**金融企业IT内控合规管理建设与实践**

IT内控合规是广义信息安全的一部分，而且是管理体系中很重要的一环，在近三年的IT内控合规管理工作经历中，总结出如下落地方法：外规对内规、内规对检查、检查对整改、整改对考核。金融企业如何做好IT内控合规管理建设，本文尝试做一些探讨。

## **写在前面**

安全领域众多，企业安全团队负责人关注的是企业安全最后一公里的问题，偏重于安全有效性和最佳实践，因此本专栏文章偏理论的讨论少一些，偏实践的多一些，这样给大家的实际工作帮助可能更大一些。互联网公司安全为什么能一定程度引领行业发展，还是因为从解决实际问题出发，很多看起来并不是高大上的话题，但却是解决企业实际问题必须的。吾生有涯而学无涯，把有限的精力投到快速解决实际问题上去。

金融行业是牌照行业，接受严格的监管，典型特征是各项业务开展以及IT发展，必须遵守各项管理规定，合规是金融企业的底线和最低要求。同时为落实监管规定，以及企业内部各项管理要求，内部控制（简称“内控”）相对其他行业要求高出不少。在大型金融机构（如全国性商业银行、股份制银行、交易所、大型证券公司等），IT内控合规是广义信息安全的一部分，而且是管理体系中很重要的一环，金融企业如何做好IT内控合规管理建设，本文尝试做一些探讨。

## ****一、总体介绍****

### **1.1 合规、内控、风险管理的关系**

没有绝对的区分。合规管理是最基础的层面，合规管理的目标是避免违反内外部法律、制度、规范，避免因不合规导致的风险。内控比合规管理更进一层，内控不但要求合规，还要审视“规”是不是完善，“规”有没有配备相应的执行点，执行“规”的过程是不是有效。风险管理，特别是全面风险管理是风险管控的最高形式，风险按标准划分为市场风险、信用风险、流动性风险、操作风险、法律风险。合规、内控只是操作风险管理的手段。大部分金融企业会设置首席风险官，属于公司高级管理层。

虽然一般意义上：风险管理>内控>合规，但由于企业习惯将风险管理及其所包含的内控、合规活动统称为内控合规管理，故本文所称内控合规是指围绕风险管理的一系列管理活动。由于从业经历所限，本文只探讨IT内控合规管理。

### **1.2 目标及领域**

金融企业IT内控合规的目标是通过建立有效的机制，实现对金融企业IT风险的识别、计量、监测和控制，对外保障IT活动符合监管层各项管理要求，对内确保各项管理要求落地和控制措施有效，最终实现IT风险可控。

实践中IT内控合规管理领域包括：信息科技风险管理、监督检查、制度和公文管理、业务连续性管理、信息科技外包管理、分支机构管理，以及其他一些工作（比如写信息技术部工作总结？）。

根据不同企业对IT内控合规的定义理解，管理的领域可能会有一些不同。

很多企业内IT内控合规管理的岗位给人的印象就是“写报告”的，这种说法比较通俗易懂，怎么写好报告还是需要能力、知识、技能和逻辑架构功底，有很大技巧的，难以写一份好报告是阻碍绝大多数安全负责人职位更进一步的主要原因。怎么写好报告不在本文探讨。

### **1.3 落地方法**

在近三年的IT内控合规管理工作经历中，总结出如下落地方法：****外规对内规、内规对检查、检查对整改、整改对考核****。

* 外规对内规。将外部规范要求分解成元要求，去重合并，和内部规范一一对应，每条元要求对应的结果为四者其一：1、满足要求；2、冲突；3、缺失。如果是2、3两种情况，要么修订内部规范，要么增加内部规范，以满足外规要求。通过识别，外部规范分解成9大类、52小类、1249条元要求，去重合并后形成外规内规对应关系。外规对内规的梳理过程中发现了部分外规元要求没有内规承接和冲突的情况。
* 内规对检查。依据监管要求、外部标准梳理出内部规范后，建立了一套适用的检查标准，并进行全面覆盖的检查，包括常规检查、专项检查和事件驱动检查。具体内容见第三章监督检查。
* 检查对整改。建立了一套电子化系统，实现检查计划制定、检查实施、报告管理、问题跟踪等全过程的电子化管理。检查发现和整改情况纳入问题管理流程。
* 整改对考核。检查发现和整改情况纳入团队和个人当月和年度考核，实实在在影响个人收入。

我看到较多大型金融机构如银行建立了外规条款数据库，并可以根据关键字进行快速检索查询，供内部使用，取得不错的效果。

## ****二、信息科技风险管理****

银监会发过《商业银行信息科技风险管理指引》，证监会（包括协会）发过《证券期货经营机构信息技术治理工作指引(试行)》、《证券期货经营机构信息技术治理工作指引(试行)》，对信息科技风险管理有明确管理要求。

注：银行业“信息科技”的提法较多，证券基金期货“信息技术”的提法较多，本文未做严格区分。

### **2.1 总体介绍**

2.1.1 信息科技风险定义

信息科技风险是指在运用信息科技过程中，由于自然因素、人为因素、技术漏洞或管理缺陷产生的操作、法律和声誉等风险。

**2.1.2 管理原则**

（1）事前预防为主原则。在风险发生以前建立有效的风险管理措施，降低风险发生的可能性或减少风险可能造成的损失。

（2）全面性原则。信息科技风险管理应覆盖到全行各部门、岗位、人员及操作环节中，使信息科技风险能够被识别、评估、计量、监测和控制。

（3）成本效益原则。对风险管理措施的实施成本与风险可能造成的损失进行分析比较，选取成本效益最佳的风险控制方案。

**2.1.3 风险偏好与容忍度**

需要根据董事会设定的风险偏好进行，在成本效益原则下，最大限度的完善信息科技风险管理体系，保障IT长期、稳定、健康的发展。

### **2.2 组织架构和职责**

信息科技风险管理组织架构示例如下：

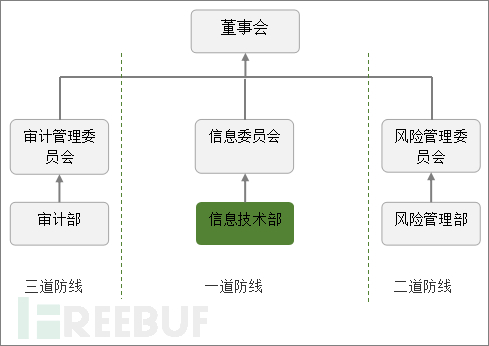
[](https://image.3001.net/images/20180429/15250071072534.png)

图1：信息科技风险管理组织

简单介绍下金融机构信息科技三道防线设置，一般商业银行提三道防线的概念比较多，其他证券保险基金期货用此概念较少，但实际部门组织架构和岗位职责设置类似。

**2.2.1 第一道防线：信息科技部门**

* 主要关注日常的风险管理
* 识别、分析与评估、控制、监测及报告风险管理情况。
* 信息技术部门各团队严格执行各项风险管理政策和要求，定期评估。

**2.2.2 第二道防线：风险管理部门**

* 侧重制定风险管理政策、制度、流程，在第一道防线的基础上对风险进行集中管理。
* 在总部层面设立风险职能部门，监督和协调整个风险管理框架的有效性和完整性，与前台部门保持相对独立。
* 对IT条线提供精细化的风险管理策略和支持。

**2.2.3 第三道防线：稽核审计部门**

* 按期进行审计或稽核，与IT部门和风险管理部门保持独立，对风险管理框架、内控体系的完整性和有效性提供独立的审计发现和管理意见。

注意：一道防线和二道防线向经营管理层汇报和负责，而稽核审计部门一般直接向董事会汇报和负责，保持独立性。

### **2.3 管理内容**

**2.3.1 IT治理**

形成分工合理、职责明确、相互制衡、报告关系清晰的信息科技治理组织结构，为公司信息科技的发展提供战略方向和资源保障，并保证信息科技的战略与全行业务战略目标相一致。

**2.3.2 信息安全**

建立信息安全管理策略，技术措施，确保所有计算机操作系统和系统软件的安全，并进行必要的员工培训。这部分内容就是狭义的信息安全内容。

**2.3.3 信息系统开发、测试和维护**

信息科技部门应针对信息系统需求分析、规划、采购、开发、测试、部署、维护、升级和报废环节，建立管理制度和流程，管理信息科技项目的排序、立项、审批和控制，并持续监控重大信息科技项目的进展情况。

**2.3.4 信息科技运行**

信息科技部门应对人员职责分配、数据保存、操作方法、服务水平、变更、故障、性能及容量管理，建立制度和流程，并对信息科技突发事件建立应急处置预案，严格执行突发事件报告制度，落实突发事件的处置职责。安全保卫部门负责信息系统机房的物理环境安全管理。

**2.3.5 业务连续性管理**

公司各相关机构应建立恢复服务和保证业务连续运行的管理机制和备用方案，并定期对其进行检查和测试，保证在业务运行中断时可以快速启动备用方案，降低业务中断带来的影响。信息科技部门负责信息系统灾难恢复方案制定、实施和维护。

**2.3.6 外包管理**

信息科技部门负责管理信息科技相关的外包业务，制定与信息科技外包业务有关的管理政策，保证信息科技外包服务有协议、服务合同和监督机制约束。

**2.3.7 内部审计**

审计部门应根据信息科技风险所涉及活动的性质、规模和复杂程度、信息科技应用情况以及信息科技风险评估结果，决定信息科技审计范围和频率，对信息科技风险管理的适当性和有效性进行审计和评价，向董事会提供独立的信息科技风险审计意见。审计部应至少每三年进行一次全面的信息科技风险审计；公司在进行重大系统开发时，审计部门应参与其中，保证系统开发符合公司的信息科技风险管理要求。

**2.3.8 外部审计**

公司根据需要在符合法律、法规和监管要求的情况下，可以委托具备相应资质的外部审计机构进行信息科技外部审计。在委托外部审计机构进行外部审计时，应与其签订保密协议，并督促其严格遵守法律法规，保守公司的商业秘密和信息科技风险信息。

### **2.4 管理手段和流程**

**2.4.1 管理手段**

信息科技风险隶属于操作风险，管理手段一般遵从二道防线风险管理部门的管理手段。实际中，无论是银行还是证券，都会按照二道防线下发的操作风险管理三大工具和要求开展工作。简单介绍下三大工具:

操作风险管理三大工具，包括风险与控制自我评估（RCSA）、损失数据收集（LDC）和关键风险指标（KRI）。三大工具贯穿操作风险管理始终，为高效率、系统化的操作风险管理提供帮助。通常采取信息科技风险与控制自我评估、设置信息科技关键风险指标、信息科技风险监控报表三种手段对信息科技风险进行管理。

（1）信息科技风险与控制自我评估（RCSA），是识别和评估信息科技风险及风险控制措施有效性的管理手段。各相关部门应按照预先设定的工作方法，对其职责范围内的信息科技风险管理现状进行评价。信息科技风险与控制自我评估是信息科技风险管理持续改进的基础工作和关键环节。

（2）损失数据收集（LDC），操作风险事件及损失数据收集是指依据监管规定、内部操作风险偏好与管理需求所定义的收集范围，针对操作风险事件的相关信息进行数据收集、内容分析、整改方案设计与执行、损失分配和内外部报告等程序。通过持续开展损失数据收集，一方面可以动态反映企业操作风险损失的分布情况及发生诱因，为有效识别评估操作风险和强化管理提供线索和方向；另一方面可以逐步建立操作风险损失数据库，为今后进行风险建模和计量积累数据。最终达到提高操作风险管理水平、降低风险损失的目的。

（3）信息科技关键风险指标（KRI），是反映信息科技风险水平的一系列统计指标，具有可量化的特点。关键风险指标用于监测可能造成重大信息科技风险事件的各项风险及控制措施，并作为反映风险变化情况的早期预警指标。通过对主要风险类型的早期预警并及时采取应对措施，避免重大信息科技风险事件的发生。

同时通过信息科技风险监控报表，定期汇总分析监控报表，能够获取信息科技风险情况，并能掌握到总体风险变化趋势。

**2.4.2 管理流程**

公司的信息科技风险管理流程包括信息科技风险识别、分析与评估、控制、监测及 ：

（1）风险识别

信息科技风险识别是指对公司具有脆弱性，可能受到威胁侵害，需要保护的信息资源或资产进行识别和分类，并对相关的威胁和脆弱性进行确认的过程。风险识别是风险管理的第一步，也是风险管理的基础。信息科技风险具有一定的可变性，风险识别是一项持续性和系统性的工作，各相关单位应密切注意原有风险的变化，并随时发现新的风险。

（2）风险分析与评估

信息科技风险分析是指对风险的可能性及其发生以后所造成的影响进行综合度量。信息科技风险评估单位应通过定性或定量的评估方法，判断风险的影响程度和发生可能性，确定风险的等级。

（3）风险控制

信息科技风险控制指根据公司的风险偏好及风险评估的结果建立相应的风险管理措施。通过建立事前预防、事中监控及事后复核的风险管控手段降低风险发生的可能性及其造成的影响，并根据公司的信息科技风险容忍程度采取规避、降低、转移风险的方式，将风险控制到公司可接受的水平之内。

（4）风险监测

信息科技风险监测是指对信息科技风险进行定期或持续的检查，及时发现新出现的信息科技风险以及风险管理措施出现的问题，并采取相应的补救措施，以保证公司的信息科技风险在不断变化的内外部环境中，始终处于公司的风险容忍水平之下。应定期通过风险评估和审计等方式对风险的发展与变化情况进行持续监测，并根据需要对风险应对策略进行调整。

（5）风险报告

信息科技风险报告指信息科技部门、风险管理部门和审计部门依据特定的格式和程序对信息科技风险状况进行描述、分析和评价，并形成的信息科技风险报告，相关部门按照规定的报告路线进行汇报。报告的内容应完整、客观、清晰。

### **2.5 报告机制**

需要建立信息科技风险报告机制，遵循以下原则：

* 逐级上报。
* 按IT业务条线及风险管理条线双线汇报。

信息技术部门、风险管理部门和审计部门分别按照以下汇报路径，向高级管理层和董事会报告全行信息科技风险状况和重大信息科技风险事件：

* 信息技术部门负责定期向高级管理层下设的风险控制委员会报告信息科技风险管理工作情况；
* 风险管理部门负责定期向董事会下设的风险与资本管理委员会报告信息科技风险状况；
* 审计部门负责定期向董事会下设的审计委员会报告信息科技审计情况。

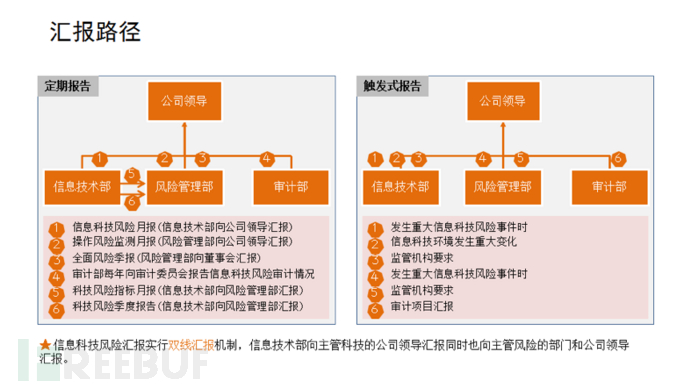
[](https://image.3001.net/images/20180429/1525007185551.png)

图2：汇报路径示例

1. 定期报告：信息技术部门向主管IT的公司领导汇报信息技术风险管理月报，向二道防线、三道防线汇报IT风险管理和IT内外部审计情况。
2. 触发式报告：由信息技术部在：

* 发生重大信息科技风险事件；
* 信息科技环境发生重大变化；
* 监管机构要求时向公司领导汇报。

信息科技风险管理月报主要是向主管科技的公司领导汇报周期内IT运行情况（事件、容量、交易量、业务连续性等）、研发情况（开发质量、）、信息安全（数据安全、人员管理、审计问题），及其他事项。

除了向公司领导进行内部汇报外，还要按照监管要求向监管机关报送与信息科技风险有关的报告。

### **2.6 信息科技风险监控指标**

信息科技风险管理在IT管理中日益重要，管理层需要全面了解公司信息科技风险及风险管控情况，并能够一定程度上对可能发生的风险事件进行预警。银监会等监管机构对银行信息科技提出了一系列监管要求，需要及时发现合规问题和潜在风险，确保整体合规。为此我们设定了一系列监控指标，并进行整合和完善，建立了一套内容全面、标准统一、结构系统的信息科技风险监控指标体系。

实际工作中我们发现：

* 监管要求来源渠道多，容易遗漏；
* 不同渠道部分监管要求重复。

因此我们采取：

* 建立信息科技风险库；
* 建立信息科技风险监控指标体系；
* 监控指标体系运用。

2.6.1 建立信息科技风险库

为了全面、体系化的识别出公日常管理中需要的信息科技风险监控指标，我们首先需要建立一套完整的信息科技风险库。风险库来源应该全面覆盖行业监管合规要求、行业风险事件、行业标准、公司风险现状和相关专家知识库，保障风险库的完备性。

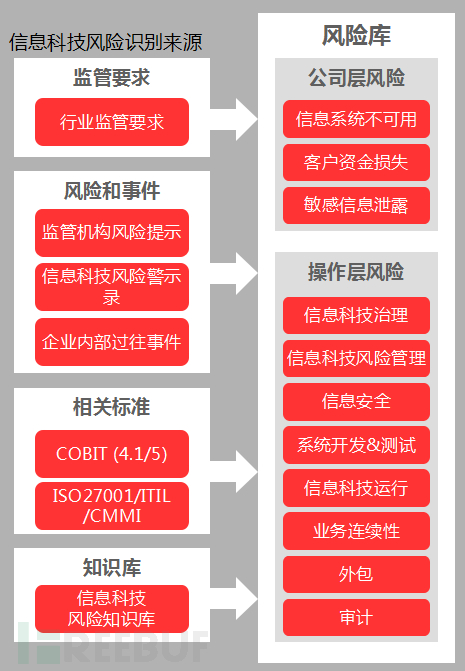
[](https://image.3001.net/images/20180429/15250072422955.png)

图3：信息科技风险指标库来源

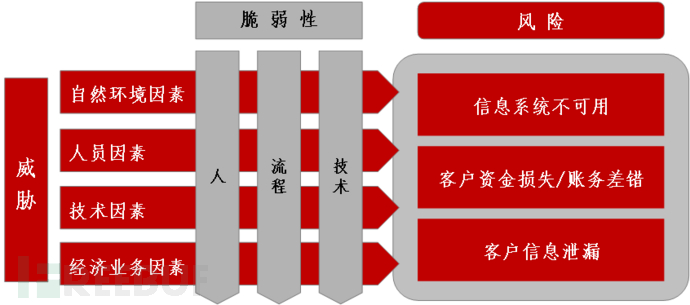
[](https://image.3001.net/images/20180429/15250072944395.png)

图4：信息科技风险识别框架

基于“威胁×脆弱性 = 风险”的理论基础，我们从监管要求、行业和公司历史风险事件、业界最佳实践标准等着手，从自然环境因素、人员因素、技术因素和业务因素等方面的威胁来分析出在人员、流程和技术等领域的脆弱性，进而识别出信息科技风险点，形成信息科技风险库。

我们通过对人民银行、银监会等监管机构发布的监管要求和标准进行详细解读，逐条提炼出相对应的信息科技风险描述，同时将业界和公司历史发生的信息科技风险事件案例作为风险识别的一个重要输入，我们通过对监管机构发布的风险提示、披露的银行业信息科技风险事件和内部过往信息科技风险事件的分析，提炼出各个风险案例中的风险点，并结合COBIT、ITIL、ISO27001、CMMI等国际标准和内部多年积累的风险知识库的内容，构建形成信息科技风险库，形成附录一、信息科技风险库示例（只列出一级和二级，三级未列出）。

**2.6.2 建立信息科技风险监控指标体系**

识别关键风险指标：基于前期建立的信息科技风险库中各个风险点的进行全面的梳理和分析，在对所有风险点进行评估的基础上，分析确定各个风险点的驱动因素，并进行关键信息科技风险指标识别。然后，从重要性、系统性、合规性、代表性和可操作性等原则对风险监控指标进行筛选。最后，在指标确定后，明确指标的含义和计算方法等关键属性。

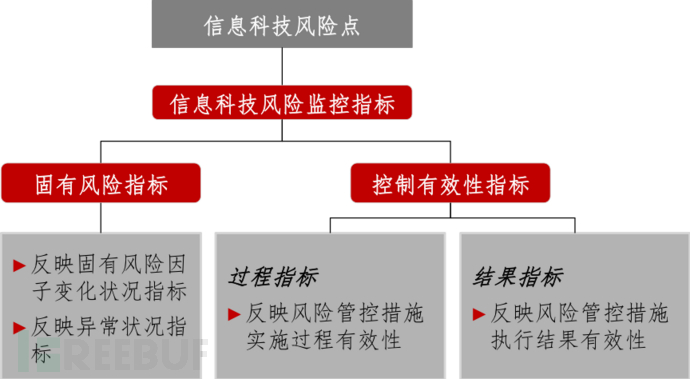
[](https://image.3001.net/images/20180429/15250073939800.png)

图5：信息科技风险关键指标识别方法

关键信息科技风险指标可以是客观的量化指标，如信息系统可用率，也可以是偏重定性的指标，如信息科技组织架构合理性等；可以是客观的，如灾备系统覆盖率，也可以是主观评价型的，如信息科技组织架构成熟度等。

**2.6.3 监控指标体系运用**

监控指标体系运用在以下几个方面：

* 有效评估信息科技风险管理水平
* 动态监测信息科技风险状况
* 合理配置信息科技风险管理资源
* 及时采取管理措施

必要时通过专业数学建模方法论，可以构建信息科技风险预警模型和管理流程，预警风险并进行风险处置。

**2.6.4 指标监测和报告**

日常进行风险指标监测，并按月向二道防线和公司领主管领导汇报监测情况，对于监测到的异常需要进行及时处置。

## ****三、监督检查****

依据监管要求、外部标准、内部规范梳理出一套适用的检查标准，并进行全面覆盖的检查。通过识别，外部规范分解成9大类、52小类、1249条元要求，去重合并后形成外规内规对应关系，也就是信息科技风险检查标准库。

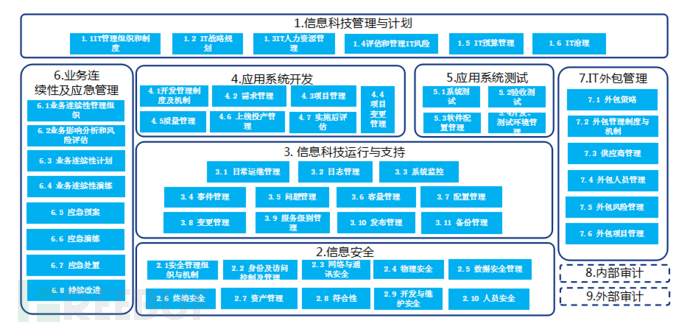
[](https://image.3001.net/images/20180429/15250074665290.png)

图6：信息科技风险检查标准库

制定全年检查计划，建立常规检查、专项检查、事件驱动检查相结合的方式，100%覆盖信息科技风险检查标准库。某年监督检查运行图示例：

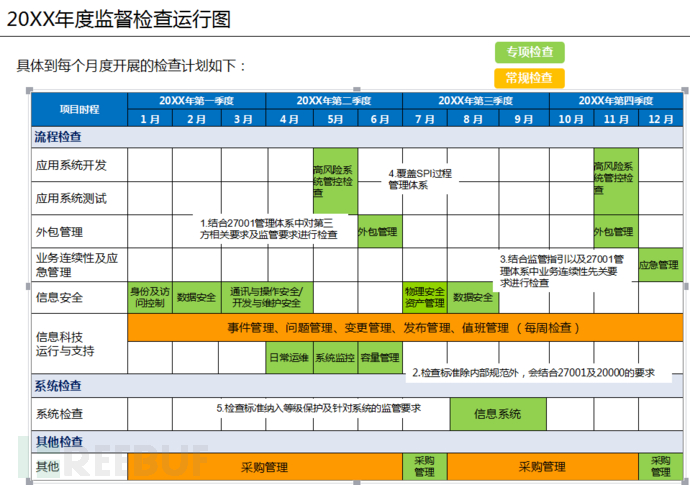
[](https://image.3001.net/images/20180429/15250074918669.png)

图7：监督检查运行图示例

专项检查围绕信息科技风险领域，如外包管理、可用性管理、数据安全、业务连续性管理等。某年共开展19项专项检查工作，提出改进完善建议200余个。

常规检查注重变更、发布、值班等日常运维重点模块，常规检查方面，按周开展监督检查，追踪变更发布近万个，追踪发现违规问题XX个，同时提出风险规避建议近白条。

事件驱动检查一般在发生可用性事件、信息安全事件或重大违规违纪事件发生后进行。检查发现，全部纳入问题管理流程进行跟踪管理。通过问题跟踪机制，归口管理二、三道防线的检查发现，可以充分确保问题统一归口管理无遗漏，相关整改的方案可实施、进度有跟踪、实施有成效。

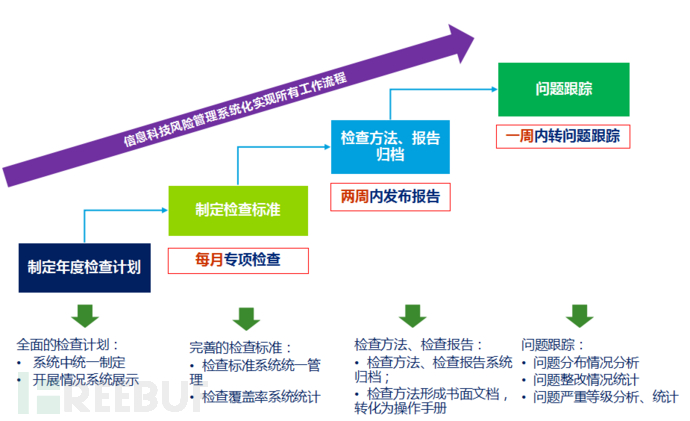
[](https://image.3001.net/images/20180429/15250075176919.png)

图8：监督检查闭环管理流程

监督检查是确保风险管理政策措施流程落地的有效保障，检查方式、投入的资源、结果的运用在于风险管理者的决策和目标定位。

## ****四、制度和公文管理****

不管企业属于什么行业、规模大小、发展快慢、战略方向如何，都需要一套科学合理的制度体系，保证制度的合规性、有效性、可操作性及规范性，IT部门也是。

制度一般以条文形式展示，名称通常冠以政策、规定、办法、规程、细则、指引等；制度可以通过制度补丁的方式进行调整、补充和完善，制度补丁可以采取条文或非条文的形式展示，一般以修订通知、补充通知或加强管理通知等标题体现。

以下不属于制度：党委、纪委、团委、工会等组织制定的制度；公司章程及公司章程规定的应当由股东大会、董事会及其专门委员会、监事会及其专门委员会制定的制度；除制度和制度补丁外，以公文形式印发的其他文件，如年度工作指导意见或考核办法、阶段性活动方案、系统操作手册、风险提示、批复等；总分机构各部门以“电邮部通”或电子邮件形式下发的通知。

### **4.1 制度体系**

制度体系应遵循架构合理、层级清晰、覆盖全面的原则，制度体系一般包括三级：

* 基本制度：是指用于规范业务条线行使经营管理职责基本事项的制度，名称一般使用制度、规定、政策、章程等；
* 专项制度：是指用于规范业务条线的工作方法和具体内容的制度，名称一般使用管理办法、管理规程等；
* 作业制度：是专项制度的细化，用于规范具体的作业内容，名称一般使用操作规程、操作细则、实施细则、指引等。

### **4.2 制度的起草**

在起草制度过程中，应开展调查研究，广泛征求制度执行部门和人员、部门内部相关人员的意见，以论证制度的必要性、有效性、合理性和可操作性。涉及其他部门职责或与其他部门关系紧密的制度，主办部门应充分征求其意见，征求意见可采取发送征求意见函、召开制度会审会、签报以及发文会签等方式进行，其中发文会签为此类制度在发文阶段的必经程序。

制度内容一般应包括：总则（含目的依据、适用范围、管理原则、职责分工、定义等）、管理流程、监督检查及罚则（如有）、附则（含制定细则要求、解释部门、施行日期、作废声明等）。

### **4.3 制度的评审**

制度评审主要审查以下内容。

* 是否符合法律、规则和准则的相关要求；
* 是否与本公司有关制度协调一致、接口清晰；
* 是否影响本公司制度整体架构的合理性和清晰性；
* 制度描述的流程是否清晰并具有可操作性；
* 是否符合本公司制度的规范性要求；
* 评审人员可以对其认为的其他制度问题（如制度实用性和适宜性等）提出评审意见。

### **4.4 制度的发布**

经评审、审核或审议通过的制度以公文形式印发。为便于制度维护和管理，印发的制度原则上应一文号对应一项制度。主办部门应根据制度的印发时间，合理确定制度的施行日期，并在制度中明确。实际中很多情况是“本文自发布之日起施行”，不如确定日期更合适。

### **4.5 制度的维护**

制度的维护包括制度的后续评估和制度改进。制度后续评估是指主办部门对制度实际管理效果进行的自我评估，旨在发现制度存在的问题，评估是否需要对制度进行改进。后续评估包括以下内容。

* 是否存在合规性、有效性、可操作性和规范性等制度问题，
* 制度间是否存在重复、冲突；
* 是否存在制度缺失和管理盲点；
* 对制度实施梳理，摸清制度补丁情况，评估实施整合的可行性和必要性。

对执行层面反映意见较多的制度，主办部门应及时进行后续评估。对于施行超过5年的制度，主办部门必须进行制度后续评估，并将评估结果报同级制度主管部门。

在日常工作中，总分支机构各部门应多方面收集和整理制度信息，提高制度后续评估的效率和质量。制度信息包括：外部政策变化，总部制度的变化，制度解释解答，基层操作人员反馈的制度问题，业务检查发现的管理漏洞，外部或同业案件反映的管理漏洞和新风险，内部组织架构、管理和业务流程调整等。

制度改进是指根据制度后续评估结果和业务管理需要，主办部门实施的制度新增、换版、修订、补充以及整合工作。在实施制度改进工作前，主办部门要评估制度改进的成本，兼顾制度的稳定性和执行的方便性，选择印发制度补丁、增加新制度或换版方式对制度实施改进。对于制度存在较多补丁的，相关部门要结合部门制度架构的安排，对制度实施整合。一般情况下，一项制度的补丁不应超过3个。

制度补丁主要有以下几种方式

* 修订通知：是指针对具体制度条款实施调整的制度补丁，发文中应明确写明作废条款的内容以及对应替换条款的内容，一般情况下其发文标题拟为“关于修订《XX公司×××》有关条款的通知”，并在文中注明解释部门和施行日期。如同时补充了相关内容，应对补充内容进行独立描述，并将发文标题拟为“关于《XX公司×××》的修订补充通知”。
* 补充通知：是指针对具体制度进行整体补充的制度补丁，不对原制度条款实施改变，发文中主要描述补充的内容，一般情况下其发文标题拟为“关于《XX公司×××》的补充通知”，并在文中注明解释部门和施行日期。如属对新增业务功能或管理内容的补充，也可采取条文的形式，一般情况下其发文标题拟为“关于印发《〈XX公司×××〉新增×××的补充规定》的通知”。
* 加强管理通知：是指从某一类业务或管理出发提出的改进要求，对原有的一系列相关制度规定均实施改变的制度补丁，一般情况下其发文标题拟为“关于加强××管理的通知”，并在文中注明解释部门和施行日期。

为加强制度补丁的关联性和针对性，以便于制度查阅和学习的系统性，各部门在选择制度补丁方式时，应尽可能采用“修订通知”或“补充通知”的方式。如以“电邮部通”方式下发的通知涉及制度管理的，一般仅限于对制度进行强调或解释，不得用于对制度进行补充和修订。

### **4.6 制度的日常管理**

制度应明确解释部门，原则上由制度主办部门负责解释，特殊情况下应明确各部门解释的范围。低层级制度与高层级制度规定相抵触时，以高层级制度规定为准，但制度解释部门另有正式批复或回复的除外。

制度框架示例见附件二。

## ****五、业务连续性管理****

### **5.1 简介**

**5.1.1 业务连续性管理的定义**

英国标准协会（BSI）：业务连续性管理（Business Continuity Management，BCM）是一个整体性的管理流程，它主要识别威胁组织的潜在影响，并且提供构建组织弹性和有效响应的框架，以保护组织关键利益相关方的利益、声誉、品牌以及价值创造的活动。（BSI，BS25999，ISO22301的前身）

中国银监会（CBRC）：商业银行为有效应对重要业务运营中断事件，建设应急响应、恢复机制和管理能力框架，保障重要业务持续运营的一整套管理过程，包括：策略、组织架构、方法、标准和程序。（《商业银行业务连续性监管指引》银监发[2011]104号）

**5.1.2 ISO 22301**

ISO22301为第一份直接以业务连续性管理（ Business Continuity Management，简称 BCM）为主题的国际标准。该标准的性质为要求（Requirements），因此将可用于审核与认证。除了ISO 22301外，另有属于指引（Guidance）的 ISO 22313，ISO 22313 与ISO 22301合为具有完整架构的业务连续性管理国际标准。

**5.1.3 BCM实施过程**

根据国际良好实践以及BCM的实施经验，将BCM的实施过程总结为以下几个关键步骤：

（1）制度和组织建设

建立BCM管理制度，组建总分支机构BCM管理组织架构，明确各部门职责

（2）BIA和RA

确定BCM的需求和管理策略，识别、分析、评价风险，确定防止、降低损失的控制措施；

（3）资源建设、预案制定

为满足业务持续运营目标而开展的资源建设，根据RA的成果制定和完善预案；

（4）演练、维护和评估

通过演练提高组织应急处置能力，验证资源可用性。评估BCM体系并持续改进；

（5）BCM企业文化建设

贯穿BCM整个过程，提高全员意识，将BCM融入企业文化中。

### **5.2 监管要求**

**5.2.1银监会**

2007年《商业银行操作风险管理指引》：业务连续要求的重点为实现从系统到业务的提升；

2008年《银行业重要信息系统突发事件应急管理规范》：明确银行突发事件应对原则，日常管理以及应急管理组织架构；细化了危机事件预测预警和内外部上报流程；

2009年《商业银行信息科技风险管理指引》：要求审阅连续性计划和应急演练；

2010年《商业银行数据中心监管指引》：明确数据中心的建设以及灾备中心的系统、数据建设目标，以满足业务连续的需求；

2011年《商业银行业务连续性监管指引》：从全行层面明确规定了业务连续性管理建设各阶段的要求，具有较强的规范性与可操作性；

2013年《商业银行资本管理办法》：明确要求业务连续性管理实施是标准法计提操作风险资本的前提条件之一。

**5.2.2 中国人民银行**

2002年《关于加强银行数据集中安全工作的指导意见》：规范银行网络可靠率、UPS供电时间、数据全备份频率、灾备中心建设、业务连续性计划和演练要求；

2006年《关于进一步加强银行业金融机构信息安全保障工作的指导意见》：强调银行需建立灾备中心，并定期进行灾备演练；

2007年《银行业信息系统灾备恢复管理流程》：规范信息系统应急响应和灾备恢复具体要求，规范灾备恢复组织架构，明确各等级系统的RTO和RPO。

**5.2.3 世界部分地区金融业监管机构发布的相关指引**

[](https://image.3001.net/images/20180429/15250075853767.png)

图9：部分地区金融监管相关指引

### **5.3 业务影响分析和风险评估**

**5.3.1 术语定义**

（1）业务连续性管理（ Business Continuity Management， 简称BCM）

《商业银行业务连续性监管指引》（银监发〔2011〕104号）第二条：业务连续性管理是指商业银行为有效应对重要业务运营中断事件，建设应急响应、恢复机制和管理能力框架，保障重要业务持续运营的一整套管理过程，包括策略、组织架构、方法、标准和程序。

（2）重要业务

《商业银行业务连续性监管指引》（银监发〔2011〕104号）第三条：重要业务是指面向客户、涉及账务处理、时效性要求较高的银行业务，其运营服务中断会对商业银行产生较大经济损失或声誉影响，或对公民、法人和其他组织的权益、社会秩序和公共利益、国家安全造成严重影响的业务。

（3）恢复时间目标和恢复时间点目标（ RTO 和 RPO）

恢复时间目标（RecoveryTime Objective，RTO）分业务RTO和系统RTO，指业务或系统从中断到恢复所需要的时间，是业务或系统恢复及时性的指标。 恢复时间点目标（Recovery Point Objective，RPO）分业务RPO和系统RPO，指业务或系统数据恢复到的时间点，是业务或系统恢复数据完整性的指标。

（4）业务影响分析

业务影响分析（ Business Impact Analysis ，简称：BIA）是整个BCM流程建立的基础工作，在这一过程中，通常会利用定量和定性分析相结合的方法对业务中断可能导致的经济与运营损失进行科学的分析，从而制定重要业务的恢复优先级、恢复目标（RTO与RPO）以及重要信息系统的恢复优先级和恢复目标等，通过BIA确定业务连续性管理的策略。

BCM就是解决运营中断事件发生时需要用多少资源、多长时间、什么方式、恢复什么业务的问题，其中资源、时间、业务都是BIA的成果。

《商业银行业务连续性监管指引》（银监发〔2011〕104号）第二十三条：商业银行应当通过业务影响分析识别和评估业务运营中断所造成的影响和损失，明确业务连续性管理重点，根据业务重要程度实现差异化管理，确定各业务恢复优先顺序和恢复指标。商业银行应当至少每三年开展一次全面业务影响分析，并形成业务影响分析报告。

（5）风险评估

风险评估（Risk Assessment，简称：“RA”）是进行风险识别、风险分析和风险评价的整个过程，基于BCM的风险评估关注于可能对BIA所识别的重要业务造成中断的各类威胁发生的可能性和影响程度，并针对潜在的威胁和影响制定进一步的风险管控措施。RA是BCM开展的基础和主要需求来源之一。

BCM就是解决运营中断事件发生时需要用多少资源、多长时间、什么方式、恢复什么业务的问题，其中资源、时间、业务都是BIA的成果，采用的方式就是RA后制定的风险管控和处置的具体措施。

《商业银行业务连续性监管指引》（银监发〔2011〕104号） 第二十八条：“商业银行应当开展业务连续性风险评估，识别业务连续运营所需的关键资源，分析资源所面临的各类威胁以及资源自身的脆弱性，确定资源的风险敞口。关键资源应当包括关键信息系统及其运行环境，关键的人员、业务场地、业务办公设备、业务单据以及供应商等。”第二十九条：“商业银行应当根据风险敞口制定降低、缓释、转移等应对策略。依据防范或控制风险的可行性和残余风险的可接受程度，确定风险防范和控制的原则与措施。”

**5.3.2 业务影响分析实施过程**

业务影响分析实施过程包括重要业务和重要系统的识别，重要业务的影响分析过程及结果，重要系统的影响分析过程及结果，从而得出整个BIA成果，具体流程如下：

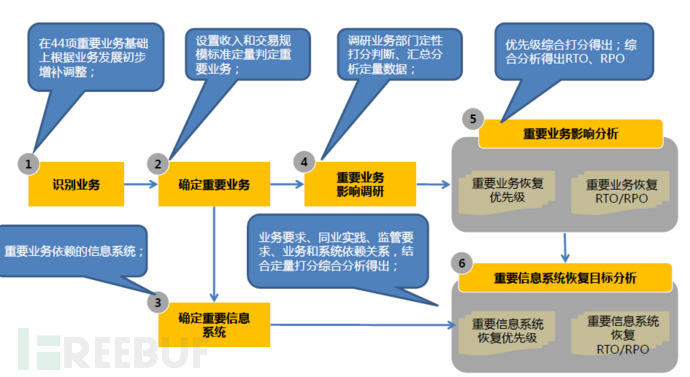
[](https://image.3001.net/images/20180429/15250076192012.png)

图10：业务影响分析实施流程

恢复时间目标和恢复时间点目标（RTO 和 RPO）：

* 业务RTO，指的是业务恢复所需要的必须时间，是业务恢复及时性的指标。对于公司来说就是允许我们用多长时间恢复中断的重要业务；
* 业务RPO，指的是业务恢复到的时间点，是业务恢复数据完整性的指标。对于公司来说就是允许我们重要业务丢失多长时间的数据。

通过收集和分析银监会、人民银行等监管机构发布的监管要求，得出银行业重要系统RTO和RPO的最低要求：

[](https://image.3001.net/images/20180429/15250076508411.png)

图11：RTO和RPO监管要求

**5.3.3 风险评估（RA）过程**

（1）实施前内部方案讨论

（2）确定RA的范围和实施方式：

* 参与范围：重要业务归属部门、数据中心、各一级分支机构（业务和IT）；
* 评估对象：重要业务、总部IT运营、分支机构业务运营整体、分支机构IT运营等；
* 实施方式：现场、非现场沟通和培训/问卷调研分析等。

（3）RA调研问卷设计

根据业务和IT特点，结合评估对象差异性，有针对性的设计调研问卷和调研方式。

（4）RA试点反馈，优化问卷

选择几家总部部门、分支机构进行RA工作的试点，根据试点情况反馈调整整体实施方案和优化调研问卷。

（5）全面启动RA工作

确定方案和问卷后统一组织总部各部门、各分支机构开展RA工作。

（6）分析整理，撰写报告

各分支机构根据各自RA结果，撰写分支机构RA报告；总部根据各部门反馈撰写总部评估报告。

RA注意事项：

* 各类风险对于业务或IT系统运营的中断威胁，而非经济损失。
* 问卷只是工具，问卷上评估对象、可能性和影响打分规则、影响类别、威胁，高中低风险划分都可以根据机构实际情况、风险偏好等进行客户化调整。
* 核心在于针对评估的高、中等级风险制定管控措施，不需大而全的措施，但要保障措施的可实施性，改进周期可自定，但不建议超1年，在下次RA时可分析措施的有效性。

### **5.4 BCP、演练和改进**

5.4.1 术语说明

业务连续性计划（Business Continuity Plan，简称“BCP”）： 是一种策略规划，当灾难发生致使组织关键业务或服务中断时，BCP 可以指导迅速恢复关键业务的正常与持续运作。BCP 是组织在实施BCM过程中的产出物，并在BCM 过程中不断更新和完善。银监会监管指引要求BCP主要内容应包括：重要业务及关联关系、业务恢复优先次序；重要业务运营所需关键资源；应急指挥和危机通讯程序；各类预案以及预案维护、管理要求；残余风险。

总体应急预案： 是商业银行应对运营中断事件的总体方案，包括总体组织架构、各层级预案的定位和衔接关系及对运营中断事件的预警、报告、分析、决策、处理、恢复等处置程序。总体预案通常用于处置导致大范围业务运营中断的事件。（银监发[2011]104号）

根据对国内监管指引理解，BCP的关注点是保障企业持续性运作的策略，应急预案的关注点是具体应对业务中断事件的处置方式。（国内监管要求2份文件，但国际上通用BCP即应急预案用于应急处置）。

5.4.2 内容

业务连续性计划的主要内容应当包括：

* 重要业务及关联关系、业务恢复优先次序；
* 重要业务运营所需关键资源；
* 应急指挥和危机通讯程序；
* 各类预案以及预案维护、管理要求；
* 残余风险。

专项应急预案的主要内容应当包括：

* 应急组织架构及各部门、人员在预案中的角色、权限、职责分工；
* 信息传递路径和方式；
* 运营中断事件处置程序，包括预警、报告、决策、指挥、响应、回退等；
* 运营中断事件处置过程中的风险控制措施；
* 运营中断事件的危机处理机制；
* 运营中断事件的内部沟通机制和联系方式；
* 运营中断事件的外部沟通机制和联系方式；
* 应急完成后的还原机制。

5.4.3 演练

（1）演练的目的

* 检验应急预案的完整性、可操作性、有效性
* 验证业务连续性资源的可用性。包括：人员、IT系统、IT灾备中心、办公和业务场地、基础公共资源、指挥中心、办公及业务开展所需的其他资源等。
* 提高运营中断事件综合处置能力。重要性：提高应急参与人员处置能力、熟悉处置流程、提高全员应急意识、提高应对信心 。

（2）监管的要求

《商业银行业务连续性监管指引》（银监发〔2011〕104号）第五章：业务连续性演练与持续改进 第一节：业务连续性计划演练中，对演练计划的制定、重要业务演练周期、演练时间点、演练重点（业务和IT配合、IT系统接管能力）、演练参与者（外部供应商要求）、外部机构演练、演练的记录、总结、评估、改进等都提出要求。

（3）演练的方式

桌面演练（说）

* 熟悉处置流程
* 检查角色分工
* 检查计划内容
* 为实战演练准备
* 场景简单

实战演练（做）

* 真实资源调配
* 真实系统切换
* 真实场地转移
* 全方位检验应急处置的有效性
* 场景复杂

5.4.4 持续改进

* 每年需要对业务连续性管理体系的完整性、合理性、有效性组织一次自评估，或者委托第三方机构进行评估，并向高管层提交评估报告。
* 每年需要对业务连续性管理文档进行修订，修订内容包括：重要业务调整，制度调整，岗位职责与人员调整等，确保文档的真实性、有效性。
* 开发新产品时候，应同步考虑是否将其纳入业务连续性管理范畴。对纳入业务连续性管理的，应当在上线前制定业务连续性计划并实施演练。
* 在业务功能或关键资源发生重大变更时，应当及时对业务连续性相关文档进行修订。
* 三年一次业务连续性管理的专项审计，在发生大范围业务运营中断事件后也要及时开展专项审计。

有部分企业采用了业务连续性管理系统（BCMS），进行业务连续性日常管理，也取得了一些不错效果。

### **5.5 DRI组织及认证**

5.5.1 国际灾难恢复协会（DRI International）

DRI International 成立于1988年。其使命是通过提供教育和帮助，以及发布标准的基础资源来推广业务连续性规划和灾难恢复行业的通用知识体系；协助建立公共和私营机构之间的合作来推广相关行业标准；通过对业务持续领域的专业人员进行认证，来提高获认证人员的可信度和专业技能。

有关DRI International 更多信息见：[http://www.drii.org](http://www.drii.org/)

5.5.2 DRI 中国委员会

DRI China委员会（DRI China Technical Committee，缩写为DRICTC）是DRI China的核心机构，其宗旨是为DRI China的发展提供组织建设、战略规划等方面的建议和决策支持，帮助DRI China推进业务连续性管理（Business Continuity Management，BCM）、突发公共事件应急管理（Emergency Management, EM）以及信息系统灾难恢复（Disaster Recovery, IT DR)在中国的发展，建立和完善相关行业标准，解决应用实践中的问题，跟踪国内外BCM的发展趋势，促进BCM向科学化、专业化、规范化和国际化方向发展；协助DRI China在中国培养更多符合国际标准的BCM人才；为国内外BCM专业人士、管理人员、政府主管部门、学术机构及厂商，搭建行业内外信息沟通与交流平台，促进相互合作，共同推进中国各行业BCM的应用和发展；提高中国政府和企业高层管理者对于防范及应对风险的认识和管理水平，增强其抵御灾难并持续发展的能力。

DRI China技术委员会的性质是以政府、金融、保险、证券、电信、交通、能源等行业负责灾难恢复（DR）,应急管理（EM）,业务持续性管理（BCM）的主管、以及该领域的专家、学者等自愿组成的学术性、公益性、非营利性组织。

有关DRI China 更多信息见：<http://www.drichina.org/>

5.5.3 有关业务连续性管理的国际认证

有关业务连续性管理的国际认证，认可度较高的是DRI International 组织维护的国际认证体系，一共四种：

（1）MBCP（Master Business Continuity Professional）

DRI国际认证的最高级别，专门用于在业务连续性/灾难恢复行业具有高级知识和技能的个人。 该认证是针对具有至少五年行业经验。

（2）CBCP（Certified Business Continuity Professional）

CBCP认证要求：（1）在业务连续性/灾难恢复行业拥有丰富知识和工作经验的人员；（2）该级别需要超过两年的经验；（3）申请人必须能够在专业实践的五个主题领域中展示具体和实际的经验。

（3）ABCP（Associate Business Continuity Professional）

ABCP级别适用于行业经验少于两年的个人，对业务连续性管理知识最少且已成功通过资格考试的人员。

（4）CFCP（Certified Functional Continuity Professional）

CFCP认证级别适用于在业务连续性/灾难恢复行业具有知识和工作经验的个人。该级别需要超过两年的经验。 申请人必须能够在专业实践的三个主题领域中展示具体的实践经验。

中国申请较多的BCM国际认证证书是CBCP，笔者的CBCP编号是：52519，同时担任DRI China委员会委员。

## ****六、信息科技外包管理****

近年来，各金融机构处于业务快速发展时期，产品不断丰富，开发需求持续增长，对研发产能需求很大，合理利用外包可以一定程度上减小自身队伍快速膨胀带来的人力资源波动风险，有效利用市场资源。同时通过引入外部公司资源，从而获取IT 服务提供商的先进经验，提升自身科技队伍的管理及创新水平。但与此同时带来了一系列外包管理风险。“工作可以外包，责任不能外包”，成为监管层的明确要求。

### **6.1 监管要求**

6.1.1 监管政策

* 银监会2009年发布《商业银行信息科技风险管理指引》
* 银监会2010年发布《银行业金融机构外包风险管理指引》
* 银监会2013年发布《银行业金融机构信息科技外包风险监管指引》

6.1.2 监管提示

* 关于开展信息科技外包风险专项治理工作的通知
* 关于通报成立银行业科技外包合作组织的函
* 关于成立银行业科技外包联合监管平台的通知
* 关于组织开展2014年度银行业重点外包服务机构外包风险管控工作的通知
* 关于协同开展对银行业重点外包服务机构外包服务风险联合检查的通知
* 关于加强银行业金融机构信息科技非驻场集中式外包风险管理的通知
* 关于开展银行业金融机构信息科技非驻场集中式外包监管评估工作的通知

### **6.2 IT外包管理重点**

本文不专门细述IT外包管理，仅就重点做一些说明。

6.2.1 IT外包战略

管理层需明确IT外包战略，并成为公司信息科技发展战略的重要组成部分，IT外包管理需要从战略层面考虑，涵盖整个信息科技建设周期。

平衡原则：保持外包风险、成本和效益的平衡。

核心能力：以不妨碍核心能力建设、积极掌握关键技术为导向。信息科技管理责任以及涉及公司战略管理、风险管理、内部审计及其他有关信息科技核心竞争力的职能不外包。核心业务产品、影响公司核心竞争力的产品、需要快速响应业务的产品，原则上不外包，

风险控制：建立与自身规模、市场地位相适应的供应商关系管理策略，通过准入和退出机制控制各类高风险供应商的数量，防范行业垄断和机构集中度风险，通过引入适当的竞争降低采购成本、提高服务质量，同时形成备份，合理控制供应商的数量。

6.2.2 IT外包治理-组织及职能

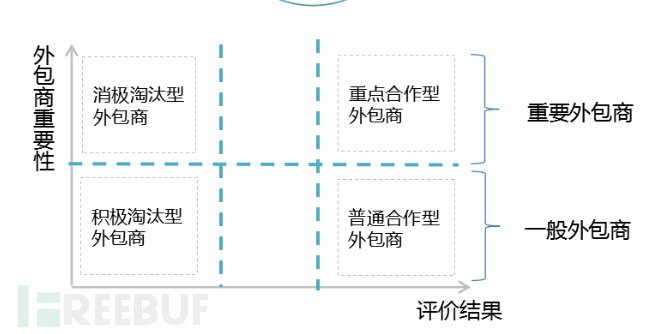
梳理公司层面和信息技术部门内部IT外包管理各流程中相关参与方的角色，明确各方的职责分工。

6.2.3 IT外包治理-制度

制定配套的IT外包管理制度

6.2.4 IT外包治理-外包商管理

制定供应商准入标准、评价标准、尽职调查模板等文档，为实践打下基础。落实准入与尽职调查，形成重要供应商清单，并不断补充调整，作为深入尽职调查的依据。

[](https://image.3001.net/images/20180429/15250077048298.png)图12：外包商分类

6.2.5 IT外包治理-外包项目管理

* 建立外包项目生命周期闭环管理，覆盖外包决策与立项、外包采购与合同、外包实施、外包结项与后评估的全生命周期管理。
* 建立是否外包的依据，外包可行性分析方法和模式决策分析模型，明确外包决策审批路径。
* 建立电子化平台，实施指纹考勤，周报监控，月度考核，季度应用，并每季度安排供应商高级经理现场述职及绩效应用跟踪。
* 及时、公开的奖惩机制，细致化合规要求，定义不同级别违规与奖励，依据级别在相对应公示范围公开公示奖惩。
* 价值+风控双维度结项审核，从人力投放、合同交付、价值收益、合规风控层面进行严格的结项审核，合理运用尾款付款权益，提高结项结论应用能力。
* 评价闭环管理及应用，将对项目实施的情况映射至相应的供应商，从人员、沟通、过程质量、交付质量、知识管理、用户满意度等维度对供应商进行评价，并将评价结果运用于新合同的决策阶段，实现闭环管理。

6.2.6 IT外包治理-外包人员管理

严格的人员甄选面试机制，对选择人员要求进行背景调查，入选后签署保密承诺书和合规操作书；建立外包人员奖惩机制，明确奖惩认定标准和流程；外包人员团队化管理模式，成立多个管理团队，从逐个管人升级至管理团队。

6.2.7 IT外包治理-外包安全管理

从外包网络安全、外包终端安全、外包人员安全、外包场地安全四个维度加强外包安全管理。

6.2.8 IT外包治理-外包应急管理

将IT外包应急管理纳入到现有的应急管理流程中，增加IT外包应急管理机制，防范IT外包服务中断等主要外包风险。

6.2.9 IT外包治理-外包风险管理

将IT外包风险纳入到现有的IT风险管理体系中进行统一管理，在IT外包事前、事中、事后分别采取相应的风险防范措施，并将核心风险放在事前进行控制。

IT外包管理后续有机会再深入探讨。

## ****七、分支机构管理****

各金融机构基本都在全国各地分步有一些分支机构，比如银行、证券，分支机构的规模都比较大，有的分支机构还有一定规模的信息技术部门。分支机构的IT风险管理也是重要内容。

### **7.1 管理内容**

主要包括：合规管理、事件管理和问题管理、项目推广、人才培养。

合规管理：明确分支机构需遵守的IT制度，并进行全覆盖的检查，检查可以是远程+现场方式结合进行。合规检查情况纳入当年度分支机构考核。

事件管理和问题管理：分支机构发生可用性事件和安全事件时，进行事件调查和处理。相关改进措施纳入问题管理跟踪督促。

项目推广：每年总部会有一些重点工作，需要分支机构落实，放入项目推广工作中。

人才培养：建立分支机构IT人才的认证模型，进行专业培训和认证考试，科学评价各分支机构岗位人才胜任情况。

7.2 有效措施

* 建立定期会议机制，比如季度分支机构IT工作例会，全体分支机构IT负责人和骨干参加。年度分支机构IT工作会议，通报各分支机构IT工作全年情况，表彰先进，督促后进。
* 建立分支机构评级机制，分支机构根据规模大小分成ABC三类，同一类之间进行科技评级，通过评级机制，将改进优化的一些非合规类要求给到分支机构，相比检查更有利于分支机构主动开展IT建设工作，评级注重的是未来持续发展能力。
* 开展分支机构检查并全覆盖，确保分支机构管理要求落地。

## ****八、其他工作****

IT内控合规管理的其他工作，包括：信息科技监管评级、公共关系管理、年度IT工作总结等，这块有机会再分享。

## ****九、附录****

9.1 信息科技风险库示例

| ****一级领域**** | | ****二级领域**** | |
| --- | --- | --- | --- |
| 1 | 信息科技治理 | 1.1 | IT战略规划 |
| 1.2 | IT组织结构管理 |
| 1.3 | IT制度管理 |
| 1.4 | IT人力资源管理 |
| 1.5 | IT预算管理 |
| 1.6 | IT培训管理 |
| 2 | 信息科技风险管理 | 2.1 | IT风险管理策略 |
| 2.2 | IT风险识别与评估 |
| 2.3 | IT风险处置 |
| 2.4 | IT风险管理流程 |
| 3 | 信息安全 | 3.1 | 安全管理组织与机制 |
| 3.2 | 身份及访问控制及管理 |
| 3.3 | 网络安全管理 |
| 3.4 | 物理安全 |
| 3.5 | 数据安全管理 |
| 3.6 | 终端安全管理 |
| 3.7 | 资产管理 |
| 3.8 | 主机及系统安全管理 |
| 3.9 | 应用安全 |
| 3.10 | 人员安全 |
| 4 | 系统开发&测试 | 4.1 | 项目管理 |
| 4.2 | 产品分析设计与实现 |
| 4.3 | 需求管理 |
| 4.4 | 软件设计和开发管理 |
| 4.5 | 版本管理 |
| 4.6 | 质量管理 |
| 4.7 | 上线投产管理 |
| 4.8 | 实施后评估 |
| 4.9 | 系统测试 |
| 4.10 | 验收测试 |
| 4.11 | 软件配置管理 |
| 4.12 | 开发、测试环境管理 |
| 5 | 信息科技运行 | 5.1 | 日常运维管理 |
| 5.2 | 日志管理 |
| 5.3 | 系统监控 |
| 5.4 | 事件管理 |
| 5.5 | 问题管理 |
| 5.6 | 性能和容量管理 |
| 5.7 | 配置管理 |
| 5.8 | 变更管理 |
| 5.9 | 服务水平管理 |
| 5.10 | 发布管理 |
| 5.11 | 备份管理 |
| 5.12 | 值班管理 |
| 5.13 | 操作管理 |
| 5.14 | 服务报告管理 |
| 5.15 | 服务请求管理 |
| 6 | 业务连续性 | 6.1 | 业务连续性管理体系 |
| 6.2 | 业务连续性管理策略 |
| 6.3 | 业务影响分析 |
| 6.4 | BCP制定 |
| 6.5 | BCP演练 |
| 6.6 | BCP检查与修订 |
| 7 | 外包 | 7.1 | 外包策略 |
| 7.2 | 外包应急 |
| 7.3 | 外包合同管理 |
| 7.4 | 外包评价 |
| 7.5 | 外包项目管理 |
| 7.6 | 供应商管理 |
| 7.7 | 合作伙伴管理 |
| 8 | 审计 | 8.1 | 内部审计 |
| 8.2 | 外部审计 |
| 8.3 | 审计覆盖 |
| 8.4 | 问题整改 |

| ****阶层**** | ****阶层含义**** | ****制度类型**** | ****用途**** | ****备注**** | ****举例**** |
| --- | --- | --- | --- | --- | --- |
| ****一阶制度**** | 宏观规定 | 总纲 | 管理体系纲领性文件 | 该阶制度一般只有一个，最多不超过两个 | XX信息科技风险管理政策XX计算机运行管理规定XX业务连续性管理工作规定XX信息系统安全管理规定 |
| 规定 | 用于规范业务条线行使经营与管理职责的基本事项 |
| ****二阶制度**** | 按照管理或技术领域进行划分 | 管理办法 | 规范业务条线的工作要求和流程，一般配对使用 | 管理办法、技术规范可以有细则，也可以单独存在 | XX服务器配置规范（201X版）XX数据库监控和检查管理规范XXIT软件外购管理办法XX上网行为管理系统管理办法XX互联网服务系统安全管理办法XX业务数据备份管理办法XX入侵检测系统管理办法XX信息系统突发事件管理办法XX病毒防治管理办法…… |
| 管理流程 |
| 技术规范 | 规范技术要求，用于制订某一个比较大的领域的技术规范 |
| 指引 | 非强制性的指导性制度，在条件允许的情况下应执行 | 如果需要进一步细化，三阶制度宜使用参考手册或参考细则 |
| ****三阶制度**** | 对二阶制度的细化或没有二阶制度配合的情况下用于独立描述一个管理或技术领域 | 细则、管理要求 | “细则”是对二阶制度的细化；“管理要求”用于综合类规定，在没有二阶制度配合的情况下用于独立描述一个管理或技术领域 | 细则可以进一步划分为：“操作细则”、“管理细则”、“实施细则” | XX变更管理 |
| 守则 | 用于人员管理类规定 |  |
| 手册 | 多为配套的操作说明 | 是否强制执行需要特别注明 |

9.2 制度框架示例

原文链接：https://www.freebuf.com/column/170332.html