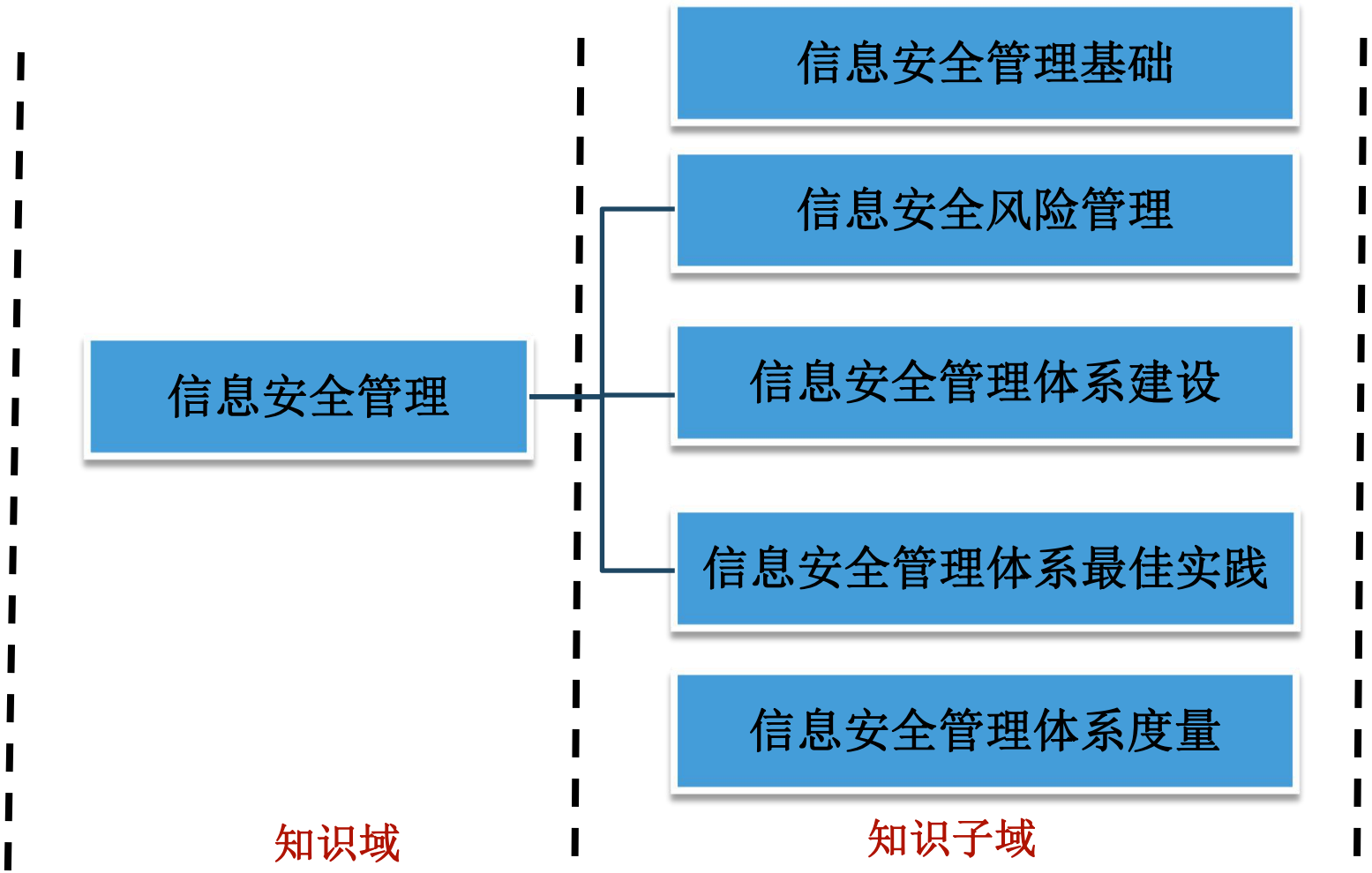
信息安全管理

版本：4.2

齐文振　　河南信安世纪

课程内容


信息安全管理
信息安全管理基础
信息安全风险管理
信息安全管理体系建设
信息安全管理体系最佳实践
信息安全管理体系度量
知识域
知识子域

知识子域：信息安全管理基础

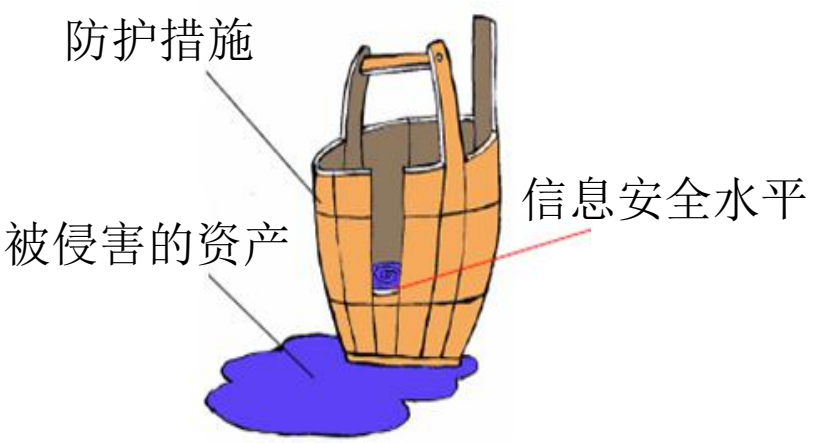
- 基本概念
  - 了解信息、信息安全管理、信息安全管理体系等基本概念。
- 信息安全管理的作用及对组织的价值
  - 理解信息安全管理的作用，对组织内部和组织外部的价值。

基本概念

- 信息
  - 企业：对用户的信息保护成为新的关注点
  - 用户：用户将安全作为选择服务的重要依据之一
  - 攻击者：不起眼的数据对攻击者可能价值很高，倒逼企业和个人更关注信息安全
- 信息安全管理
  - 信息安全管理是组织管理体系的一个重要环节
- 信息安全管理体系
  - 组织管理体系的一部分
  - 基于风险评估和组织风险接受水平

信息安全管理的作用及对组织的价值

- 信息安全管理的作用
  - 信息安全管理是组织整体管理的重要、固有组成部分，是组织实现其业务目标的重要保障
  - 信息安全管理是信息安全技术的融合剂，保障各项技术措施能够发挥作用
  - 信息安全管理能预防、阻止或减少信息安全事件的发生
- 对组织的价值
  - 对内
  - 对外



知识子域：信息安全风险管理

- 风险管理概述
  - 了解信息安全风险、风险管理的概念；
  - 理解信息安全风险管理的作用和价值；
- 常见风险管理模型
  - 了解COSO报告、ISO31000、COBIT等风险管理模型的作用。
- 安全风险管理基本过程
  - 理解风险管理的背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询六个方面的工作目标及内容；

风险管理基本概念

- 风险：事态的概率及其结果的组合
  - 风险是客观存在
  - 风险管理是指导和控制一个组织相关风险的协调活动，其目的是确保不确定性不会使企业的业务目标发生变化
  - 风险的识别、评估和优化
- 风险管理的价值
  - 安全措施的成本与资产价值之间的平衡

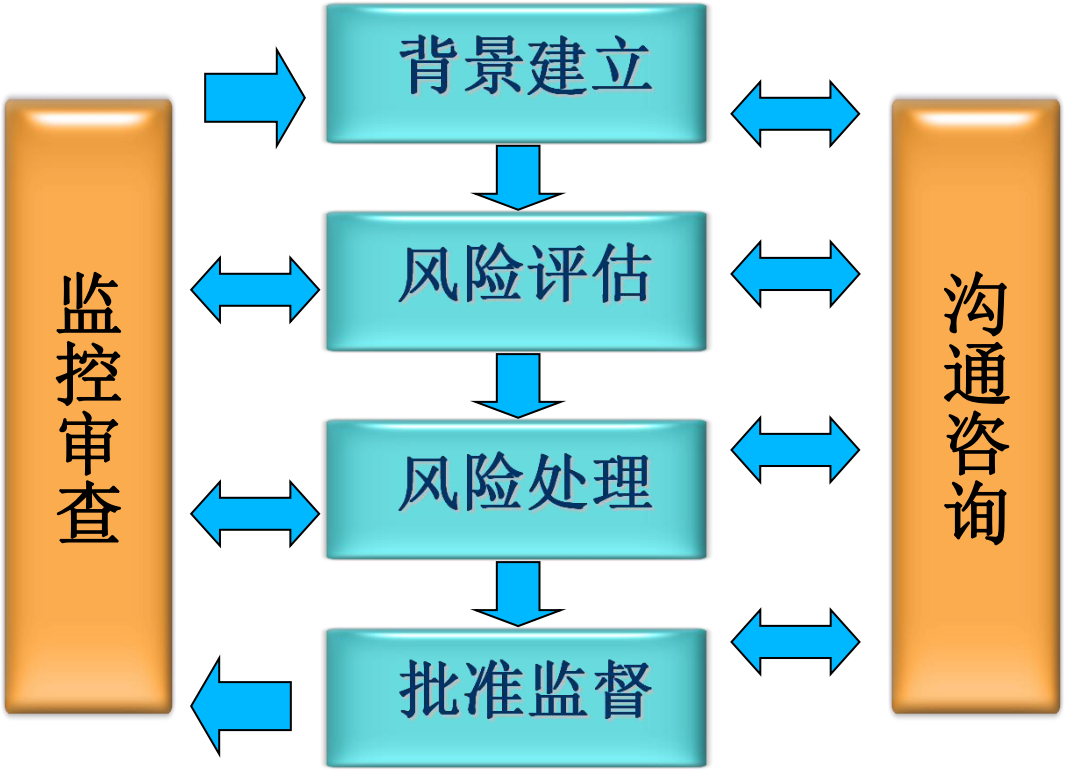
基于风险的思想是所有信息系统安全保障工作的核心思想！

常见风险管理模型

- 内部控制整合框架（COSO报告）
  - 三个目标：财务报告可靠性、经验效率和效果、合规性
  - 五个管理要素：内制环境、风险评估、控制活动、信息与沟通、监控
- ISO31000
  - 为所有与风险管理相关的操作提供最佳实践结构和指导
- COBIT
  - 为信息系统和技术的治理及控制过程提供最佳实践
  - 组件：框架、流程描述、控制目标、管理指南、成熟度模型

信息安全风险管理基本过程

- GB/Z 24364《信息安全风险管理指南》
  - 四个阶段
  - 两个贯穿



背景建立

- 背景建立是信息安全风险管理的第一步骤，确定风险管理的对象和范围，确立实施风险管理的准备，进行相关信息的调查和分析
  - 风险管理准备：确定对象、组建团队、制定计划、获得支持
  - 信息系统调查：信息系统的业务目标、技术和管理上的特点
  - 信息系统分析：信息系统的体系结构、关键要素
  - 信息安全分析：分析安全要求、分析安全环境

风险评估

- 信息安全风险管理要依靠风险评估的结果来确定随后的风险处理和批准监督活动
  - 风险评估准备：制定风险评估方案、选择评估方法
  - 风险要素识别：发现系统存在的威胁、脆弱性和控制措施
  - 风险分析：判断风险发生的可能性和影响的程度
  - 风险结果判定：综合分析结果判定风险等级

风险处理

- 风险处理是为了将风险始终控制在可接受的范围内。
  - 现存风险判断：判断信息系统中哪些风险可以接受，哪些不可以
  - 处理目标确认：不可接受的风险需要控制到怎样的程度
  - 处理措施选择：选择风险处理方式，确定风险控制措施
  - 处理措施实施：制定具体安全方案，部署控制措施

批准监督

- 批准：是指机构的决策层依据风险评估和风险处理的结果是否满足信息系统的安全要求，做出是否认可风险管理活动的决定

- 监督：是指检查机构及其信息系统以及信息安全相关的环境有无变化，监督变化因素是否有可能引入新风险

监控审查

- 监控与审查可以及时发现已经出现或即将出现的变化、偏差和延误等问题，并采取适当的措施进行控制和纠正，从而减少因此造成的损失，保证信息安全风险管理主循环的有效性

沟通咨询

- 通过畅通的交流和充分的沟通，保持行动的协调和一致；通过有效的培训和方便的咨询，保证行动者具有足够的知识和技能，就是沟通咨询的意义所在

沟通咨询
• 与**领导**沟通，以得到理解和批准 • **单位内部各有关部门相互**沟通，以得到理解和协作 • 与**支持单位和系统用户**沟通，以得到了解和支持
• 为所有层面的相关人员提供咨询和培训等，以提高人员的安全意识、知识和技能

知识子域：信息安全管理体系建设

- 信息安全管理体系成功因素
  - 理解GB/T 29246-2017中描述的信息安全管理体系成功的主要因素。
- PDCA过程
  - 理解PDCA过程模型的构成及作用；
  - 了解ISO/IEC 27001:2013中定义的PDCA过程方法四个阶段工作。

GB／T 29246-2017 信息技术 安全技术信息安全管理体系

ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29246—2017/ISO/IEC 27000:2016
代替 GB/T 29246—2012

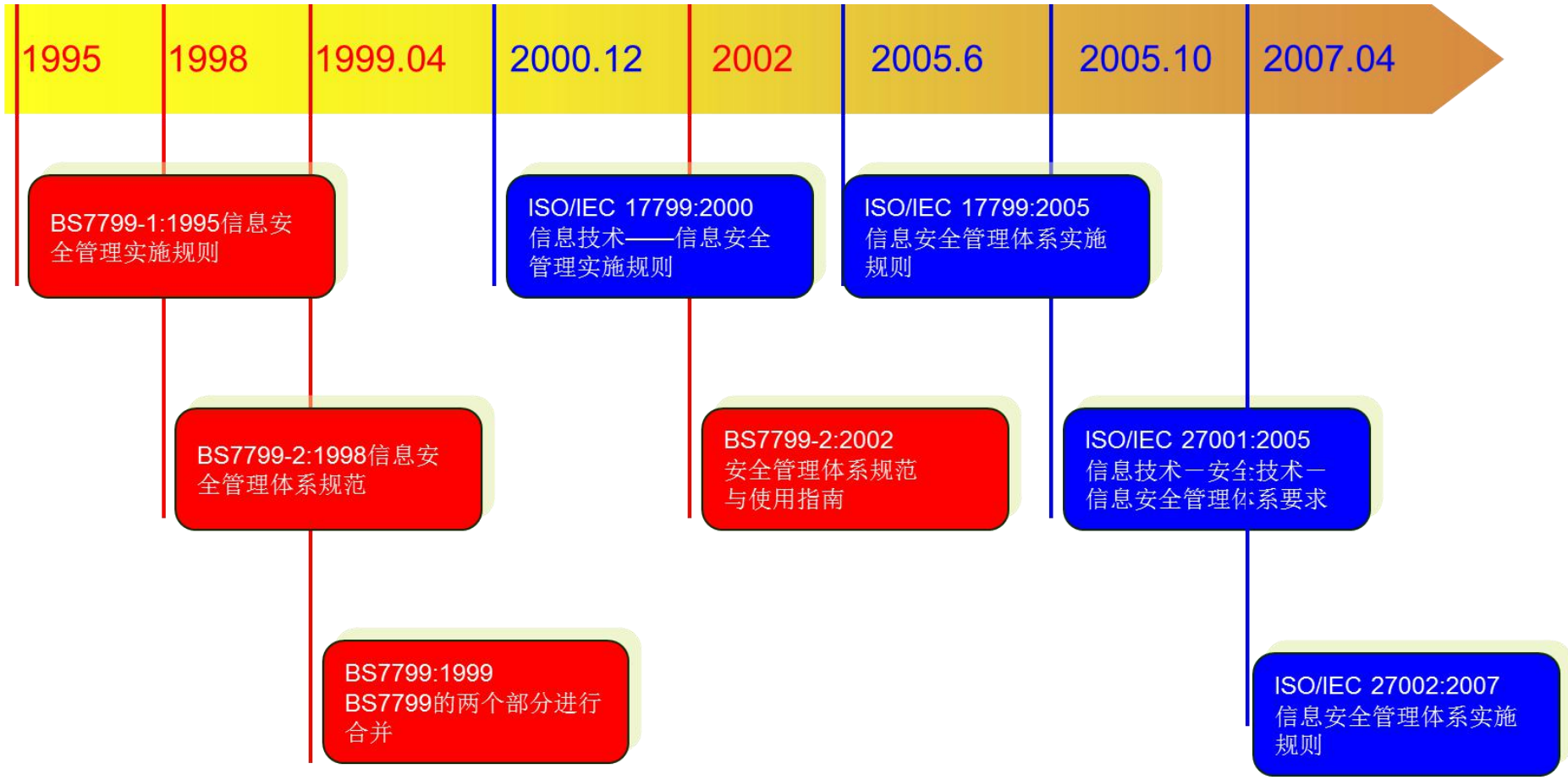
信息技术　安全技术
信息安全管理体系　概述和词汇

Information technology—Security techniques—
Information security management systems—Overview and vocabulary

(ISO/IEC 27000:2016,IDT)

IDT：等同采用 indentical
MOD：修改采用 modified
EQV：等效采用 equivalent
NEQ：非等效采用 noequivalen

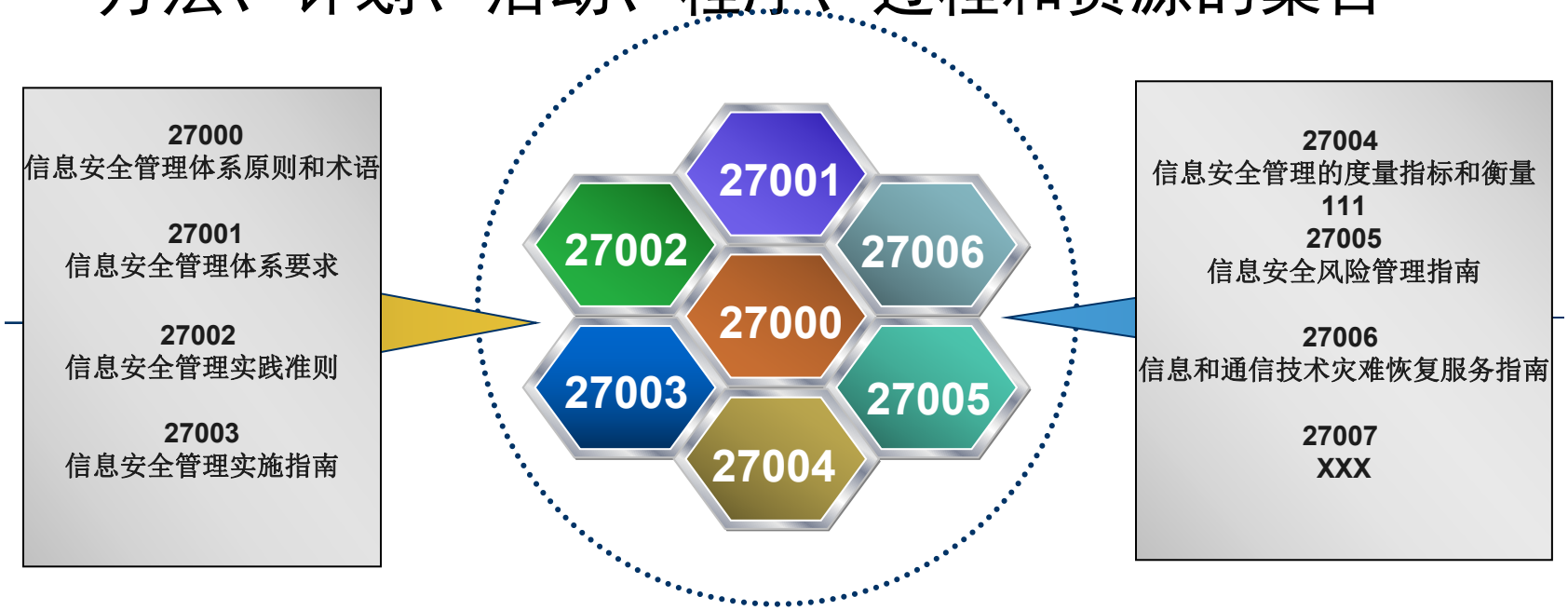
ISO27000标准的发展



信息安全管理体系建设

信息安全管理体系

- 组织在整体或特定范围内建立的信息安全方针和目标，以及完成这些目标所用的方法和体系。它是直接 管理活动的结果，表示为方针、原则、目标、方法、计划、活动、程序、过程和资源的集合



信息安全管理体系建设成功的因素

- 信息安全策略、目标和与目标一致的活动；
- 与组织文化一致的，信息安全设计、实施、监视、保持和改进的方法与框架；
- 来自所有管理层级、特别是最高管理者的可见支持和承诺；
- 对信息安全要求、风险评估和风险管理有好的理解；

信息安全管理体系建设成功的因素

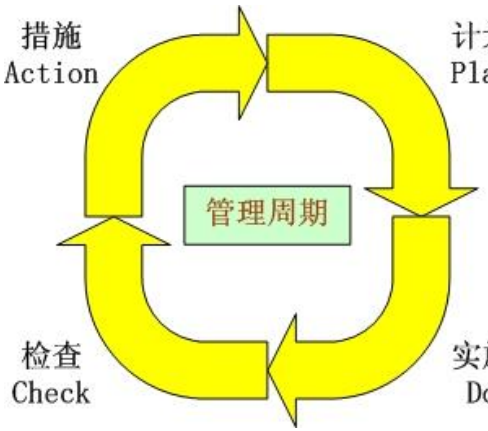
- 有效的信息安全意识、培训和教育计划，已使所有员工和其他相关方知悉在信息安全策略、标准等当中他们的信息安全义务，并激励他们做出相应的行动；
- 有效的信息安全事件管理过程；
- 有效的业务持续性管理方法；
- 评价信息安全管理性能的测量系统和反馈的改进建议。

信息安全管理体系模型

PDCA信息安全管理模型：任何信息安全事务的规律

针对检查结果采取应对措施，改进安全状况。

根据风险评估结果、法律法规要求、组织业务运作自身需要来确定控制目标与控制措施。

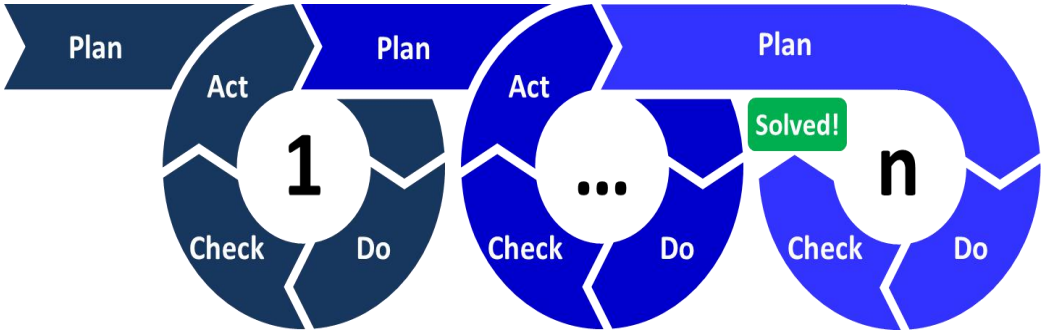


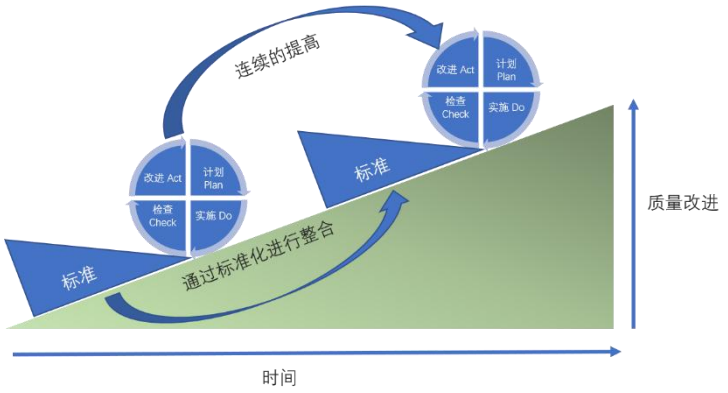
依据策略、程序、标准和法律法规，对安全措施的实施情况进行符合性检查。

实施所选的安全控制措施。

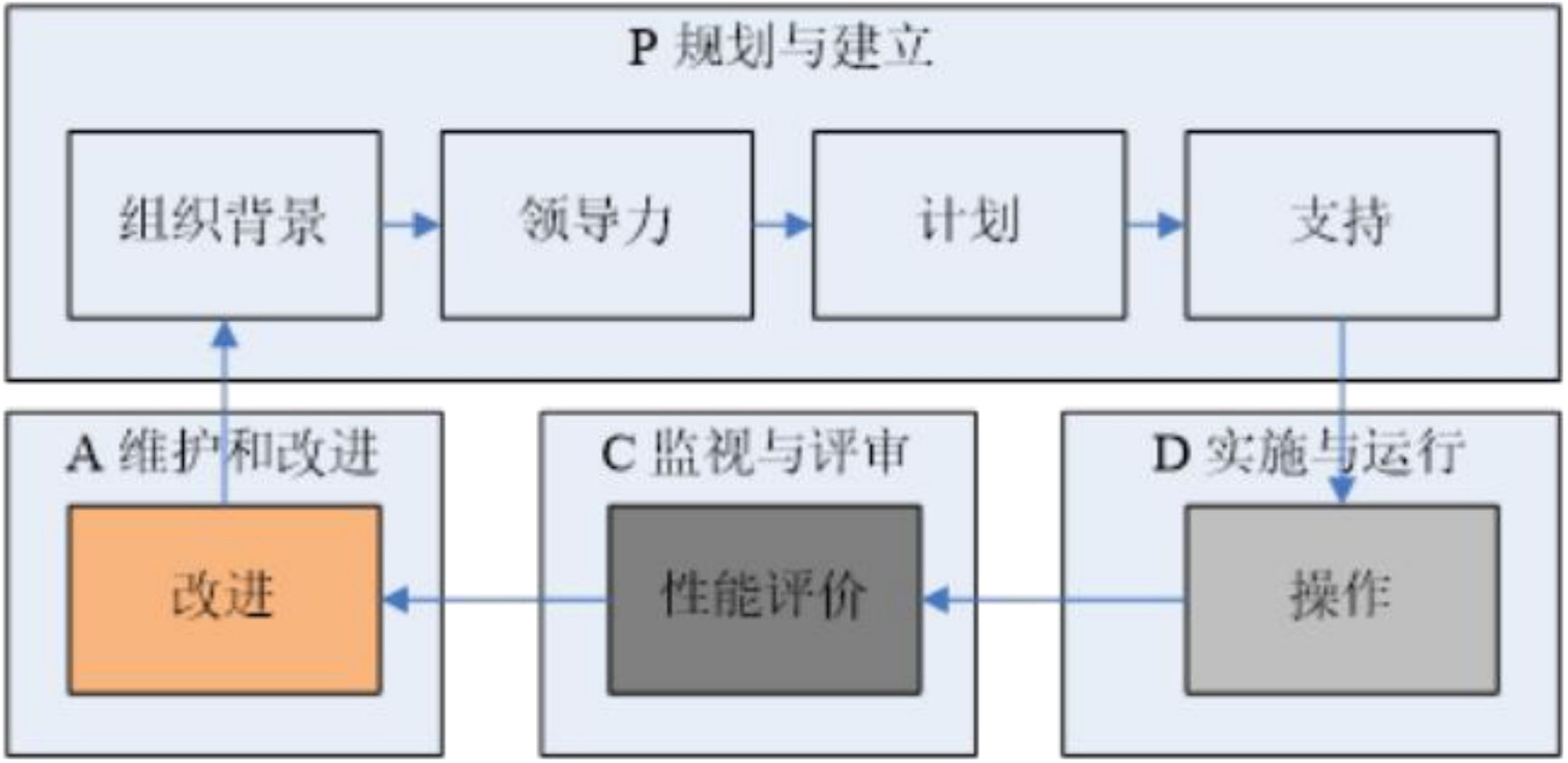
PDCA过程方法

- 管理学常用的过程模型
  - P（Plan）：计划、策划
  - D（Do）：实施、执行、行动
  - C（Check）：检查、论证、分析
  - A（Act）：处置、处理、改进、
- 按照PDCA 进行循环，大环套小环，持续改进
- PDCA是27001定义的过程方法





27001中定义的PDCA过程方法阶段工作



知识子域：信息安全管理体系建设

- 信息安全管理体系建设过程
  - 掌握规划与建立阶段组织背景、领导力、计划、支持等主要工作的内容；
  - 理解实施与运行、监视和评审、维护和改进阶段工作内容。
- 文档化
  - 理解文档化的重要性并了解文件体系及文件控制的方式。

规划与建立

- 组织背景
  - 建立信息安全管理体系的基础
  - 了解组织有关信息安全的内部（人员、管理、流程等）和外部（合作伙伴、供应商、外包商等）问题
  - 确定ISMS管理范围
  - 建立、实施、运行、保持和持续改进符合国际标准要求的ISMS

规划与建立

- 领导力
  - 管理承诺是建立信息安全管理体系的关键成功因素之一
  - 建立在组织的整体管理基础，需要组织整体参与
  - 组织高层确定的信息安全方针并文档化，明确描述组织的角色、职责和权限

规划与建立

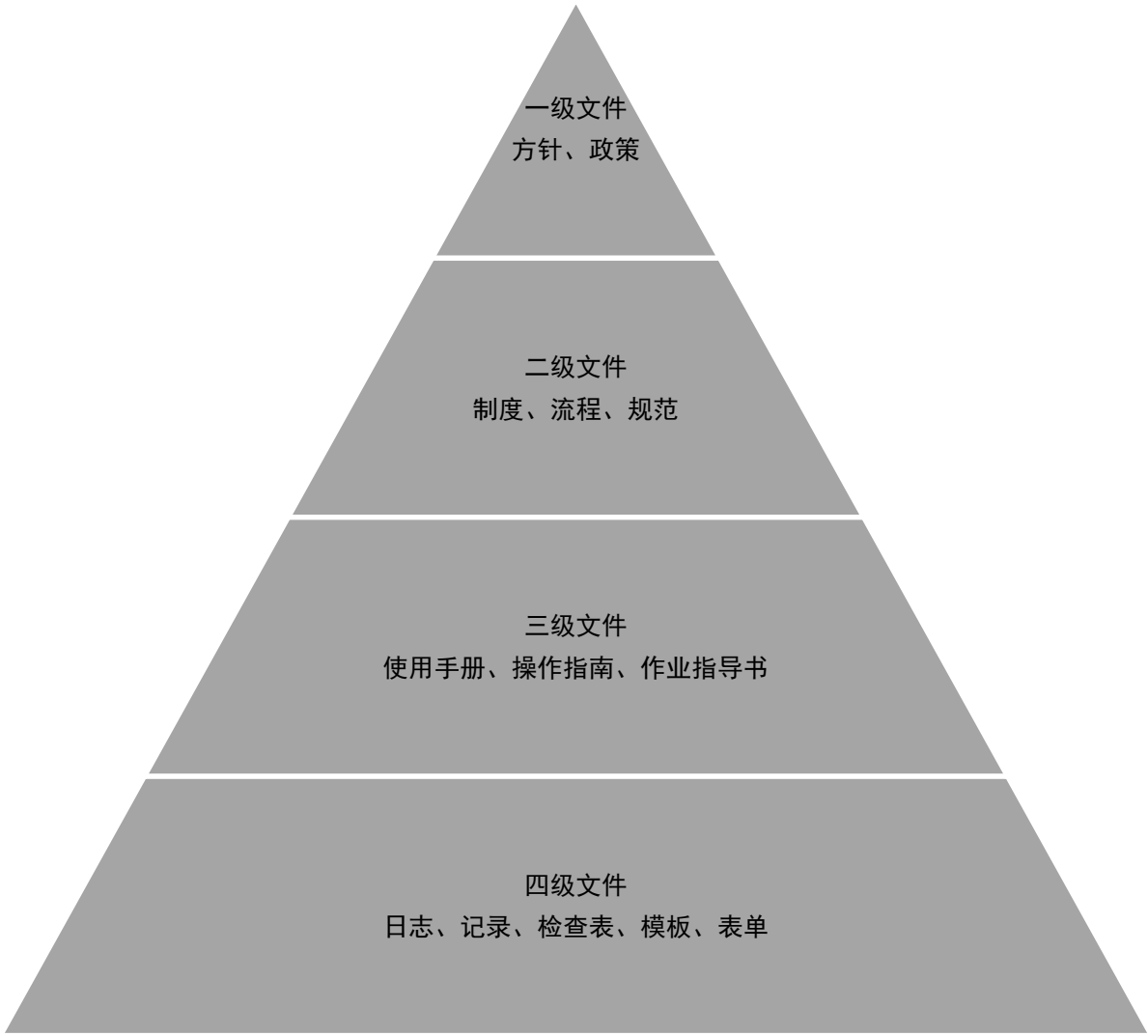
- 计划
  - 计划建立在风险评估基础上
  - 计划必须符合组织的安全目标
  - 层次改进
- 支持
  - 获得资源
  - 全员宣贯培训

实施与运行

- 实施与运行
  - 实施风险评估，确定所识别信息资产的信息安全风险以及处理信息安全风险的决策，形成信息安全要求
  - 控制措施适度安全
  - 控制在适用性声明中形成文件
- 监视和评审
  - 根据组织政策和目标，监控和评估绩效来维护和改进ISMS
- 维护与改进
  - 不符合和纠正措施
  - 持续改进

文档化

- 文档结构
- 文件控制
  - 建立
  - 批准发布
  - 评审与更新
  - 文件保存
  - 文件作废



知识子域：信息安全管理体系最佳实践

- 信息安全管理体系控制类型
  - 了解预防性、检测性、纠正性控制措施的差别及应用。
- 信息安全管理体系控制措施结构
  - 了解安全方针、信息安全组织、人力资源安全、资产管理、访问控制、密码学、物理和环境安全、操作安全、通信安全、安全采购开发和维护、供应商关系、安全事件管理、业务连续性管理及合规性14个控制章节的控制目标、控制措施并理解实施指南的相关要素。

信息安全管理体系（ISMS）应该包含什么内容？

- 有效的信息安全组织架构
- 全面的信息安全策略、制度和程序
- 按照计划实施各项风险控制措施
- 所有人员都具备信息安全意识并承担相应责任
- 在日常工作中实践信息安全
- 需要必要的资源支持

安全控制措施内部结构

- 结构
  - 14个类别
  - 35个目标
  - 114个控制措施
- 描述方式
  - 控制类
  - 控制目标
  - 控制措施
  - 实施指南

信息安全方针

- 控制目标:组织的安全方针能够依据业务要求和相关法律法规提供管理指导并支持信息安全
- 控制措施
  - 信息安全方针
    - 信息安全方针应由管理者批准、发布并传达给所有员工和外部相关方
  - 信息安全方针评审
    - 宜按计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保它持续的适宜性、充分性和有效性

信息安全组织

- 内部组织
  - 控制目标：建立一个管理框架，用以启动和控制的组织内信息安全的实施和运行
  - 控制措施
    - 信息安全的角色和职责、职责分离、与政府部门的联系、与相关利益方的联系、项目管理的信息安全
- 移动设备与远程办公
  - 控制目标：确保远程办公和使用移动设备时的安全性
  - 控制措施
    - 移动设备方针，管理移动带来的风险
    - 保护远程工作地点的信息访问、处理和存储

人力资源安全

- 任用前
  - 控制目标：确保雇员、承包方理解其职责，对其考虑的角色是适合的
  - 控制措施：审查、任用条款及条件
- 任用中
  - 控制目标：确保雇员、承包方意识并履行其信息安全职责
  - 控制措施：管理职责、意识教育和培训、纪律处理
- 任用终止和变化
  - 控制目标：将聘用的变更或终止作为组织过程的一部分以保护组织的利益
  - 控制措施：雇佣责任的改变和终结

资产管理

- 对资产负责
  - 控制目标：标识组织资产并确定适当的保护责任
  - 控制措施：资产清单、资产责任人、资产的可接受使用、资产归还
- 信息分类
  - 控制目标：确保信息受到适当级别的保护
  - 控制措施：分类指南、信息的标记、资产的处理
- 介质处理
  - 控制目标：防止介质存储信息的未授权泄露、修改、移动或销毁
  - 控制措施：可移动介质的管理、介质的处置、物理介质传输

访问控制

- 访问控制的业务要求
  - 控制目标：限制对信息和信息处理设施的访问。
  - 控制措施：访问控制方针、网络和网络服务的访问
- 用户访问管理
  - 控制目标：确保授权用户访问系统和服务，并防止未授权的访问
  - 控制措施：用户注册和注销、用户访问配置、特殊权限管理、用户的秘密验证信息管理、用户访问权的复查、访问权限的移除或调整

访问控制

- 用户职责
  - 控制目标：使用户负责维护其授权信息。
  - 控制措施：秘密验证信息的使用
- 系统和应用访问控制
  - 控制目标：防止对系统和应用的未授权访问。
  - 控制措施：信息访问限制、安全登录规程、口令管理系统、特权实用程序的使用、程序源代码的访问控制

密码学

- 控制目标：通过加密方法保护信息的保密性、真实性或完整性。
- 控制措施：
  - 使用加密控制的策略
  - 密钥管理

物理与环境安全

- 安全区域
  - 控制目标：防止对组织场所和信息过程设备的未授权物理访问、损坏和干扰。
  - 控制措施：物理安全边界、物理入口控制、办公室、房间和设施的安全保护、外部和环境威胁的安全防护、在安全区域工作、送货和装卸区
- 设备安全
  - 控制目标：防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断
  - 控制措施：设备安置和保护、支持性设施、备维护
  - 资产的移动、……

操作安全

- 操作规程和职责
  - 控制目标：确保正确、安全地操作信息处理设施
  - 控制措施：文件化的操作规程变更管理、容量管理、开发、测试和运行设施分离
- 恶意代码防范
  - 控制目标：保护信息和信息处理设施以防恶意代码
  - 控制措施：控制恶意代码
- 备份
  - 控制目标：防止数据丢失
  - 控制措施：信息备份

操作安全

- 日志记录和监视
  - 控制目标：记录事件并生成证据。
  - 控制措施：事件日志、日志信息的保护、管理员和操作员日志、时钟同步
- 操作软件控制
  - 控制目标：确保操作系统的完整性。
  - 控制措施：操作系统软件的安装
- 技术漏洞管理
  - 控制目标：防止对技术漏洞的利用。
  - 控制措施：技术脆弱性管理、软件安装限制

操作安全

- 信息系统审计的考虑
  - 控制目标：极小化审计行为对业务系统带来的影响
  - 控制措施：信息系统审计控制

通信安全

- 网络安全管理
  - 控制目标：确保网络中信息和支持性基础设施的安全性
  - 控制措施：网络控制、网络服务安全、网络隔离
- 信息的交换
  - 控制目标：保持组织内以及与组织外信息交换的安全。
  - 控制措施：信息交换策略和规程、信息交换协议、电子消息、保密或不披露协议

信息获取开发及维护

- 信息系统的安全要求
  - 控制目标：确保信息安全是信息系统生命周期中的一个有机组成部分。这同样包含了在公共网络上提供服务的信息系统的要求。
  - 控制措施：安全需求分析和说明、公共网络上的安全应用服务、应用服务交换的保护
- 开发和支持过程中的安全
  - 控制目标：确保信息系统开发的生命周期中设计和实施的信息安全。
  - 控制措施：安全开发策略、系统变更控制规程、操作系统变更后应用的技术评审、软件包变更的限制、安全系统工程原理、……

信息获取开发及维护

- 开发和支持过程中的安全
  - 控制目标：确保信息系统开发的生命周期中设计和实施的信息安全。
  - 控制措施：安全开发策略、系统变更控制规程、操作系统变更后应用的技术评审、软件包变更的限制、安全系统工程原理、…….
- 测试数据
  - 控制目标：确保用于测试的数据得到保护
  - 控制措施：测试数据的保护

供应商关系

- 供应商关系中的信息安全
  - 控制目标：确保供应商可访问的组织资产受到保护
  - 控制措施：供应商关系的信息安全方针、供应商协议中解决安全问题、信息和通信技术的供应链
- 供应商服务交付管理
  - 控制目标：根据供应协议，维持信息安全和服务交付在协定的等级
  - 控制措施：监控和审查供应商服务、供应商服务变更管理

信息安全事件管理

- 信息安全事件的管理和改进
  - 控制目标：确保采用一致和有效的方法对信息安全事件进行管理，包括通信安全事件和弱点。
  - 控制措施：
    - 职责和规程
    - 信息安全事态报告
    - 信息安全弱点报告
    - 信息安全事态的评估和决策
    - 信息安全事件的响应
    - 从信息安全事件中学习
    - 证据的收集

业务连续性管理

- 信息安全的连续性
  - 控制目标：应将信息安全连续性嵌入组织业务连续性管理之中。
  - 控制措施：信息安全连续性的计划、信息安全连续性的实施、信息安全连续性的确认、审查和评估
- 冗余
  - 控制目标：确保信息过程设施的可用性。
  - 控制措施：信息过程设施的可用性

符合性

- 符合法律和合同规定
  - 控制目标：避免违反任何法律、法令、法规或合同义务，以及任何安全要求
  - 控制措施：可用法律和合同要求的识别、知识产权、记录的保护、个人身份信息的隐私和保护、加密控制的监管
- 信息安全审核
  - 控制目标：确保信息安全依据组织方针和规程实施和操作。
  - 控制措施：信息安全的独立审核、符合安全策略和标准、技术符合性核查

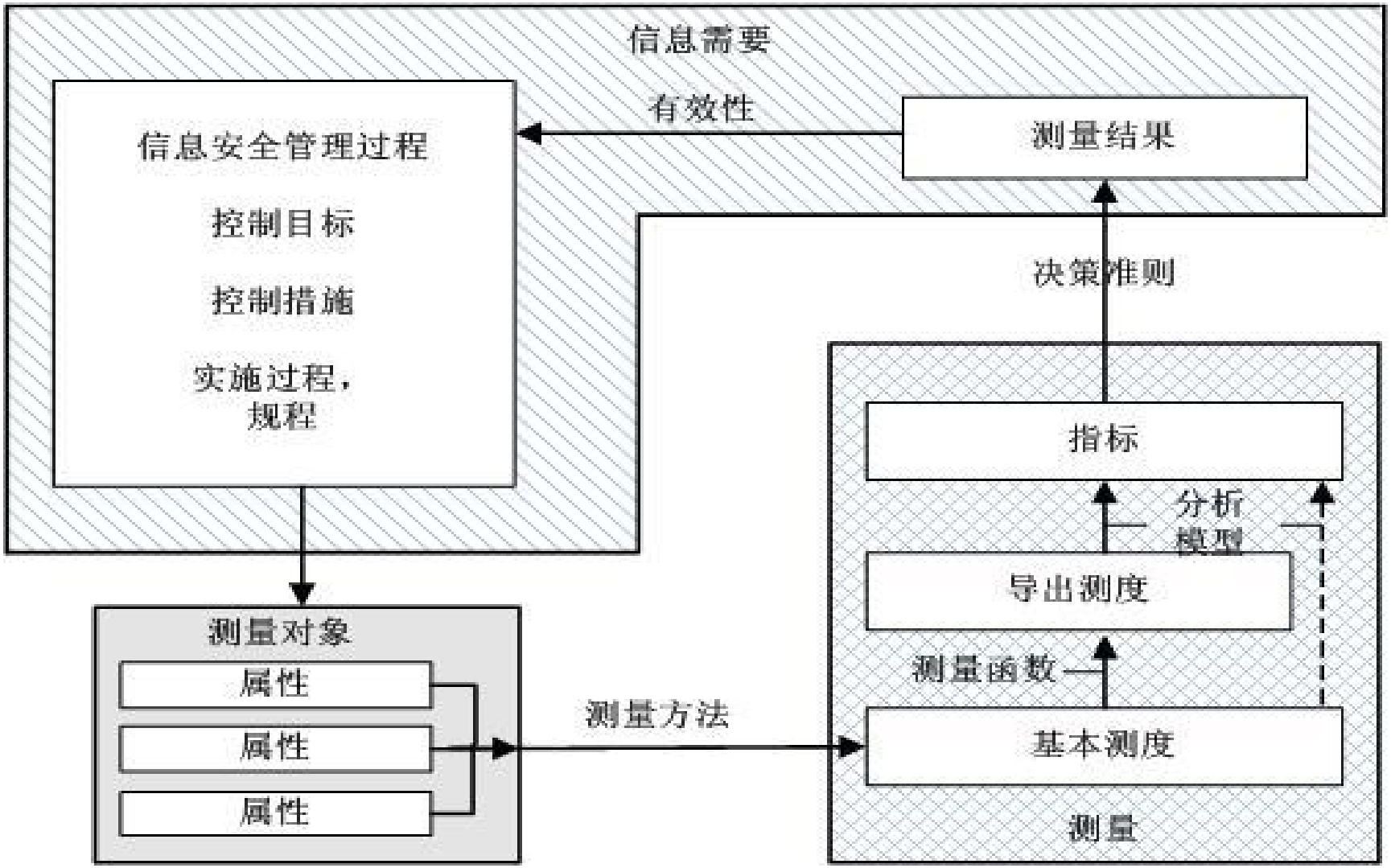
知识子域：信息安全管理体系度量

- 基本概念
  - 了解ISMS测量的基本概念、方法选择、作用；
  - 了解27004定义的测量模型。
- 测量要求与实现
  - 了解测量实现的工作内容。

基本概念

- 测量的概念
  - 根据多个因素选择合理的测量方法
- 测量的目的
  - 帮助管理层识别和评价不符合和无效的控制措施
  - 帮助组织展示与组织信息安全管理体系的符合程度，并能产生管理评审过程的输入

27004测量模型


信息需要
有效性
信息安全管理过程
控制目标
控制措施
实施过程，
规程
测量结果
决策准则
指标
分析
模型
导出测度
测量函数
基本测度
测量
测量对象
属性
属性
属性
测量方法

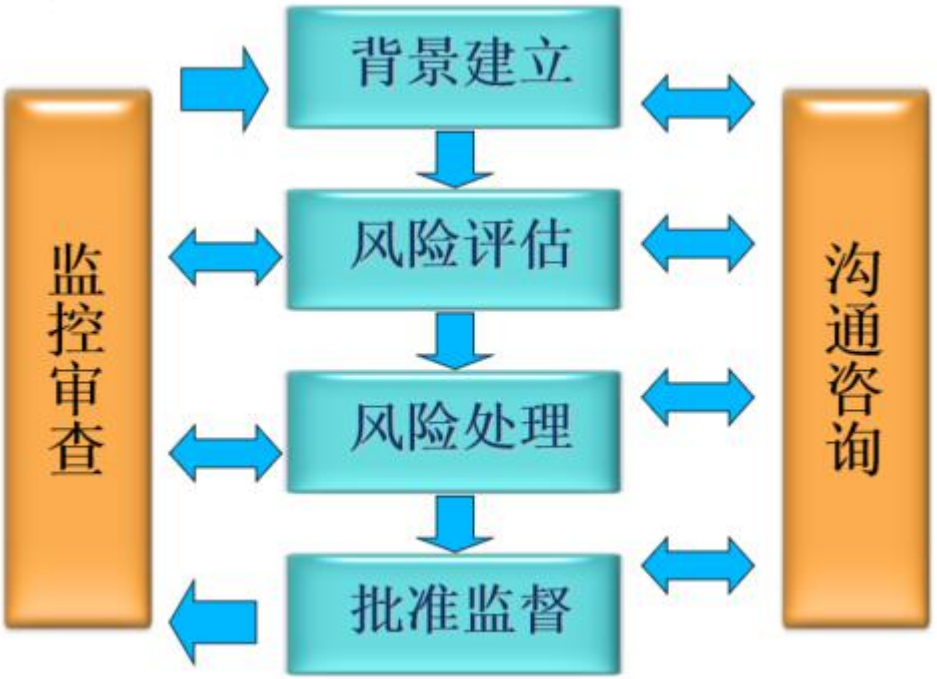
测量要求与实现

- 管理职责：管理者建立测量方案，利益相关者参与测量活动
- 测度和测量开发：建立测量所需活动及测度
- 测量运行：收集、存储和验证被用来创建信息安全测度的数据
- 测量分析和报告：对已收集的数据进行分析并提交报告
- 测量项目评价和改进

总结

- 信息安全管理基础
  - 信息、信息安全管理、信息安全管理体系
- 信息安全风险管理
  - 风险管理作用
  - 风险管理过程方法
- 信息安全管理体系建设
  - PDCA
  - 信息安全管理体系最佳实践
- 信息安全测量

- 在风险管理工作中，下列哪项工作实现的是“过程质量管理”工作？
- A. 沟通咨询
- B. 风险评估
- C. 审核批准
- D. 监控审查



信息安全管理体系是基于（）方法，来建立、实施、动作、监视、评审、保持和改进信息安全。

- A. 信息安全
- B. 业务风险
- C. 信息系统防护
- D. 安全风险

CISP

谢谢，请提问题！