



DISE 数智实审

研究型审计视角下的 金融行业信息科技外包管理

演讲人：王科

日期：2025年7月23日



数字风险赋能中心

智审未来 数造精彩！



目录

01 什么是研究型审计

02 外包活动管理
要点剖析

03 如何持续
改进

04 总结



01

什么是研究型审计



1.1 传统审计类型



合规型 审计

评估被审计对象（如组织、流程、交易）是否遵循了特定的法律、法规、行业标准、内部政策、合同条款或其他强制性要求。特点是“**符合性**”



咨询型 审计

超越了单纯的合规性检查，其核心目标是识别改进机会、提供建设性意见和解决方案，以帮助组织提升效率、效果、风险管理水平或实现战略目标。特点是“**可用性**”

1.2 什么是研究型审计

把审计的内容作为研究对象，从不同的角度进行全方位、多层次的
分析研究，找准审计重点，揭示审计问题。

信息科技发展日新月异，对审计工作要求更高、标准更严、覆盖更
广。面对新形势和任务，吃老本、凭经验，“以不变应万变”的时代已经
过时。

2020年，审计署党组书记、审计长侯凯在审计署集中整训时要求：
“如果不研究，审计工作将难以开展，甚至丧失审计的资格。”“聚焦主
责主业，着眼促进改革，在揭示问题的同时，推动完善制度机制，发挥审
计的建设性作用。”

2021年《“十四五”国家审计工作发展规划》明确提出了创新审
计理念，积极开展研究型审计的要求。研究的目的是知己知彼，确保揭示
问题有的放矢，精准到位。





“一二道防线”能管的，
审计要知道如何管；“一二道
防线”不会管的，审计指导他
们管。公司特许，这就是审计！



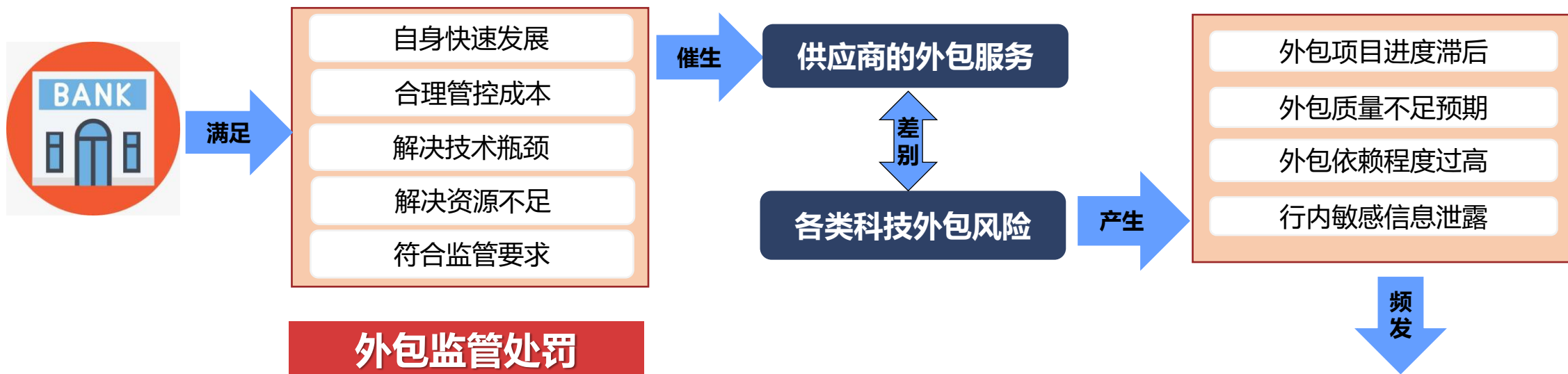
O2

外包活动管理 要点剖析



2.1发展背景

科技外包需求与监管发展趋势



- 1、2024年1月5日 中国银行-信息科技外包管理不审慎
- 2、2024年1月5日 中信银行-对外包数据中心的准入前尽职调查和日常管理不符合监管要求，部分数据中心存在风险隐患
- 3、2022年3月11日 上海汇付数据-违反特约商户实名制审核管理规定和外包业务管理规定

2.1 发展背景



豆包AI生成

《银行保险机构信息科技外包风险监管办法》（银保监办发〔2021〕141号）（以下简称《办法》）发布已有三年多，由于部分管理要求不明晰，如外包管理战略、外包管理制度体系、尽职调查、实地检查、外包服务目录、外包应急管理、供应链安全管理等，在很多金融机构中并未真正有效执行。本次直播通过“研究型”审计方式，分析管理要求中这些“难点”，讨论如何落地执行。

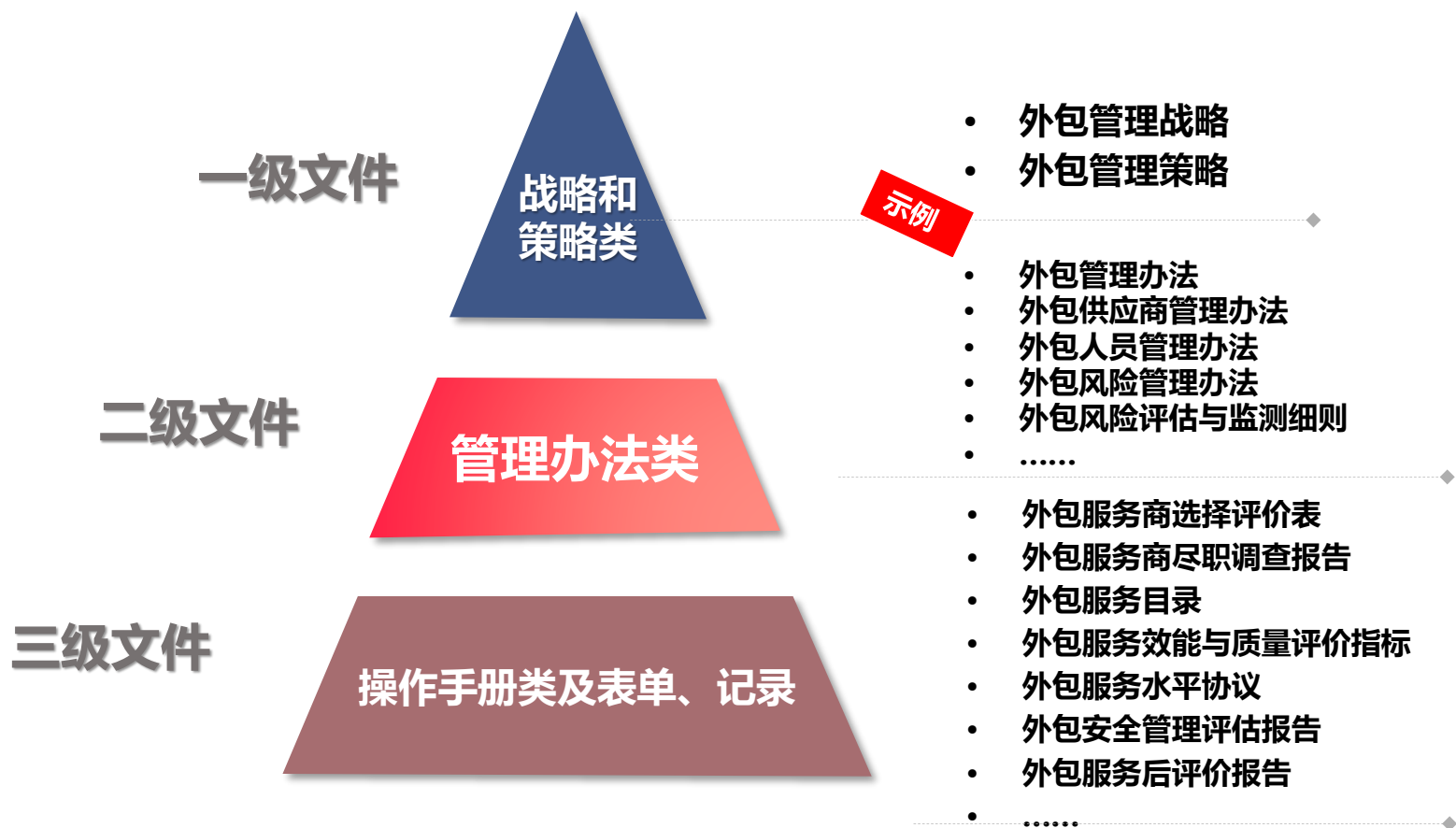


科技外包管理组织架构及职责



2.2外包治理

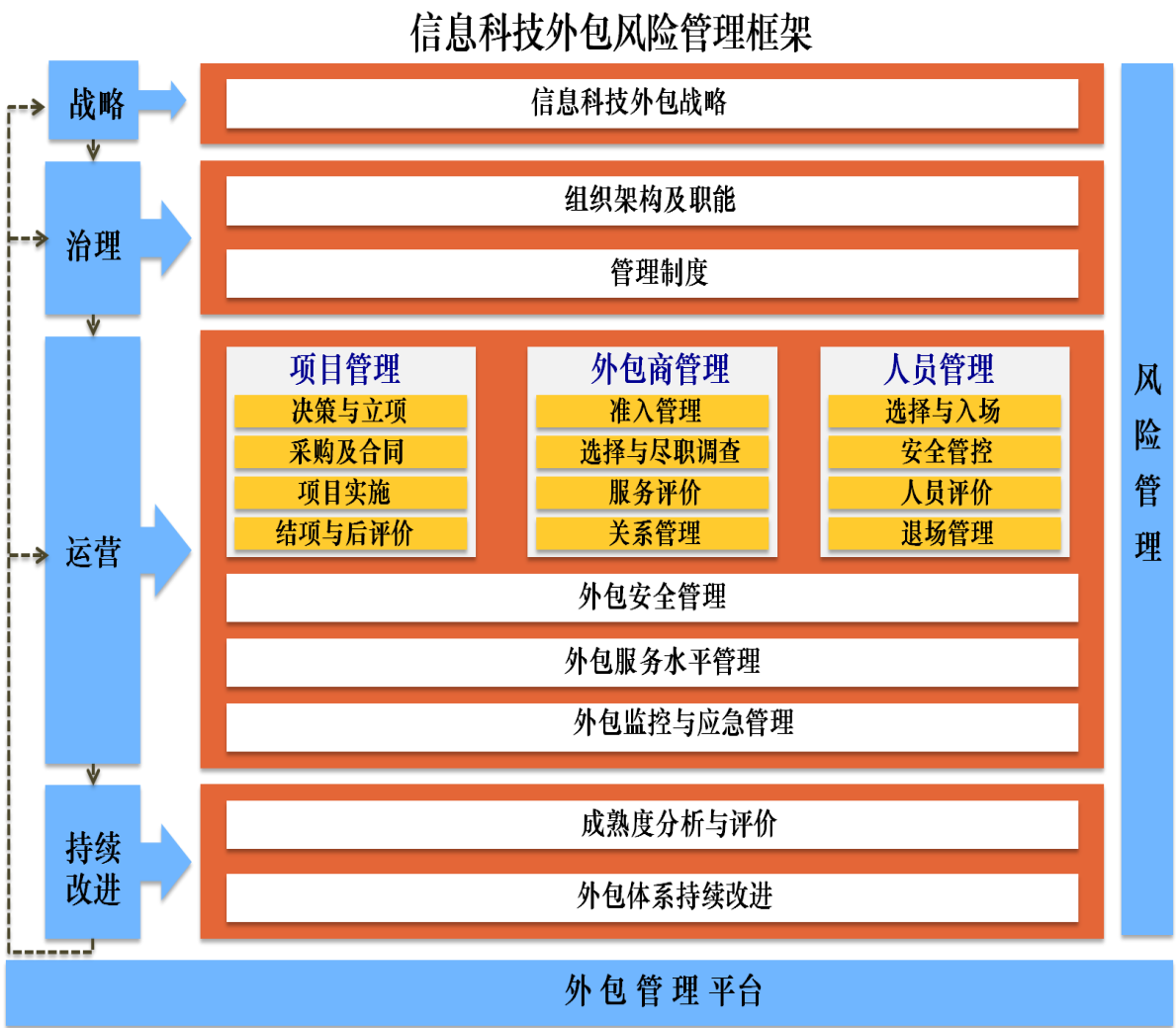
信息科技外包管理制度体系



2.2外包治理

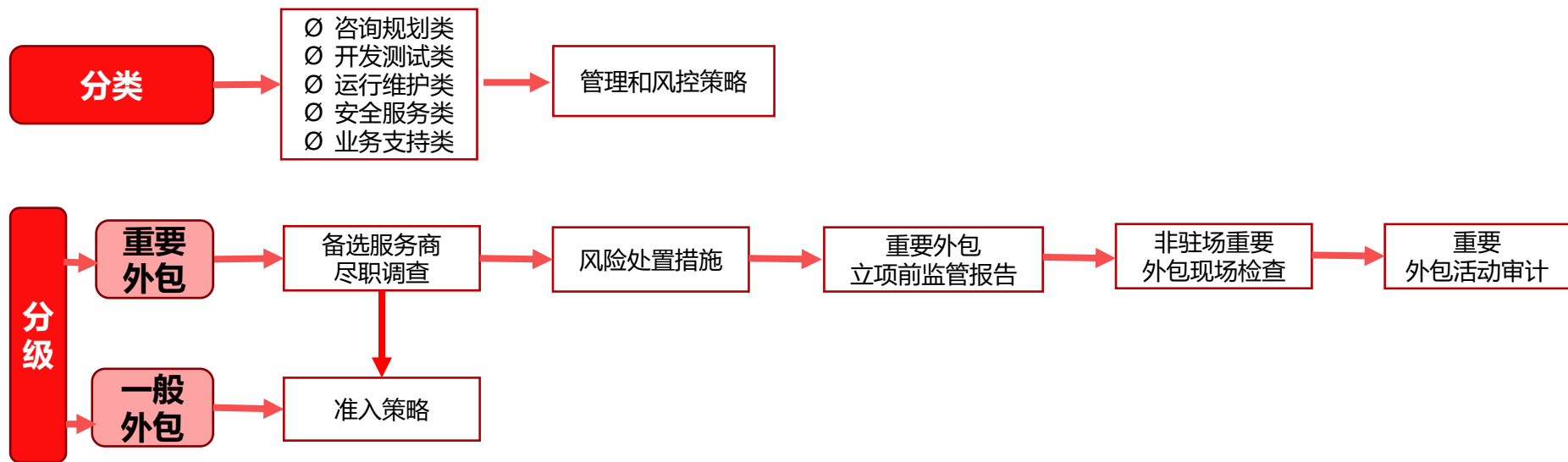
科技外包战略

应根据银行业务战略、信息科技战略、总体外包战略、外包市场环境、自身风险控制能力和风险偏好制定信息科技外包战略，战略内容至少应覆盖：外包管理现状、外包发展原则、外包总体目标和年度分项目标、外包发展蓝图、外包实施路径、具体任务、保障措施、不能外包的职能、资源能力建设方案等，并对外包战略进行解码，分析评价阶段目标的落实情况，推进外包战略的有效实施。



2.2外包治理

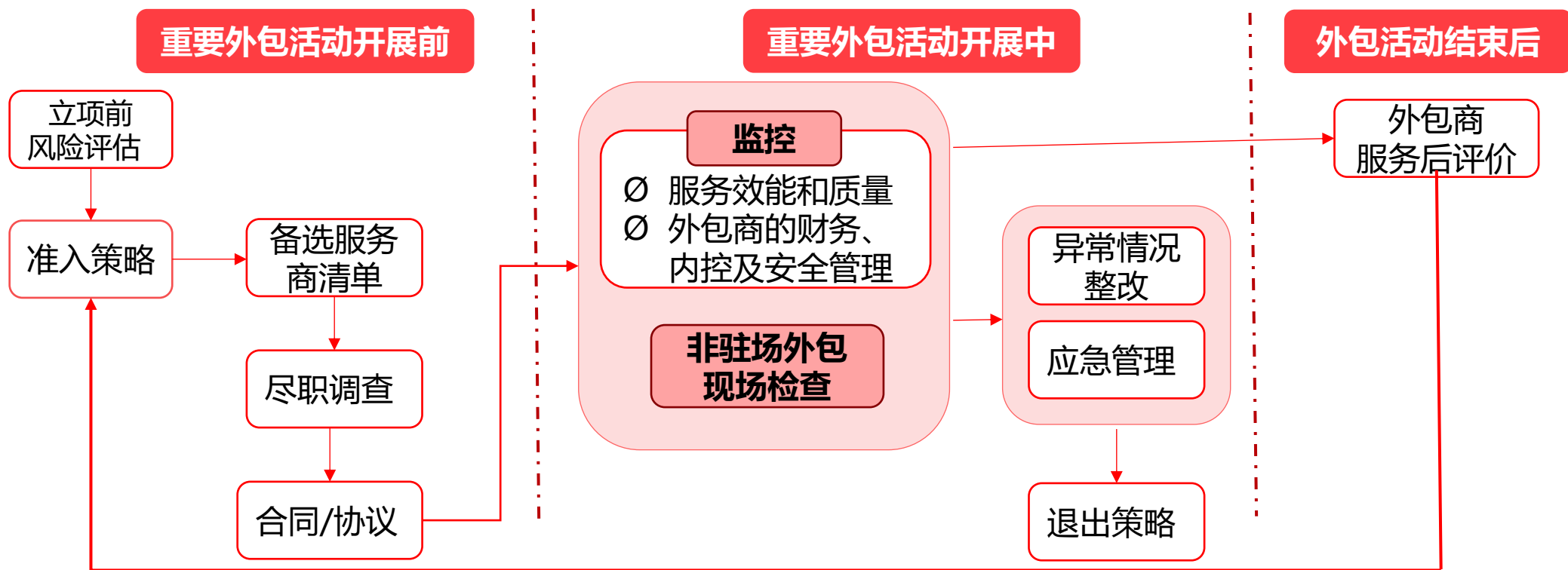
信息科技外包分类分级



2.3外包活动管理

信息科技外包活动全生命周期管理

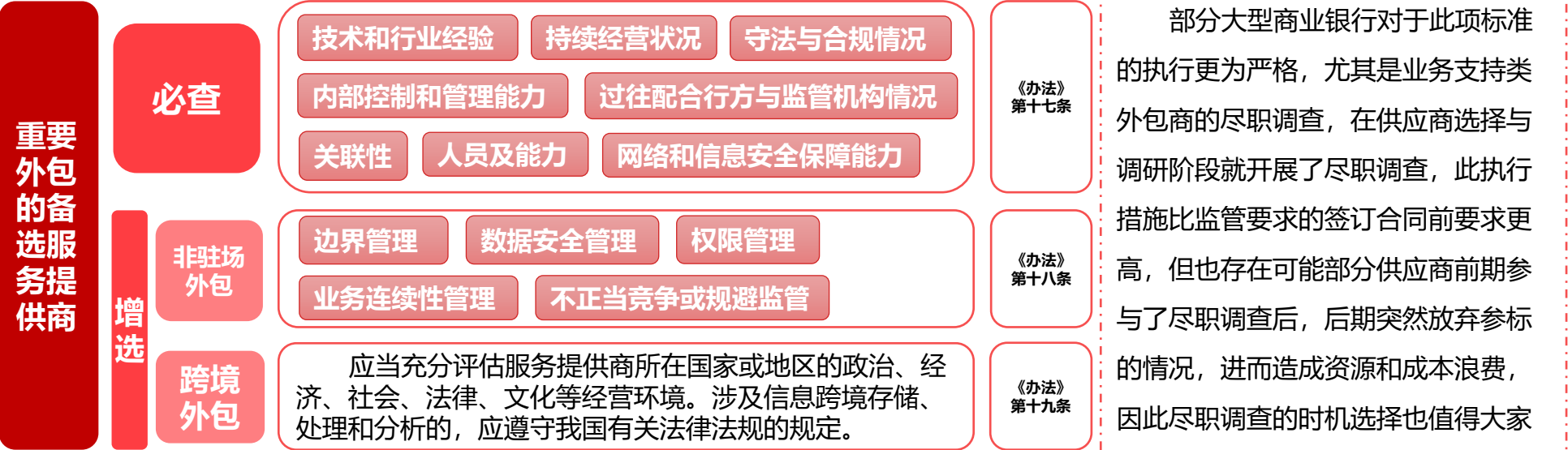
银行保险机构应对重要外包活动建立全生命周期的管控措施，从外包开展前的立项前风险评估、备选服务商尽职调查，到外包实施时的服务效能和质量监控、外包商运营状况监控，直至外包商服务后评价，形成完整的外包活动风险闭环管控。



2.3外包活动管理

外包商尽职调查

外包商尽职调查，就是在重要外包项目中标后，签订合同前这段时间内对外包服务备选商的经营状况、商业信誉、技术能力、财务、人员能力、经验能力等情况进行深入调查，一般银行保险机构会选出前三名的中标单位，会对三家备选商均开展尽职调查，价值如下：一是了解外包商真实的管理和经营情况，验证投标文件所说的事实情况，避免出现投标文件与事实产生较大的偏差或不符，存在外包风险；二是对备选商实施尽职调查，不仅是对第一名，第二、三名也同样做尽调，一旦第一名尽调出现问题，顺序第二名可以补充上，亦或者第一名在实施过程中突然的异常退出，由于前面实施了尽调，第二名可作为应急预案中的处置措施进行替补。



部分大型商业银行对于此项标准的执行更为严格，尤其是业务支持类外包商的尽职调查，在供应商选择与调研阶段就开展了尽职调查，此执行措施比监管要求的签订合同前要求更高，但也存在可能部分供应商前期参与了尽职调查后，后期突然放弃参标的情况，进而造成资源和成本浪费，因此尽职调查的时机选择也值得大家思考。



2.3外包活动管理

外包商尽职调查

条款	主要条款	检查领域
第十七条	(一) 服务提供商的技术和行业经验，人员及能力	公司治理、人员管理
	(二) 服务提供商的内部控制和管理能力	内控管理
	(三) 服务提供商的网络和信息安全保障能力	网络和信息安全
	(四) 服务提供商的持续经营状况	公司治理
	(五) 服务提供商及其母公司或实际控制人遵守国家和银保监会相关法律法规要求的情况	外部评价
	(六) 服务提供商过往配合银行保险机构审计、评估、检查及监管机构监督检查情况	内控管理
	(七) 服务提供商与银行保险机构的关联性	公司治理
第十八条	(一) 服务提供商对银行保险机构与其他机构的设施、系统和数据是否有明确、清晰的边界	网络和信息安全
	(二) 服务提供商是否有管理制度和技术措施保障银行保险机构数据的完整性和保密性	网络和信息安全
	(三) 服务提供商对涉及银行保险机构的服务器、存储、网络设备、操作系统、数据库、中间件等软硬件基础设施是否具有最高访问权限	网络和信息安全
	(四) 服务提供商是否拥有或可能拥有业务系统的最高管理权限或访问权限，是否能够浏览、获取重要数据或客户个人敏感信息	网络和信息安全
	(五) 服务提供商是否有完善的灾难恢复设施和应急管理体系，是否有业务连续性安排	连续性要求
	(六) 服务提供商是否存在不正当竞争或规避监管的情形	外部评价



2.3外包活动管理

外包商尽职调查

检查领域	子领域	检查项
公司治理	企业概况	企业性质
		服务年限
		企业规模
		经验范围
	组织架构	治理组织
		工作职责
	经营状况	股权结构
		财务状况
		服务团队
	认证资质	企业资质
	关联关系	关联关系
	知识产权	知识产权
	软件正版化	软件正版化
	专利及知识产权产品	专利产品
内控管理	售后服务	售后服务
	内控制度建设	内控制度
	内部审计评估	评估审计
	监督检查配合	配合检查
	转分包管理	转分包限制

检查领域	子领域	检查项
人员管理	管理制度	人力制度
	保密管理	保密约束
	安全培训	安全培训
	人员能力	人员能力
	人员稳定性	人员稳定性
	人员离职	人员离职
项目管理	进度管理	进度管理
	质量控制	质量控制
	文档管理	文档管理
连续性要求	技术保障	技术保障体系建设
	应急预案	应急预案
	突发情况报告机制	突发情况报告
外部评价	媒体评价	媒体评价
	违约评价	违约评价
	监管评价	监管评价
	企业信誉	企业信誉

检查领域	子领域	检查项
网络和信息安全	物理安全	门禁控制
		门禁区域
		视频监控
		备用场地
	网络安全	网络限制
		安全传输
		访问控制
	数据安全	数据保护机制
		数据传输
		数据隔离
		数据使用
		数据销毁
	终端安全	准入控制
		存储控制
		病毒管控
		软件管控



2.3外包活动管理

非驻场重要外包现场检查

现场检查要求

第三十四条 银行保险机构应当对符合重要外包标准的非驻场外包服务进行实地检查，原则上每三年覆盖所有重要的非驻场外包服务。对具有行业集中度性质的服务提供商，银行保险机构可采取联合检查、委托检查等形式，减少重复性工作，减轻服务提供商的检查负担。监管没有对现场检查内容进行明确要求，在行业实践中，检查内容通常覆盖《办法》中尽职调查的相应要求，并重点关注网络和信息安全方面。

检查领域	子领域	检查项	检查领域	子领域	检查项	检查领域	子领域	检查项	检查领域	子领域	检查项	检查领域	子领域	检查项
公司治理	企业概况	企业性质	内控管理	内控制度建设	内控制度	人员管理	管理制度	人力制度	网络和信息安全	安全团队	安全团队	网络和信息安全	数据安全	数据保护机制
		服务年限		内控制度发布	制度发布		人员招聘	人员招聘		网络与信息安全策略	安全策略			操作员安全
		企业规模		制度监督执行	制度执行		保密管理	保密约束		自评估机制	安全自评估			提供信息限制
		经验范围		内部审计评估	评估审计		安全培训	安全培训		物理安全	门禁控制			数据传输
	组织架构	治理组织		监督检查配合	配合检查		人员能力	人员能力			门禁区域			系统及数据边界
		工作职责		转分包管理	转分包限制		人员稳定性	人员稳定性			视频监控			数据隔离
	经营状况	股权结构	项目管理	进度管理	进度管理		人员经验	人员经验			备用场地			数据使用
		财务状况		质量控制	质量控制		绩效考核	绩效考核		网络安全	值班管理			数据销毁
		服务团队		文档管理	文档管理		人员追责	人员追责			网络限制		终端安全	管理制度
	认证资质	企业资质		系统环境	系统环境		人员离职	人员离职			安全传输			准入控制
	关联关系	关联关系		项目后评价	项目后评价	外部评价	媒体评价	媒体评价			访问控制			存储控制
	知识产权	知识产权		技术保障	技术保障体系建设		违约评价	违约评价		用户权限	网络边界控制			端口控制
	软件正版化	软件正版化	连续性要求	应急预案	应急预案		监管评价	监管评价			用户口令			病毒管控
	专利及知识产权产品	专利产品		突发事件处理机制	突发事件处置		企业信誉	企业信誉			安全意识		运维安全	软件管控
	创新能力	创新能力		突发情况报告机制	突发情况报告						权限管理			运维体系建设
	售后服务	售后服务									敏感信息控制			最高访问权限



2.3外包活动管理

科技外包服务效能和质量监控

银行保险机构应建立明确的信息科技外包服务目录、服务水平协议与监控评价机制，对信息科技外包服务制定服务效能和质量监控指标，并进行相应监控，当指标出现异常时，应及时采取处置措施。

外包服务目录

按照外包服务内容建立外包服务目录，并根据外包服务类型进行分类，如咨询规划类、开发测试类、运行维护类、安全服务类、业务支持类等

服务水平协议

根据外包服务类型，制定相应的服务水平协议模板。和外部服务提供商签订服务水平协议时，需结合服务内容对模板进行裁剪。

服务效能和质量 监控指标

根据外包服务类型，制定相应的服务效能和质量监控指标。在对外包活动进行监测时，需结合相应的服务水平协议内容对监控指标进行筛选。

服务效能和质量 监控

根据服务效能和质量监控指标，进行相应监控。当指标超出阈值，应及时督促服务提供商采取纠正措施。

2.3外包活动管理

科技外包服务目录

《信息技术服务 外包 第1部分：服务提供方通用要求》（GBT 33770.1-2017）

服务目录：服务提供方提供的服务列表。 **一般包括：**服务名称、服务描述、服务指标、服务等级、服务时间、安全方案等。

序号	服务类型	服务子类	外包活动等级	服务名称	服务描述	合同编号	合同名称
1	咨询规划类	信息科技战略规划咨询	重要	2025-2030年信息科技战略咨询	提供规划选项分析报告（最终决策权保留在行方科技委员会），不含架构设计实施权	CT-2025-CNS-001	2025-2030年信息科技战略建议服务合同
2	开发测试类	移动端应用开发	一般	手机银行二期功能模块迭代开发	基于行方提供的架构标准进行编码；核心身份认证模块由行方自主开发	CT-2025-DEV-007	手机银行二期功能开发外包服务合同
合同签订日期	服务结束时间	服务指标	归口管理部门	行方服务接口人	服务商接口人	是否驻场	安全方案
2025/1/10	2025/6/30	交付物通过行方评审率100%；知识转移培训≥8学时	战略发展部	周*（首席信息官）	张*（麦*合伙人）	是	所有数据脱敏后提供；报告存储于行方加密服务器；服务商签署保密协议
2025/3/1	2025/12/31	代码安全漏洞数≤3/千行	移动金融部	吴*（开发经理）	陈*（东*项目经理）	是	开发环境与生产环境物理隔离；代码仓库权限按功能模块分离；双人复核生产发布



2.3外包活动管理

服务效能和质量监控指标

《办法》第二十五条 银行保险机构应当对信息科技外包服务建立服务效能和质量监控指标，并进行相应监控。常见指标包括：（一）信息系统和设备及基础设施的可用率；（二）故障次数、故障解决率、故障的响应时间、故障的解决时间；（三）服务的次数、客户满意度；（四）**业务需求的及时完成率、程序的缺陷数、需求变更率**；（五）外包人员工作饱和度、外包人员的考核合格率；（六）网络和信息安全指标、业务连续性指标。

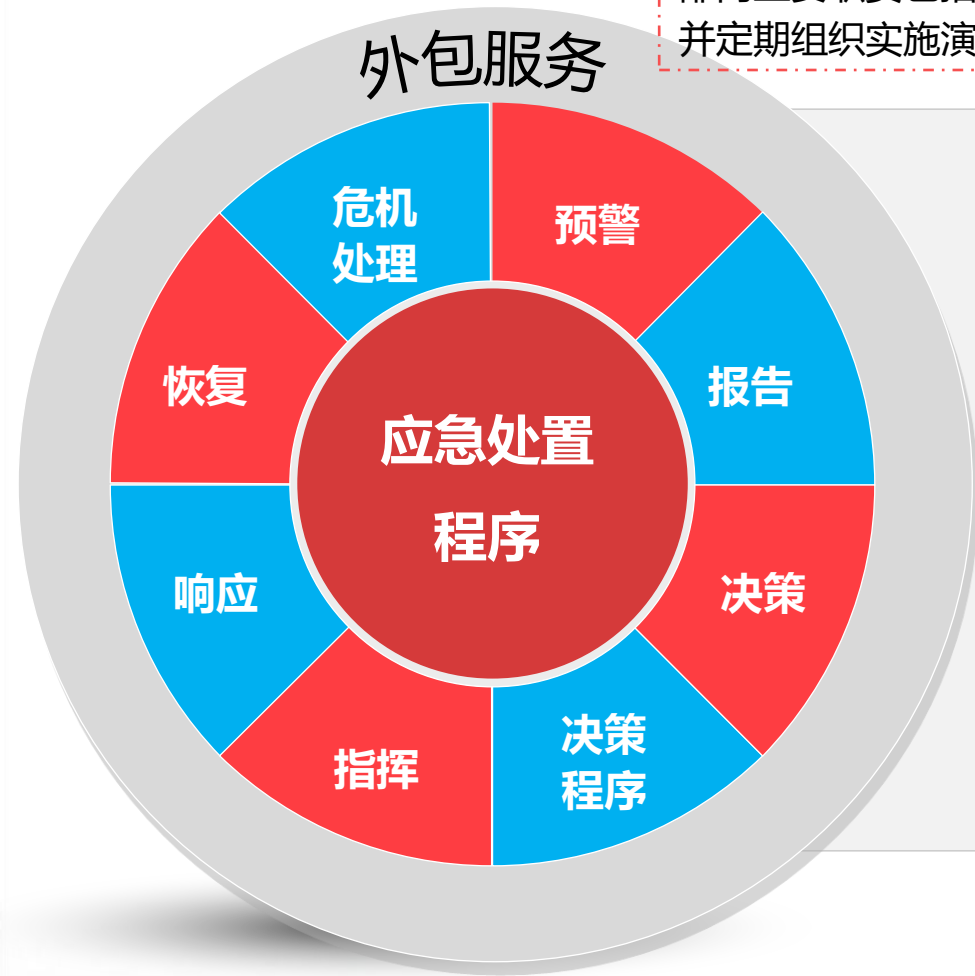
示例

指标名称	指标定义	评分标准
业务需求的及时完成率	衡量服务商业务需求实现的及时程度 $\text{业务需求及时完成率} = (\text{及时达成的业务需求数} / \text{所有业务需求数}) * 100\%$	5: 业务需求及时完成率不低于标准阈值; 4: 业务需求及时完成率低于标准阈值, 但不超过5%; 3: 业务需求及时完成率低于标准阈值, 但不超过10%; 1: 业务需求及时完成率低于标准阈值, 且超过10%.
需求变更率	衡量项目需求的稳定性, 通过变更数量和总体需求数量的比较, 来判断该项目是否超出了预先设定的变更范围。 $\text{需求变更率} = \text{变更数量} / \text{总体需求数量} * 100\%$	5: 需求变更率 $\leq$ 标准阈值 4: 需求变更率 $>$ 标准阈值, 但不超过标准阈值95% 3: 需求变更率 $>$ 标准阈值, 但不超过标准阈值90% 1: 需求变更率超过标准阈值90%
程序的缺陷率	服务商开发软件产品统计周期内单位功能点内发现的有效缺陷数量 $\text{产品缺陷率} = \text{统计周期内累计发现的该系统有效缺陷数} / \text{统计周期内该系统功能点总数}$	5: 无产品缺陷率 4: 产品缺陷率1% 3: 产品缺陷率5% 1: 产品缺陷率15%

2.3外包活动管理

外包应急与演练

《办法》第八条 银行保险机构应指定信息科技外包风险主管部门，该部门主要职责包括：（三）制定保障外包服务持续性的应急管理方案，并定期组织实施演练；



Ø 应急场景分析

- n 场景一：重要IT外包供应商重要人员流失导致相应服务质量无法保证
- n 场景二：重要IT外包供应商因经营不善、内部结构调整导致外包服务中断
- n 场景三：重要IT外包供应商因重大外包事件，被监管机构或同业金融机构风险通报
- n 场景四：重要IT外包供应商因违反行方安全及内控管理规定，造成重大损失被行内要求停止合作

- 第1章 总则
 - 1.1 目的
 - 1.2 范围
- 第2章 外包应急管理组织架构
 - 2.1 应急决策小组
 - 2.2 应急指挥小组
 - 2.3 应急执行小组
 - 2.4 应急保障小组
- 第3章 外包服务应急处置程序
 - 3.1 外包服务异常预警
 - 3.2 外包异常事件报告
 - 3.3 外包服务中断应急决策
 - 3.4 外包服务中断应急指挥
 - 3.5 外包服务中断应急响应
 - 3.6 外包服务应急恢复
 - 3.7 外包服务中断事件关闭
- 第4章 外包服务中断应急场景分析
- 第5章 重要外包服务中断应急场景及处置措施
- 第6章 预防与危机处理
 - 6.1 预防措施
 - 6.2 危机处理
- 第7章 外包应急演练与预案更新
- 第8章 内部沟通管理
- 第9章 对外沟通管理
- 第10章 附录

示例

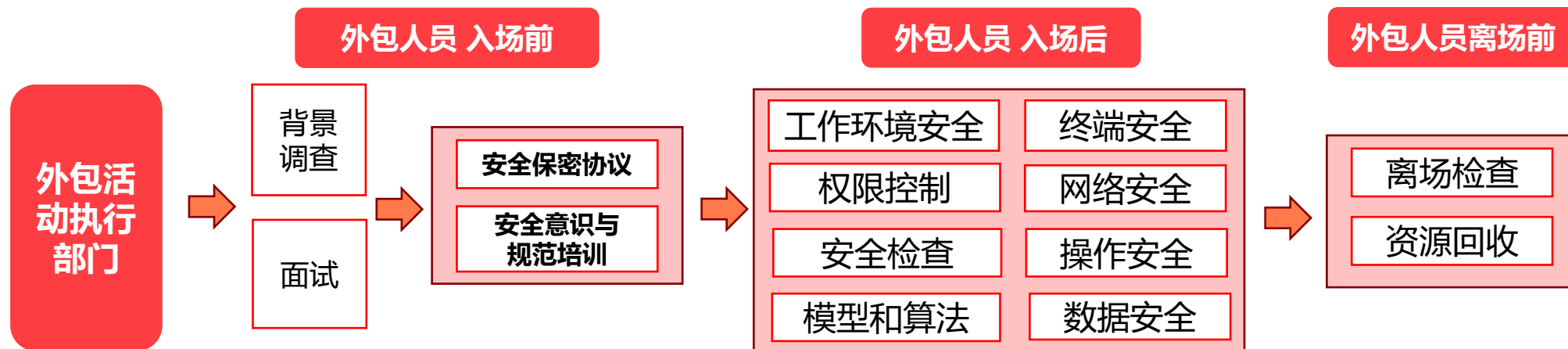
信息科技外包应急预案



2.3外包活动管理

外包人员管理

外包活动执行团队应进一步提升基于外包人员活动全生命周期的管理能力，从外包人员入场、开展外包项目实施、外包人员离场等阶段，加强管理与技术措施，降低敏感信息泄露风险。外包风险管理部门应定期对外包活动进行网络和信息安全评估。审计部门应定期开展信息科技外包及其风险管理的审计工作。



2.4供应链安全管理

第三十一条 针对可能给业务连续性管理造成重大影响的重要外包服务，银行保险机构应当事先建立风险控制、缓释或转移措施，包括但不限于：（一）事先制定退出策略和供应链安全保障方案，并外包服务实施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或服务质量下降的情况；

国家战略及法律法规

Ø 《国家网络空间安全战略》(2016年发布)

四、战略任务（三）保护关键信息基础设施

建立实施网络安全审查制度，**加强供应链安全管理**，对党政机关、重点行业采购使用的重要信息技术产品和服务开展安全审查，提高产品和服务的安全性和可控性，防止产品服务提供者和其他组织利用信息技术优势实施不正当竞争或损害用户利益。

Ø 《网络产品和服务安全审查办法(试行)》(2017年发布)

第四条 网络安全审查重点审查网络产品和服务的安全性、可控性，主要包括：……（二）产品及关键部件生产、测试、交付、技术支持过程中的**供应链安全风险**……

国家标准

Ø GB/T 40753-2021《供应链安全管理体系 ISO 28000实施指南》。

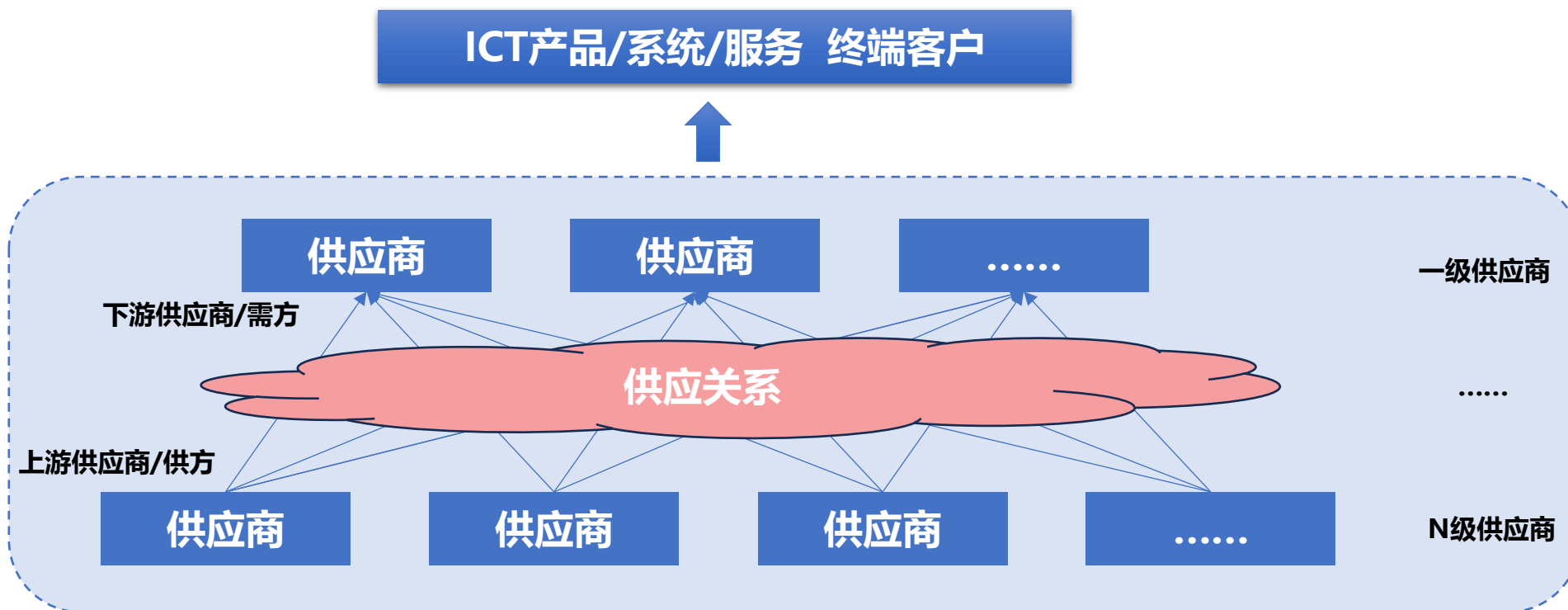
Ø GB/T 38702-2020《供应链安全管理体系 实施供应链安全、评估和计划的最佳实践 要求和指南》

Ø GB/T 36637-2018《信息安全技术 ICT供应链安全风险指南》



2.4供应链安全管理

管理范围



2.4供应链安全管理

管理制度

供应链安全管理办法	组织架构	科技部门、相关业务部门、风险部门、审计部门、法律部门、采购部门
	管理机制	总体要求、采购管理、运营管理、退出管理
	技术要求	物理环境安全、系统通信安全、访问控制 身份标识与鉴别、供应链完整性保护、可追溯性
	风险监测	监测流程、风险评估、事件处置、报告机制、应急演练
	审计监督	审计范围、审计机制、监督改进
	教育培训	培训计划与频次



2.4供应链安全管理

风险管理框架

ICS 35.040
L 80



中华人民共和国国家标准

GB/T 36637—2018

信息安全技术

ICT 供应链安全风险 管理指南

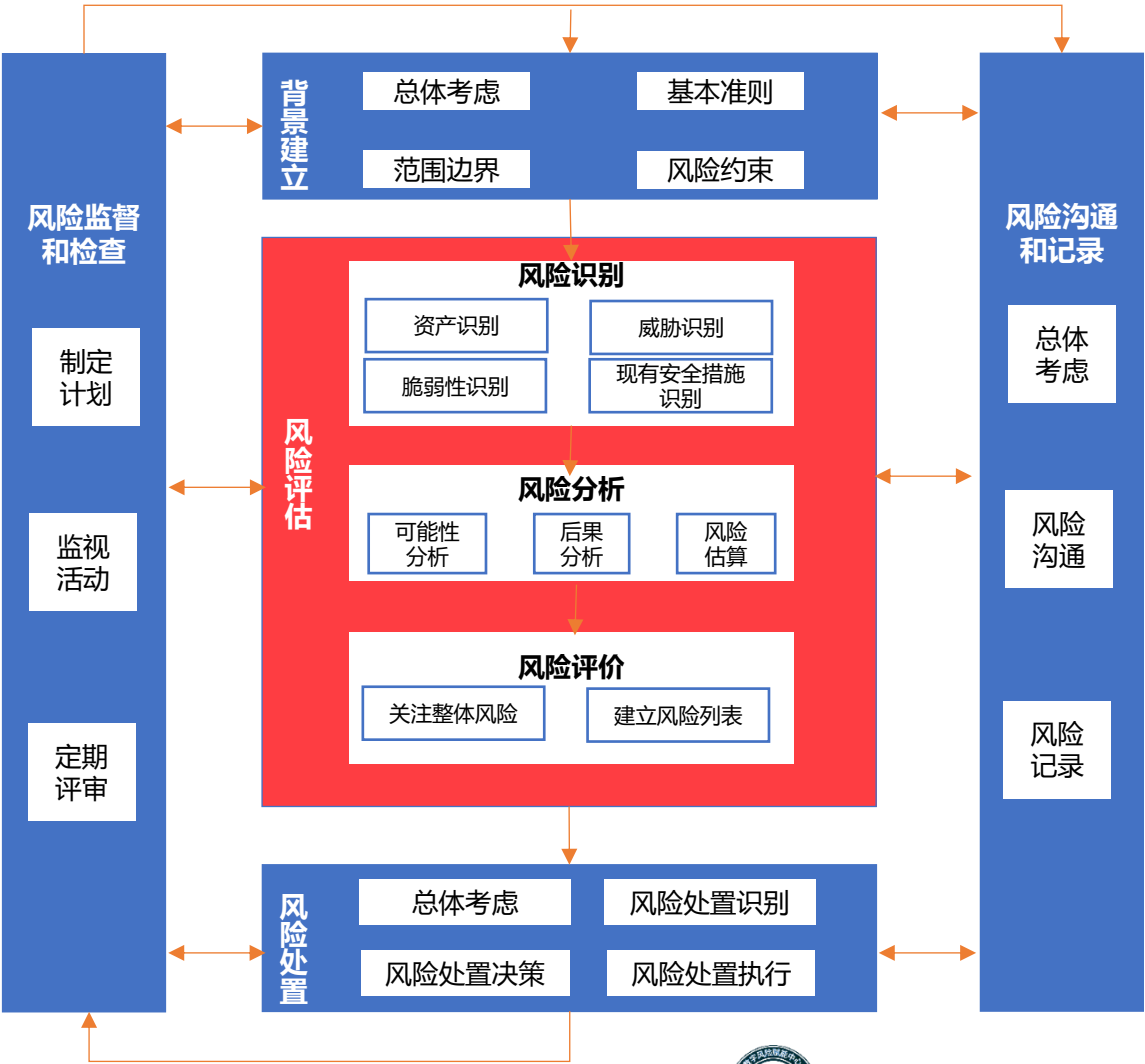
Information security technology—Guidelines for the information and communication technology supply chain risk management

2018-10-10 发布

2019-05-01 实施

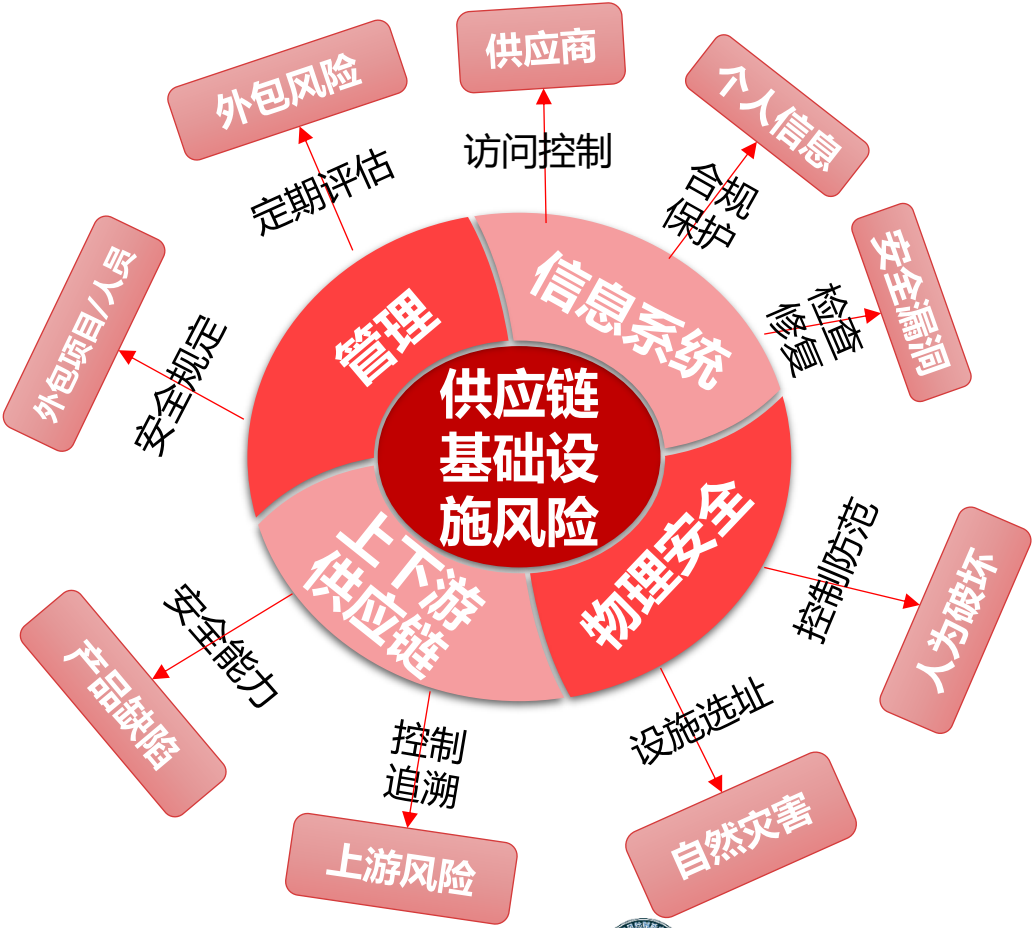
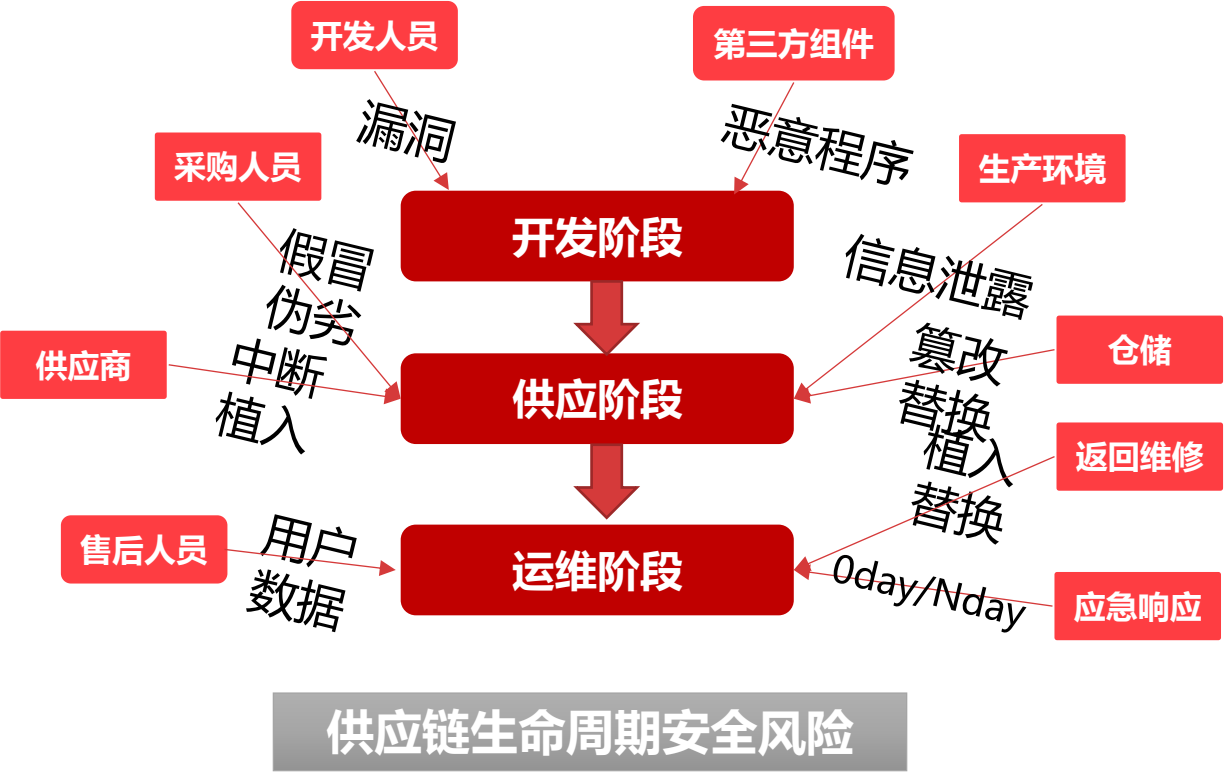
国家市场监督管理总局
中国国家标准化管理委员会

发布



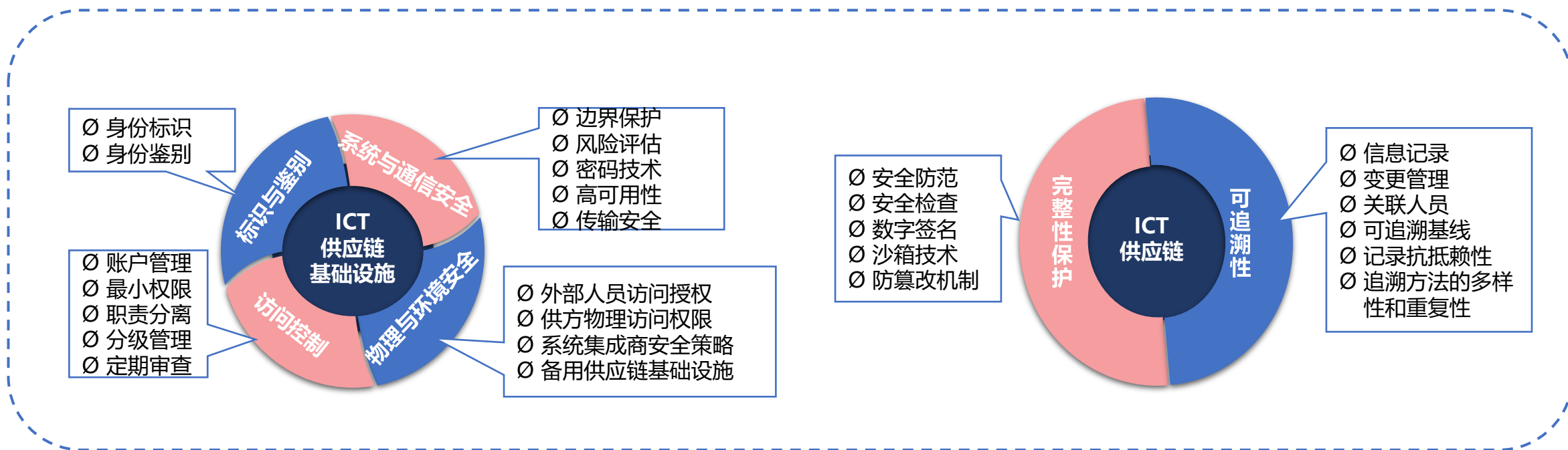
2.4供应链安全管理

安全风险分析



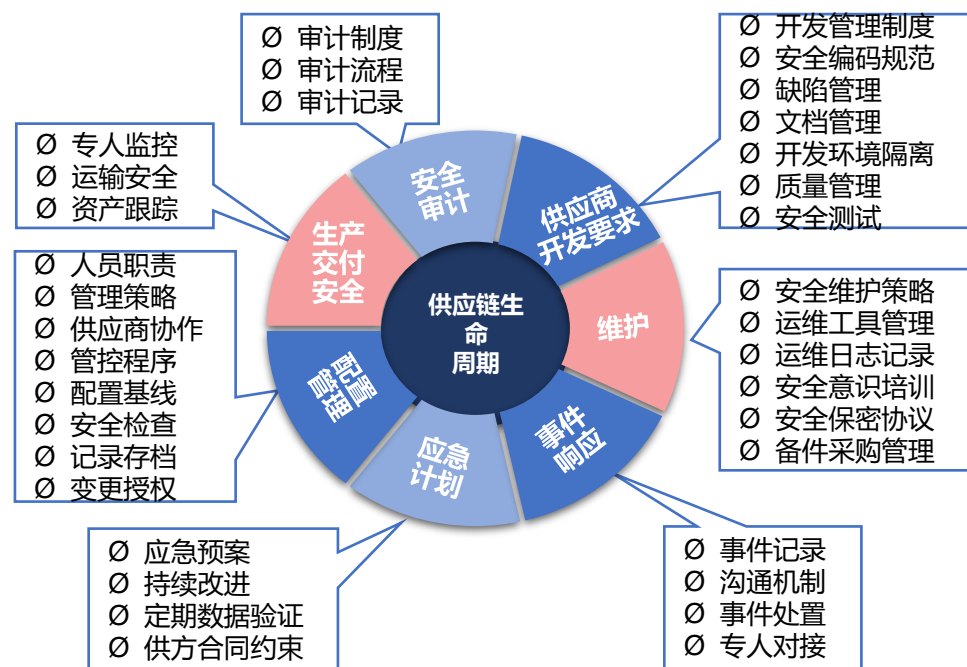
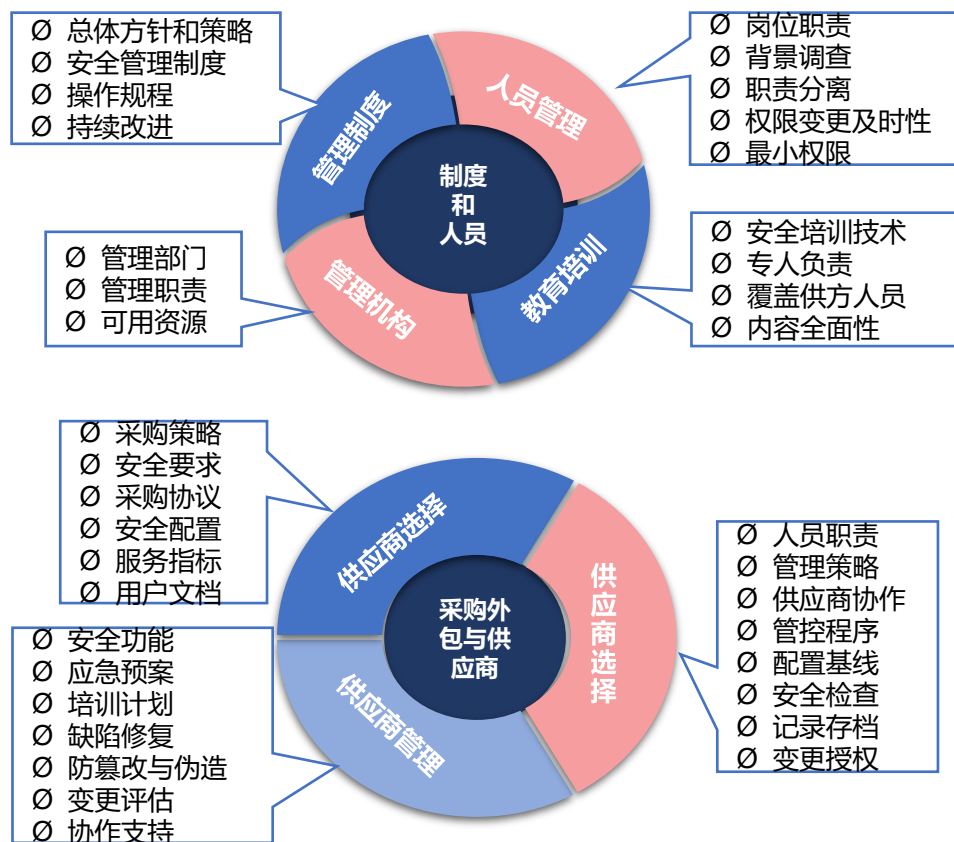
2.4供应链安全管理

技术安全措施



2.4供应链安全管理

管理安全措施





O3

如何持续改进



3.1外包管理能力框架

ICS 35.240
CCS L67

T/CCUA
中国计算机用户协会团体标准
T/CCUA 003-2023
代替T/CCUA 003-2019

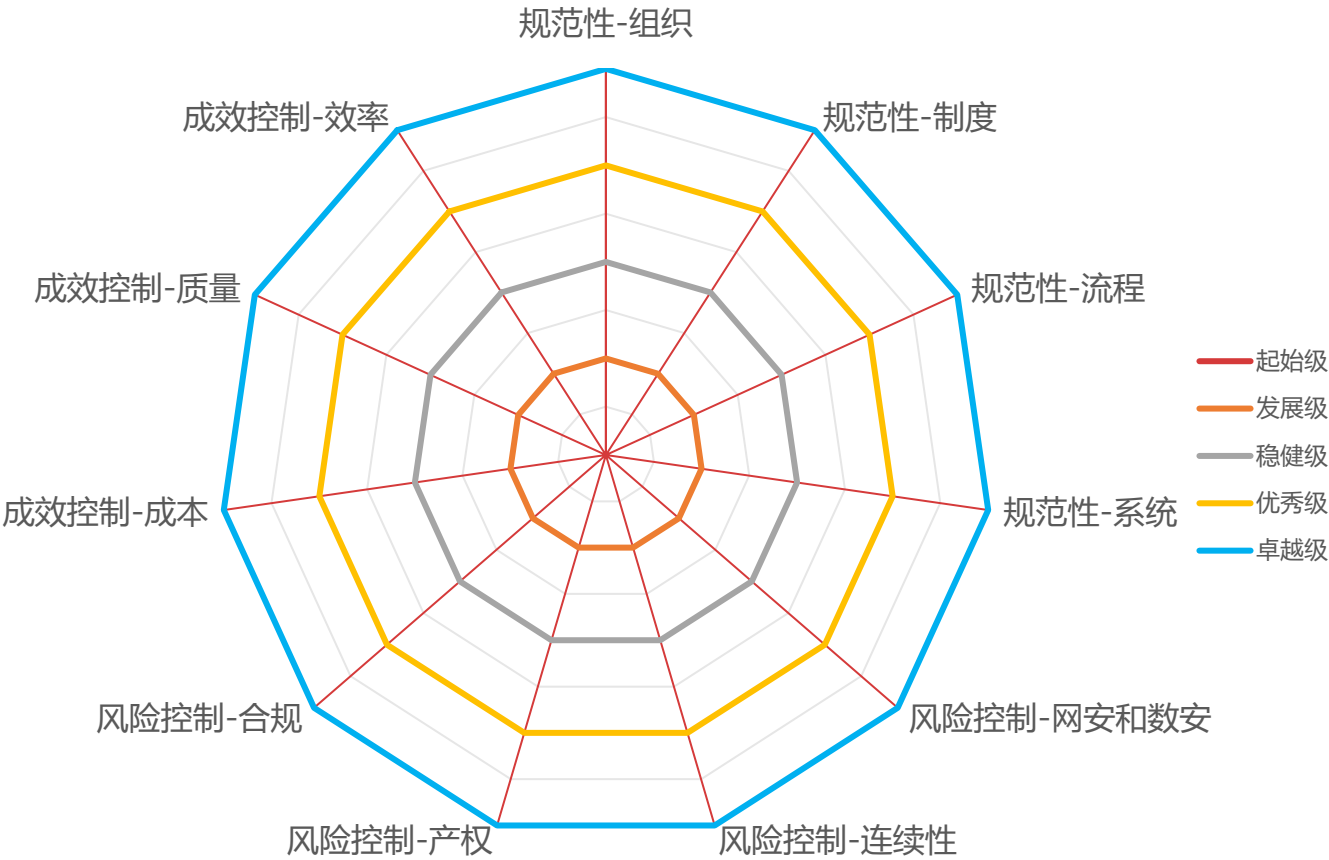
金融信息科技外包风险管理能力
成熟度模型与评估规范

Risk management capability maturity model and assessment for outsourcing of
financial information technology specification

2023-03-24 发布

2023-04-24 实施

中国计算机用户协会 发布



数字风险赋能中心

3.2外包管理能力成熟度等级



3.3 D1-规范性

01

P1
组织

原则性能力

- (1) 自上而下的外包管理组织架构，组织架构基于外包量化数据可以快速调整、持续调优，不断推进外包活动的精细化管理
- (2) 良好的组织架构和组织调整制度促进组织外包管理能力成熟度的提升

02

P2
制度

原则性能力

- (1) 形成定期更新制度的机制，并随着新技术、新管理、科技战略持续优化
- (2) 建立组织级优秀实践库
- (3) 应建立外包战略、项目后评价、外包关系管理制度

03

P3
流程

非原则性能力

- (1) 流程应随组织的业务发展、研发技术、管理模式创新做出更新
- (2) 应建立高度成熟的自动化流程，流程流转高效，且流程流转时效能够进行度量，并不断调优

04

P4
系统

非原则性能力

- (1) 系统能实现外包项目生命周期全流程的管理，外包驻场人员的管理，服务提供商信息
- (2) 系统能提供数据统计、分析、汇总功能，能提供数据用于外包管理的持续优化
- (3) 系统实现项目后评价



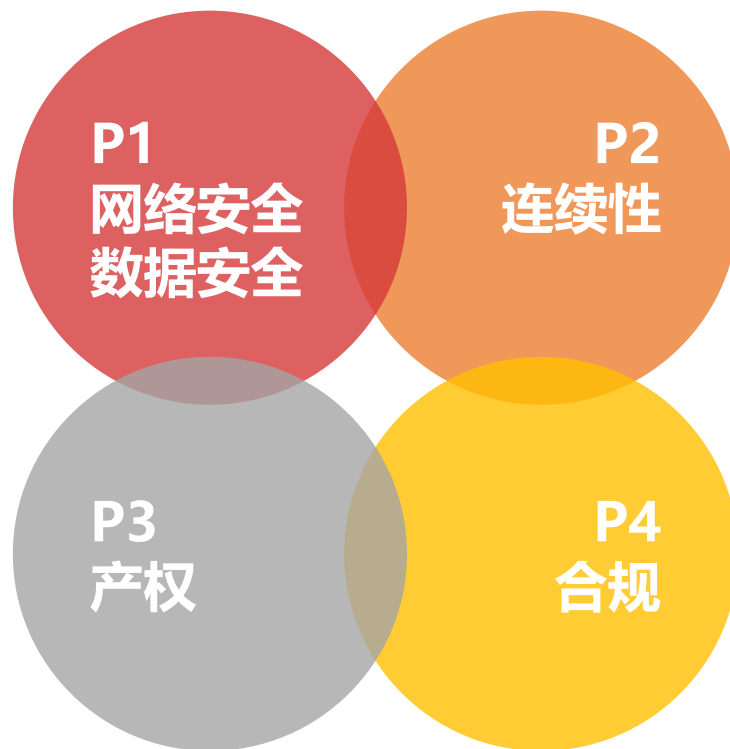
3.4 D2-风险控制

原则性能力

- (1) 发布了外包网络安全、数据安全规范，并将安全要求融入到外包活动的流程和操作规范中，参与外包管理的员工养成了安全意识，并有定期检查、审计、持续改进的机制
- (2) 能定期提出外包网络安全、数据安全提升规划

非原则性能力

- (1) 建立了针对知识产权的确认、审批，以及侵权事件的处理的管理流程
- (2) 形成了完善的文档模板和优秀实践文档库，根据服务外包管理的量化数据来辅助管理，并有持续优化机制



原则性能力

- (1) 通过了行业认可的服务连续性管理资质认证，组织发布了完善的服务连续性管理体系，并落实到外包项目和服务提供商管理中
- (2) 建立了对服务连续性管理的定期监测和年度评估机制，并利用监测指标和评估结果进一步优化服务连续性管理体系和机制

原则性能力

- (1) 遵照法律法规和监管要求建立了完备的外包活动合规要求识别、评估与处置、检查与回顾的管理制度与流程
- (2) 形成了完备的文档模板和优秀实践文档库，根据服务外包管理的量化数据有效辅助管理，持续优化机制有效
- (3) 近4年内无国家有关部门及监管相关公开处罚记录



3.5 D3-成效控制

P1 成本

非原则性能力

- (1) 建立了完备的组织级项目估算量化体系，有效指导外包项目工程造价的成本估算
- (2) 能够根据市场变化持续优化成本，成本核算机制有效

P2 质量

非原则性能力

- (1) 制定了完备的外包质量管全面理规范，包含量化外包质量管控流程、措施、监测方法
- (2) 建立外包质量指标体系，包括：缺陷密度、系统可用率、故障解决率、故障响应时间、故障解决时间、延期率、人员本科率、人员异动率、人员流失率、违规数
- (3) 有定期回检质量数据并改进的机制，组织级度量数据不断调优，外包质量管理数据呈上升趋势

P3 效率

非原则性能力

- (1) 建立了全面外包效率监控指标体系
- (2) 能定期回检效率数据并改进的机制，组织级度量数据不断调优，效率指标呈上升趋势





O4

总结







DISE 数智实审

感谢观看

演讲人：王科

日期：2025年7月23日



数字风险赋能中心

智审未来 数造精彩！

加入我们

感兴趣的朋友可以持续关注“数智实审”视频号！

Ø 大家可以关注视频号，私信回复‘进群’，获取微信生态群入口，获取直播PPT、标准汇编、标准解读报告、安全牛行业分析报告等众多福利！

Ø 宣讲团正在积极**招募分享嘉宾**，共同打造数字风险赋能新生态，期待您的加入！

