服务，金融机构应事先建立风险控制、缓释或转移措施，包括但不限于以下内容：

a) 在外包服务实施的过程中持续收集服务提供商相关信息，尽早发现可能导致服务中断的情况；
b) 与服务提供商事先约定在意外情况下购买其外包服务资源的优先权；
c) 要求服务提供商制定服务中断相关的应急处理预案，如提供备份人员；
d) 对于涉及重要的业务的外包服务，金融机构需考虑预先在其内部配置相应的人力资源，掌握必要的技能，以在外包服务中断期间自行维持最低限度的服务能力。

10.4.2 金融机构应针对重要外包服务中断的场景，拟定相应的应急计划,应急计划应考虑的因素包括但不限于以下内容：

a) 事件场景，如重要人员流失导致服务无法持续，服务提供商主动退出，因资质变更、被收购、兼并或破产等原因导致的服务提供商被动退出等；
b) 事件持续时间和恢复可能性；
c) 事件影响范围和可能的应急措施；
d) 服务提供商自行恢复服务的可能性和时间；
e) 备选的服务提供商以及外包服务迁移方案；
f) 外包服务过渡给金融机构自行运作的可能性、时效及资源需求。

10.4.3 对于会对金融机构重要业务连续运行带来影响的重要信息技术外包,金融机构应有针对性的完善业务连续性管理计划，包括但不限于：

a) 识别出重要业务所涉及的服务提供商和资源；
b) 通过合同协议等形式明确要求服务提供商提前准备并维护好相关资源；
c) 对服务提供商业务连续性管理进行监控，并评价其管理水平；
d) 在进行业务连续性计划演练时将相关的服务提供商纳入演练范围。

10.4.4 在服务提供商无法满足外包服务要求或引发重大事件时,金融机构应当在充分评估退出影响及制定退出计划的前提下，考虑主动要求外包服务提供商终止服务。

11 跨境外包

11.1 跨境外包除具有本指引前述风险外，还包括由于某一国家或地区经济、政治、社会变化及事件而产生的国别风险，及由于外包实施场地远离金融机构而产生的非驻场风险，金融机构应采取措施控制由于跨境外包而发生的额外风险。

11.2 金融机构应当充分了解并持续监控服务提供商所在国家或地区状况,通过建立业务连续性计划防范跨境外包所带来的国别风险。

11.3 金融机构应关注国外监管法律、法规和监管要求对其获取服务提供商外包管理信息可能造成的影响。实施跨境外包应以不妨碍金融机构有效履行外包服务监控管理职能及监管机构延伸检查为前提。

11.4 金融机构在选择跨境外包时，还应充分审查评估服务提供商保护客户信息的能力，并将其作为选择服务提供商的重要指标。涉及客户信息的跨境外包，应当在符合监管法律、法规、规章和规范性文件的规定并获得客户授权的前提下开展。

11.5 金融机构在实施跨境外包时，其合同应包括法律选择和司法管辖权的约定，明确争议解决时所适用的法律及司法管辖权，原则上应当要求服务提供商依照中国的法律解决纠纷。

12 审计

12.1 金融机构内部审计部门应将信息技术外包纳入信息技术审计的范围内,并配备足够的资源和具有专业能力的审计人员开展信息技术外包审计工作。

12.2　金融机构内部审计部门应根据信息技术外包的性质、规模及复杂度对信息技术外包的管理制度及流程的适当性、有效性及执行情况进行审计和评价。

12.3　对于重大的外包项目，金融机构内部审计部门应进行专项审计，审计范围包括但不限于外包的评估及决策过程、外包合同、外包服务的监控管理、服务提供商的履约情况等。

12.4　金融机构内部审计部门应对外包管理相关部门的履职情况进行审计，推进金融机构各职能部门加强信息技术外包的风险管理工作，降低重大外包项目的风险。

12.5　金融机构可以在符合监管法律、法规、规章和规范性文件的规定的情况下，委托具备相应资质的外部审计机构进行信息技术外包管理的外部审计。