信息安全管理
先锋论坛

跟我学信息安全管理

信息安全管理实操 - 安全团队构建与管理　汪明

信息安全管理专家委员会发布
2016年7月

信息安全管理论坛（http://www.iso27001cn.com）成立于2014年9月，为国内目前最专业的信息安全管理学习和实践交流平台。是学习信息安全管理方法、分享实战经验、提升实践水平的好地方！

关于我们

我们提供

- 最全的信息安全管理资料
- 信安经理高薪工作机会推荐
- 每周专家讲堂（ 每周四晚上8点半YY频道89519382 ）
- 物美价廉的ISO27001课程团购

- 信息安全管理学习实践QQ群 207723402
- 微信 IT管理精英圈 itilxf_(记得有下划线)

欢迎关注

授课专家

汪明

资深IT管理咨询顾问及讲师，12年IT从业经验，包括6年20多个信息安全管理（ISO27001）、IT服务管理（ISO20000）、业务连续性管理（ISO22301）咨询项目经验，以及6年大型高科技制造型企业的信息系统架构规划与研发、IT项目管理及网络安全运维管理经验。

服务过的主要公司：

中国银行数据中心	中国银行软件中心	中国农业银行数据中心
华融资产	华夏银行	盛京银行
南充商业银行	山东省农信社	四川省农信社
上海期货交易所	中国金融期货交易所	中国证券登记结算
上海证券通信	兴业全球基金	陆金所
中银商务	上海讯联	上海银天下
中国南车	中国石化	苏州和舰科技

几个基本概念

组织 vs 团队

岗位 vs 角色

职责 vs 责任

ISO27002关于“A.6.1.1信息安全角色与职责”的指南

- 信息安全职责的分配与信息安全策略相一致。
- 识别各类资产的保护职责，也包括执行特定信息安全流程的职责。
- 定义信息安全风险管理活动，特别是残余风险接受的职责。
- 分配有信息安全职责的人员，具备相关能力，能够履行相关职责，能够与时俱进。

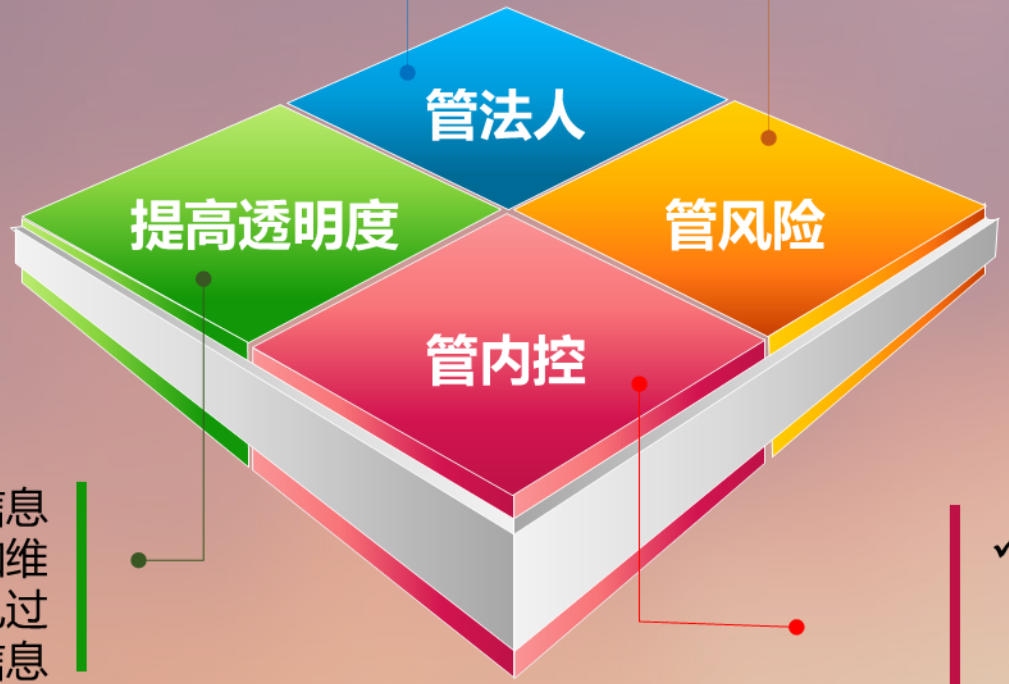
在许多组织中会任命一名信息安全管理人员，全面负责信息安全的开发和实施，并支持控制措施的识别。

然而，为控制措施提供资源并负责实施这些控制措施的职责通常归于各个管理人员。

一种通常的做法是为每一项资产指定一名责任人，负责该项资产的日常保护。

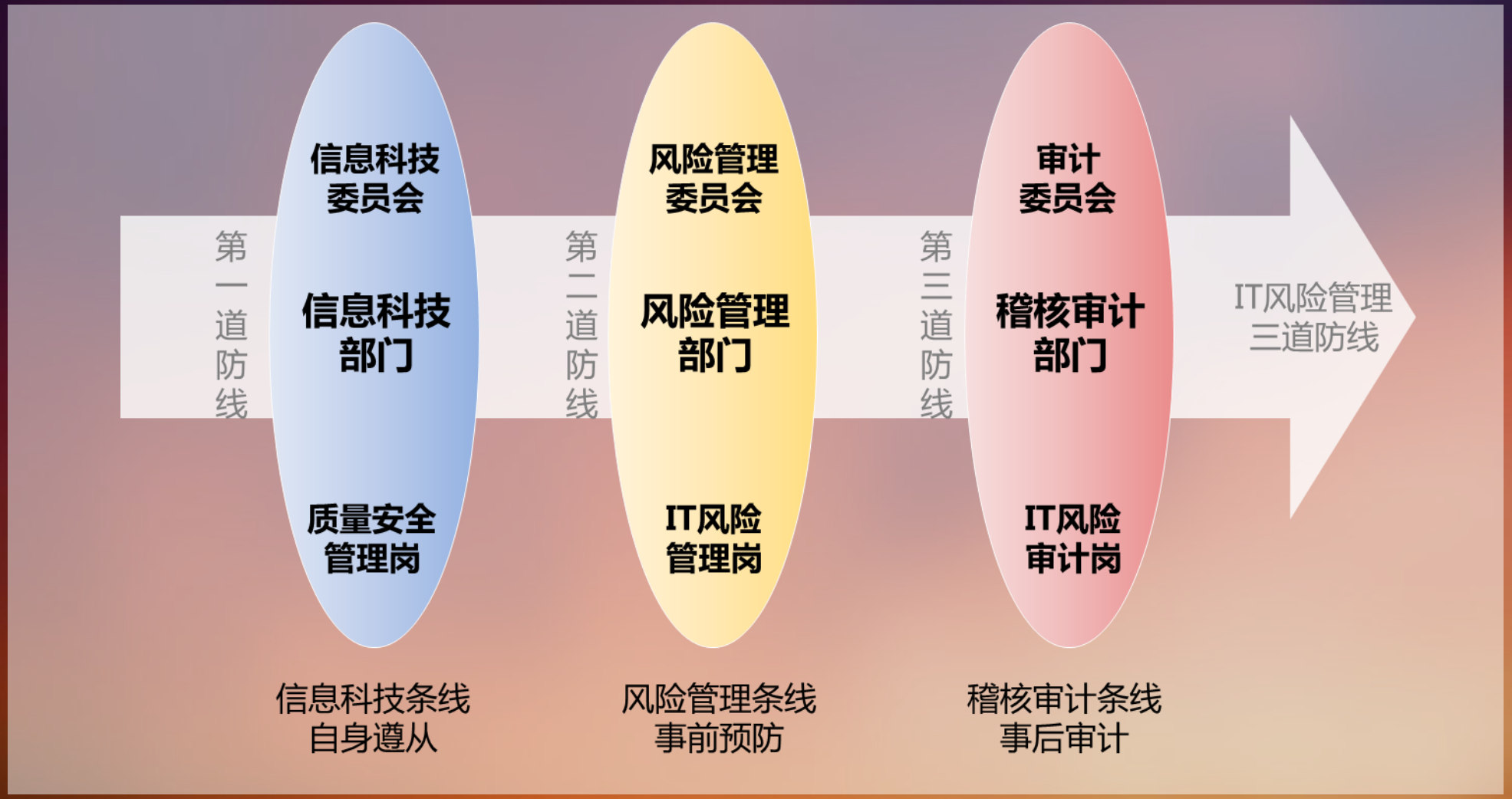
银监会关于信息科技风险管理的监管理念

- ✓ 指出商业银行法定代表人是本机构信息科技风险管理的第一责任人
- ✓ 要求商业银行建立有效的机制，实现对信息科技风险的识别、计量、监测和控制，提高信息技术使用水平



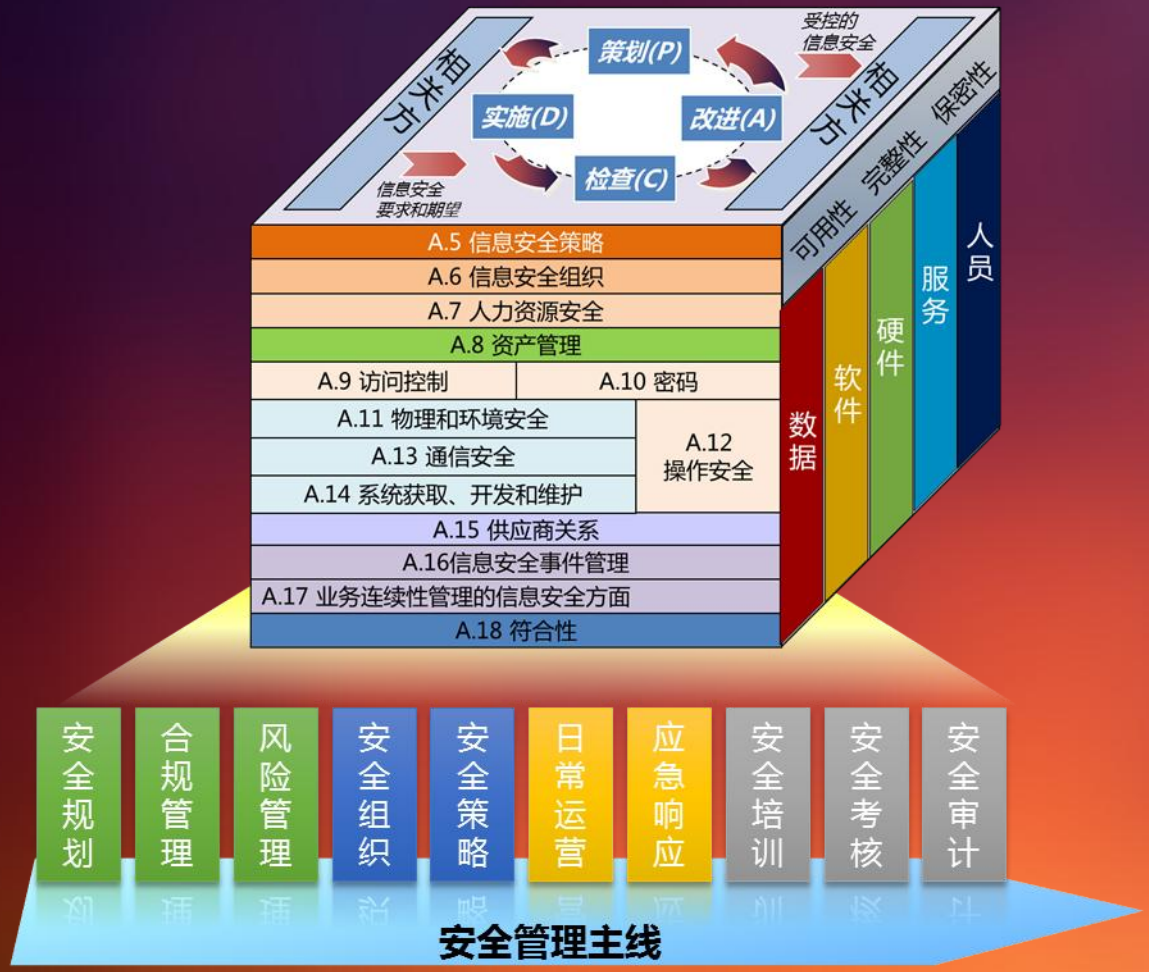
- ✓ 要求商业银行在信息系统开发、测试和维护，以及服务外包过程中加强对客户信息的保护，防止敏感信息泄露
- ✓ 要求商业银行建立完整的管理组织架构，制订完善的管理制度和流程

商业银行信息科技风险管理三道防线理念



从银监会的监管理念中，我们能获得哪些启示？

管理与技术的融合

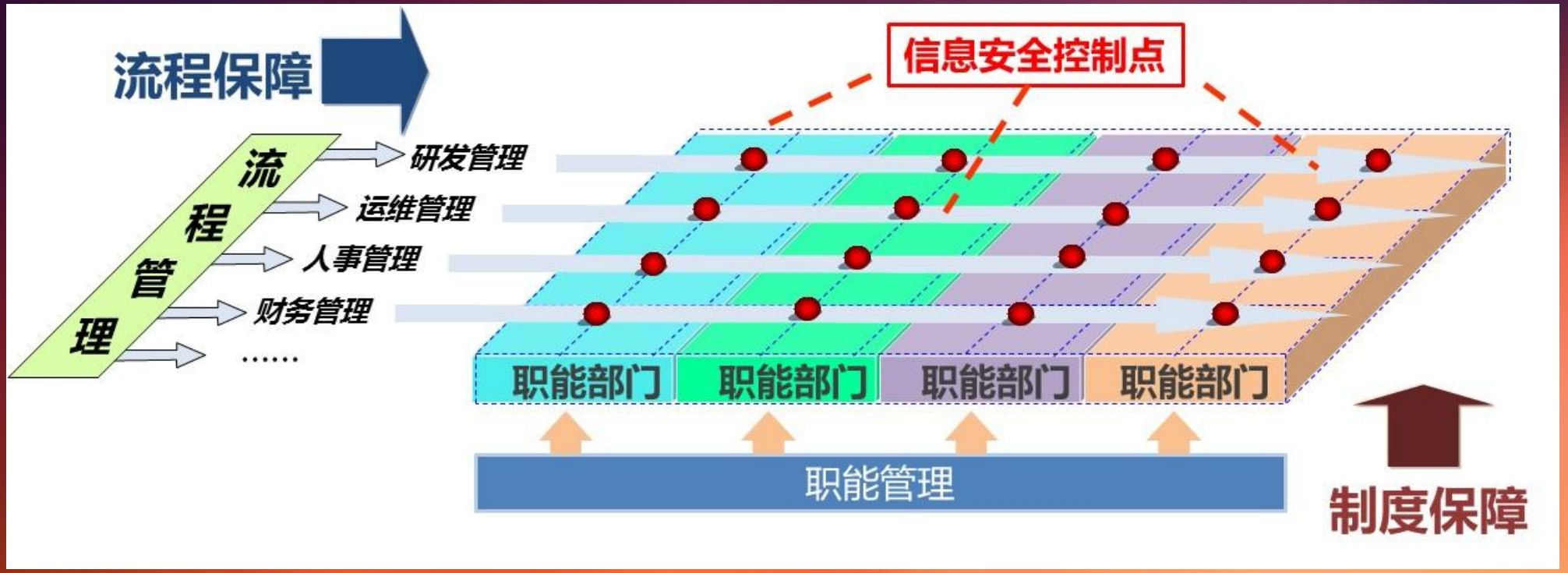


物理环境安全	• 机房建设与维护 • 设备安置保护
基础架构安全	• 网络架构安全 • 网络及主机入侵防护 • 系统安全加固 • 冗余与容灾 • 系统资源监控与容量管控 • 恶意程序防范 • 终端安全控制
应用安全	• 业务逻辑安全 • 系统设计安全、编码规范 • 代码安全检查、黑盒测试、渗透测试
数据安全	• 敏感信息鉴别、加密、脱敏 • 防泄漏、防篡改、抗抵赖 • 数据归档、备份与恢复 • 数据存储介质安全
访问控制	• 网络准入、账号权限管控 • 身份认证、会话管理
安全运维	• 操作行为审计 • 安全监控与事件响应 • 安全状态关联分析

安全技术主线

80%的安全控制要求可通过**技术手段**来实现
80%的安全控制要求需要靠**管理手段**来落实

信息安全职责的落实


流程保障
流程管理
研发管理
运维管理
人事管理
财务管理
.....
信息安全控制点
职能部门
职能部门
职能部门
职能部门
职能管理
制度保障

信息安全职责的落实

信息	数据	生成	存储	处理/传输	备份/归档	删除	销毁
信息资产	人员任职	前：筛选/入职	中：能力/责任/意识	后：转岗/离职			
	供应商项目	前：筛选/合同	中：监督/评价	后：交接/验收			
	硬件设备	容量计划	采购/入库	上架/投产	监控/巡检	下架/淘汰/报废	
	移动介质	登记/授权/发放	保管	使用	回收	销毁	
	采购的软件	申请/采购	登记/授权	使用	回收	升级/淘汰	
	开发的应用	需求分析	设计/编码	测试/验收	维护/升级	下线	
	网络与系统	规划设计	部署实施	监控/巡检	补丁升级	改造/优化	
	密钥	生成	存储	归档/检索	分发	回收	销毁
其他	账号权限	申请/审批	授权/分配	使用	审计	注销/回收	
	信息安全事件	事态监控/报告	评判	处理/上报	升级	证据收集	总结/改进

信息安全团队

狭义的信息安全团队

信息安全管理体系
维护团队

信息安全经理

信息安全技术团队

广义的信息安全团队

每一位资产责任人

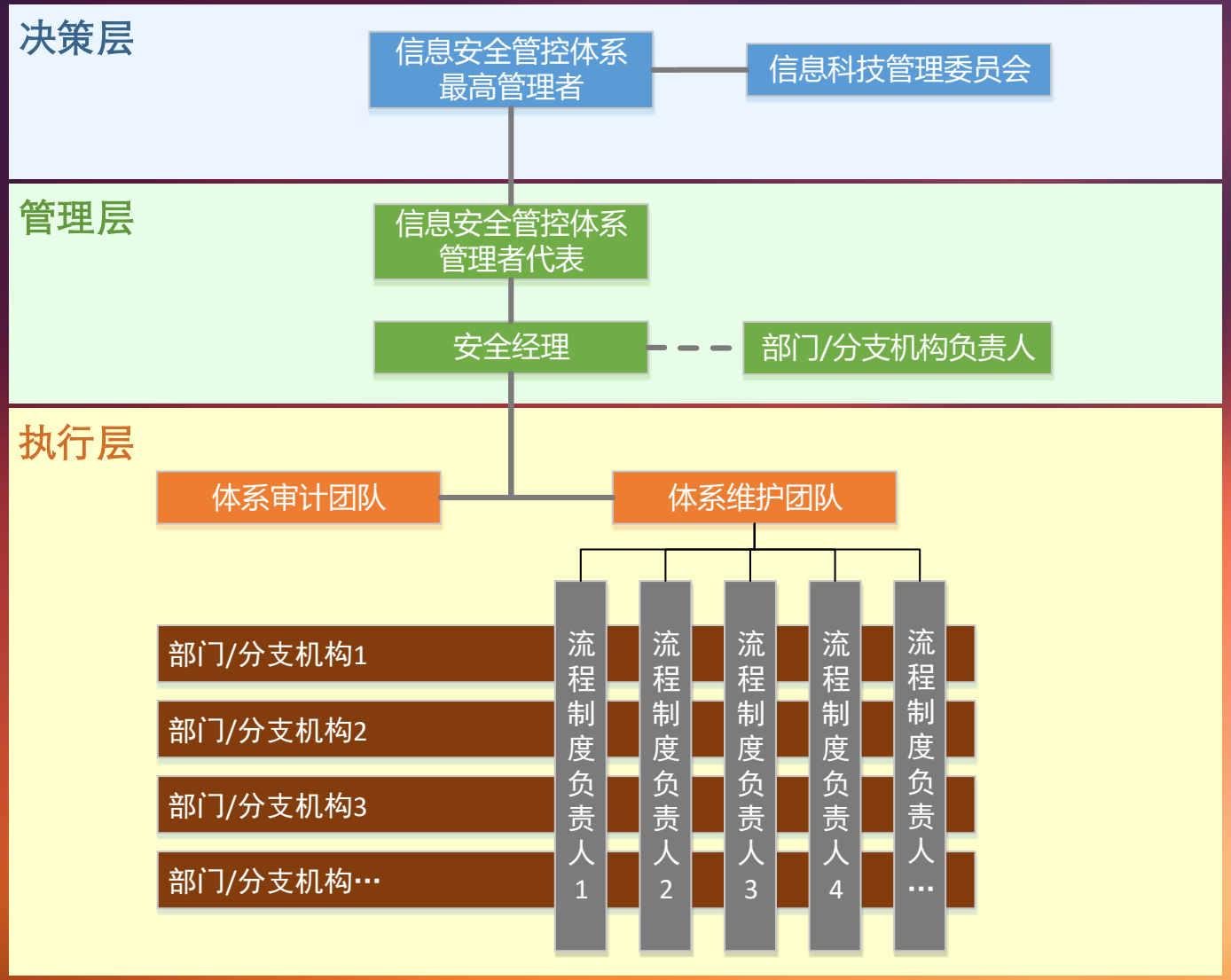
信息安全流程
的每一位参与者

职责

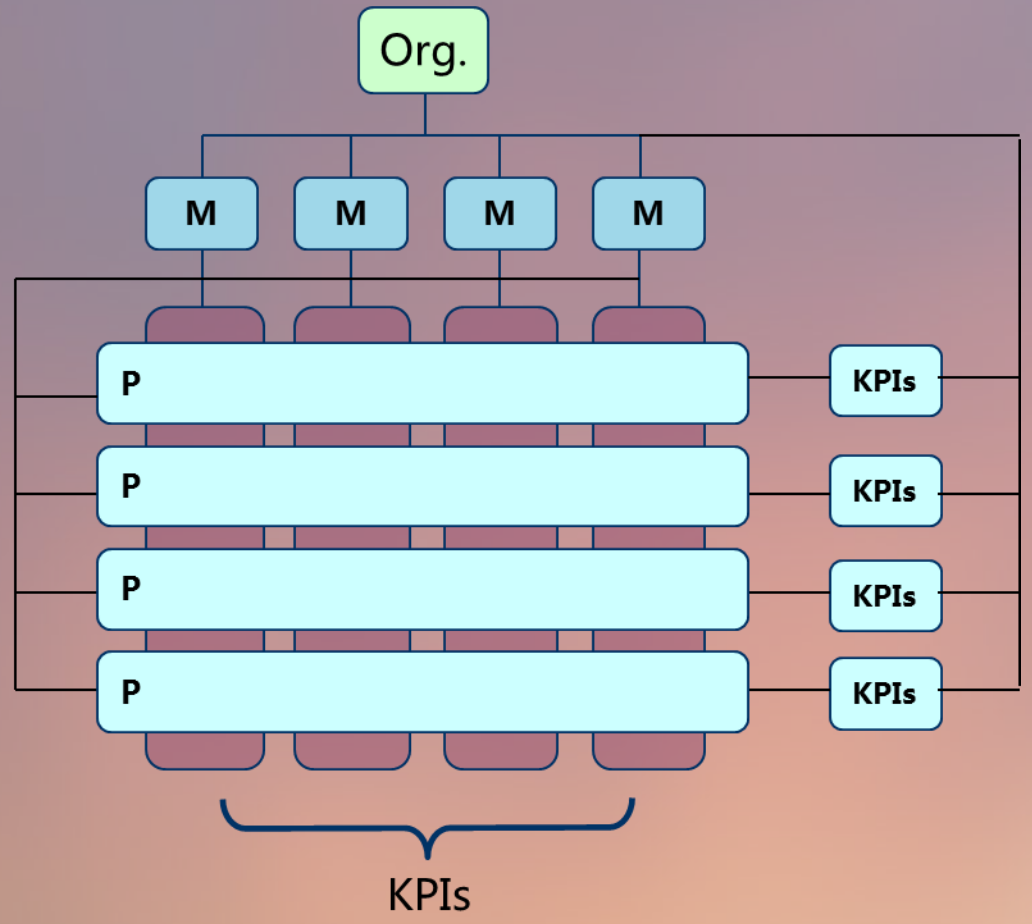
兼职的团队/角色
or
专职的部门/岗位

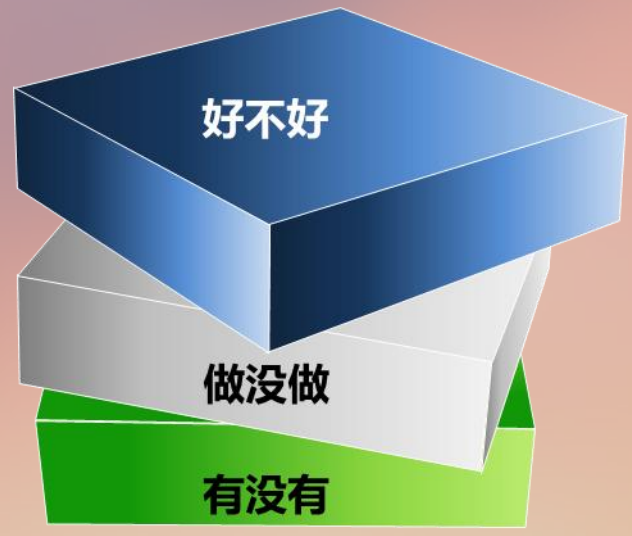
责任

信息安全管理体系的治理结构（示例）



信息安全团队绩效管理





M = 职能管理/岗位人员

KPI=关键绩效指标

信息安全管理与企业文化

管理体系建设：从人治走向法治

管理体系运行：从法治走向人治

Thank you

作者：汪明

特别鸣谢

北宙咨询 North Universe

Trendsetting Consulting

艾拓咨询 AituoXianfeng Consulting

特别鸣谢