
IT治理基础
IT治理的驱动因素
（1）良好的 IT 治理能够确保组织 IT 投资有效性
（2）IT 属于知识高度密集型领域，其价值发挥的弹性较大
（3）IT 已经融入组织管理、运行、生产和交付等各领域中，成为各领域高质量发展的重要基础
（4）信息技术的发展演进以及新兴信息技术的引入，可为组织提供大量新的发展空间和业务机会等
（5）IT 治理能够推动组织充分理解IT 价值，从而促进IT 价值挖掘和融合利用
（6）IT 价值不仅仅取决于好的技术，也需要良好的价值管理，场景化的业务融合应用
（7）高级管理层的管理幅度有限，无法深入到 IT 每项管理当中，需要采用明确责权利和清晰管理去确保IT 价值
（8）成熟度较高的组织以不同的方式治理 IT，获得了领域或行业领先的业务发展效果
IT治理的目标价值
与业务目标一致
IT 治理要从组织目标和数字战略中抽取信息与数据需求和功能需求，形成总体的 IT 治理框架和系统整体模型，为进一步系统设计和实施奠定基础，保证信息技术开发利用跟上持续变化的业务目标
有效利用信息与数据资源
通过 IT 治理对信息与数据资源的管理职责进行有效管理，保证投资的回收，并支持决策
风险管理
IT 治理重视风险管理，通过制定信息与数据资源的保护级别，强调对关键的信息与数据资源，实施有效监控和事件处理
IT 治理的管理层次
最高管理层
证实IT战略与业务战略是否一致；证实通过明确的期望和衡量手段交付IT 价值；指导IT 战略、平衡支持组织当前和未来发展的投资；指导信息和数据资源的分配
执行管理层
制定IT 的目标；分析新技术的机遇和风险；建设关键过程与核心竞争力；分配责任、定义规程、衡量业绩；管理风险和获得可靠保证等
业务与服务执行层
信息和数据服务的提供和支持；IT 基础设施的建设和维护；IT 需求的提出和响应


IT 治理关键决策
IT 原则
组织高层关于如何使用IT的陈述
IT 架构
组织从一系列政策、关系以及技术选择中捕获为购买或内部开发IT应用确定业务需求 关于应该在IT的哪些方面投资以及投资多少的决策，包括项目的审批和论证技术的数据、应用和基础设施的逻辑，以达到预期和商业、技术的标准化和一体化
IT 基础设施
集中协调、共享IT服务可以给组织的IT能力提供基础
业务应用需求
为购买或内部开发IT应用确定业务需求
IT 投资和优先顺序
关于应该在IT的哪些方面投资以及投资多少的决策，包括项目的审批和论证技术
IT 治理体系框架
IT 战略目标
为实现IT 价值和目标，使组织从IT 投入中获得最大收益，而针对 IT 与业务关系、IT 决策、IT 资源利用、IT 风险控制等方面制定的目标
IT 治理组织
界定组织中各相关主体在各自方面的治理范围、责权利及其相互关系的准则，它的核心是治理机构 (如IT 治理委员会等) 的设置和权限的划分
IT 治理机制
IT 治理决策机制、执行机制、风险控制机制、协调机制的综合体，各机制之间是相辅相成、相互促进的关系
IT 治理域
在IT 治理的规则之下，对组织的 IT 资源进行整合与配置，根据IT 目标所采取的行动
IT 治理标准
IT 治理基本规范、IT 治理实施参照、IT 治理评价体系和 IT 治理审计方法等方面，作为组织实施 IT 治理最佳实践和对标依据
IT 绩效目标
关注 IT 价值的实现，评价 IT 规划与 IT 构建过程中是否满足业务需求以及构建过程中的工期、成本、质量是否达到目标

1.IT治理

IT治理体系

IT 治理核心内容

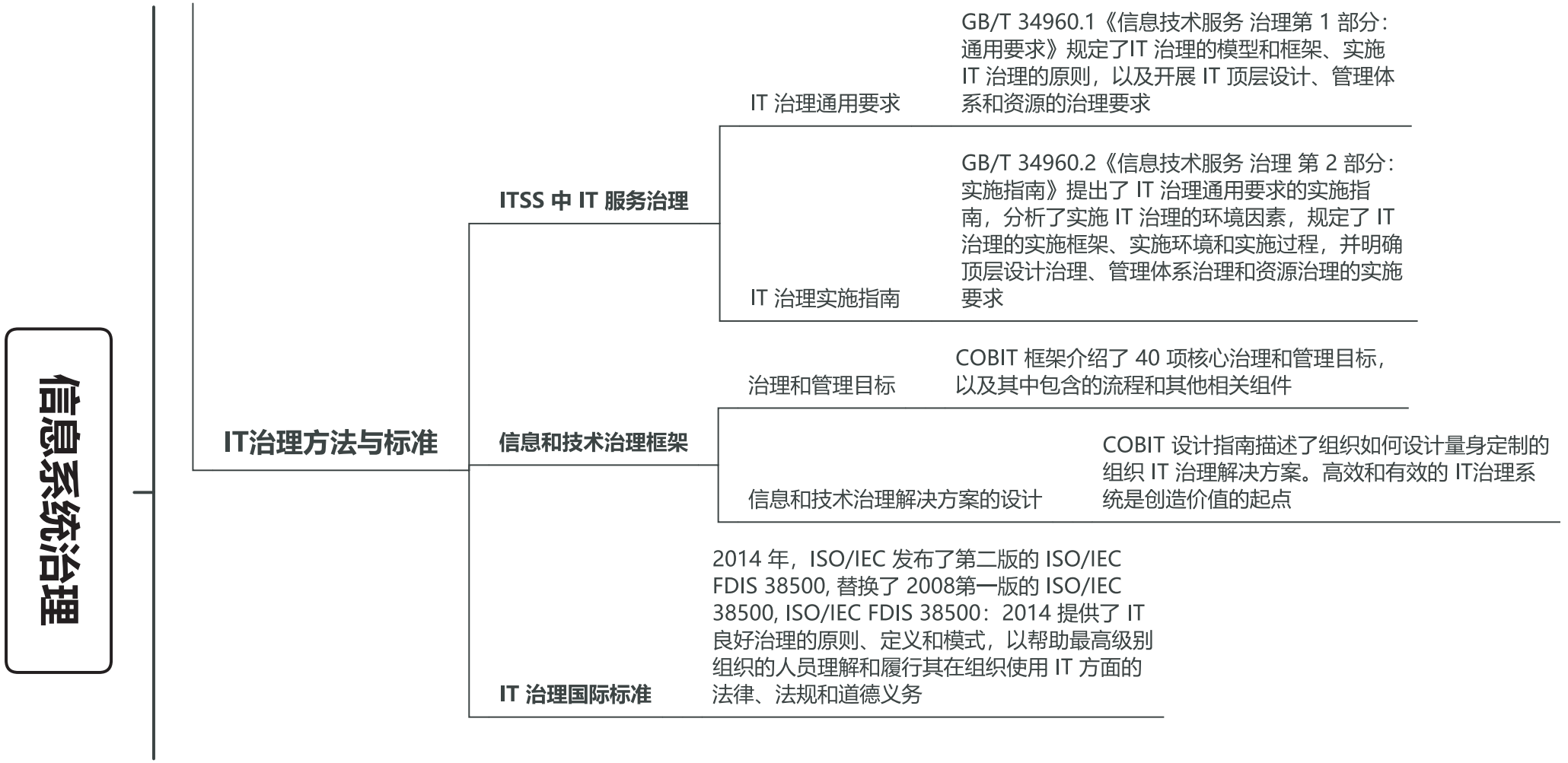
组织职责	组织参与 IT 决策与管理的所有人员的集合，明确组织信息部门和业务部门之间的关系和责任，正确划分信息系统的所有者、建设者、管理者和监控者
战略匹配	IT 治理的一个重要内容，是使组织的 IT 建设与组织战略相匹配，也就是通常所说的“战略匹配”。而战略匹配是 IT 为组织贡献业务价值的重要驱动力
资源管理	资源管理的主要功能是确保用户对组织的应用系统和基础设施都有良好的理解和应用，优化IT 投资、IT 资源 (人、应用系统、信息、基础设施) 的分配，做好人员的培训、发展计划，以满足组织的业务需求
价值交付	通过对 IT 项目全生命周期的管理，确保IT 能够按照组织战略实现预期的业务价值
风险管理	是确保 IT 资产的安全和灾难的恢复、组织信息资源的安全以及人员的隐私安全
绩效管理	追踪和监视 IT 战略、IT 项目的实施、信息资源的使用、IT 服务的提供以及业务流程的绩效

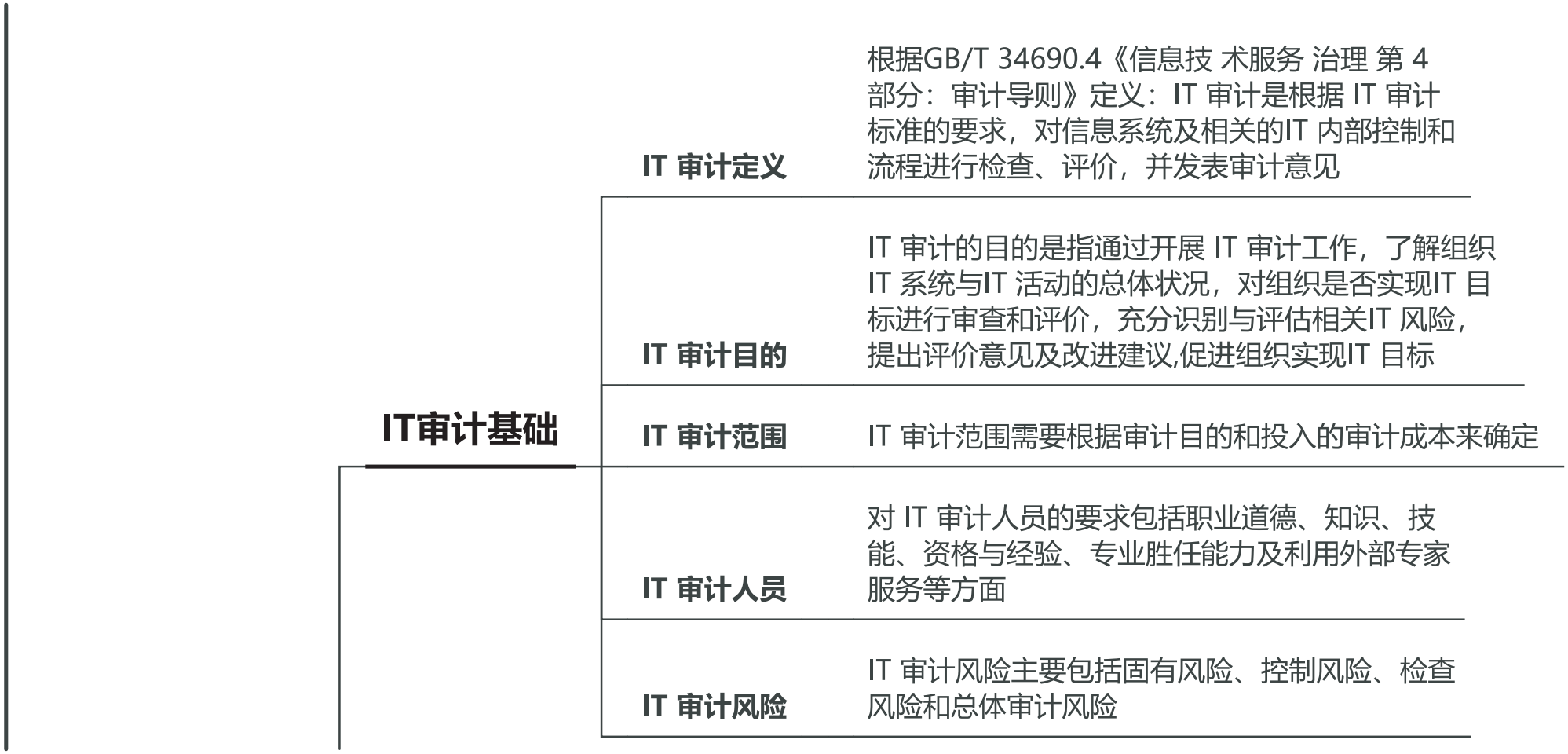
IT 治理机制经验

- IT指导委员会要吸纳有才干的业务经理，使之负责组织范围的IT治理决策，并在IT原则中加入严格的成本控制；
- 谨慎管理组织的IT架构和业务架构，以降低业务成本；
- 设计严格的架构例外处理流程，使昂贵的例外最小化，并可以从中不断学习；
- 建立集中化的IT团队，用以管理基础设施、架构和共享服务；
- 应用连接 IT投资和业务需求的流程，既可以增加透明度，又可以权衡中心和各运营部门或团队的需求；
- 设计需要对 IT投资进行集中协作和核准的 IT投资流程；
- 设计简单的费用分摊和服务水平协议机制，以明确分配IT开支等

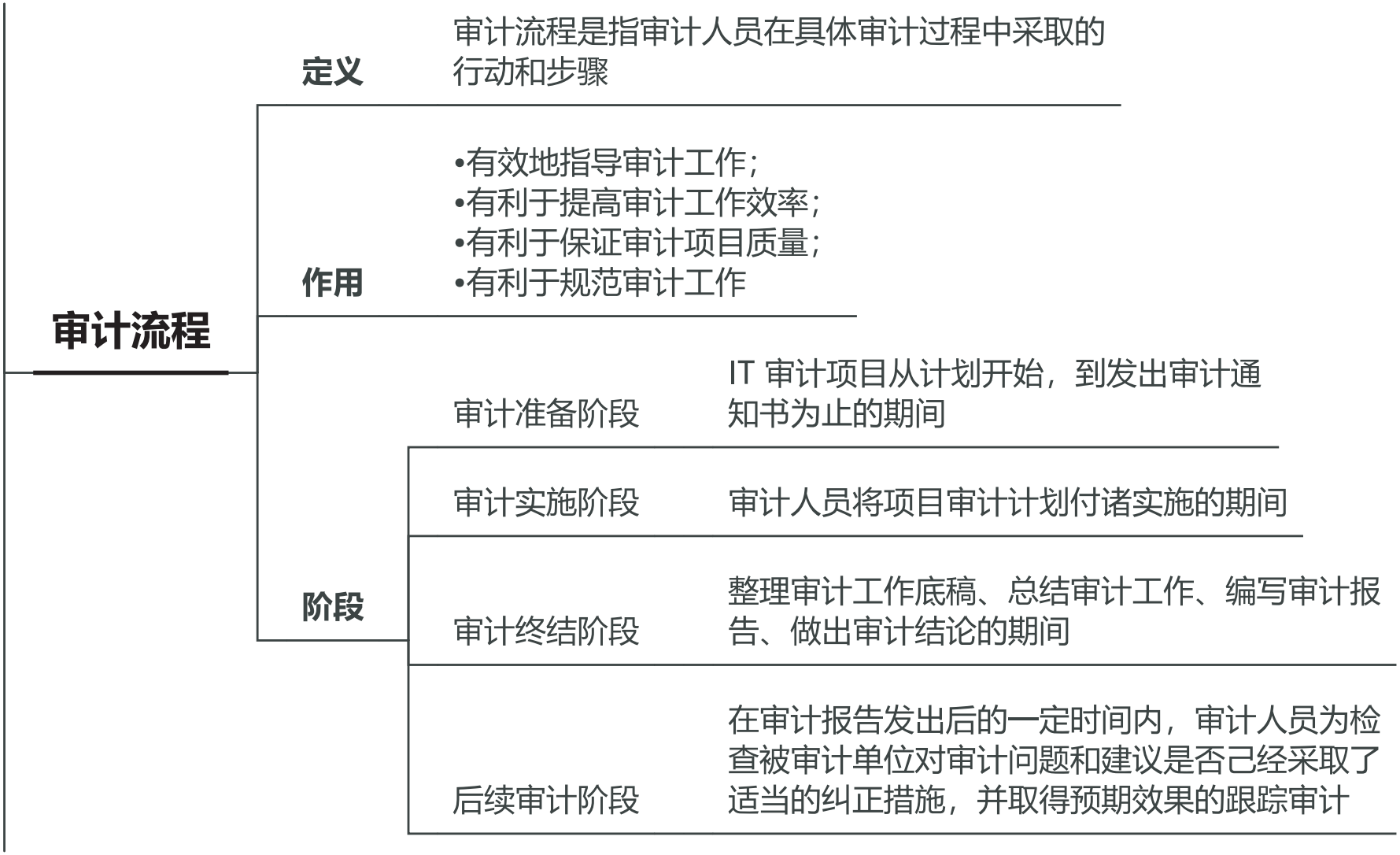
IT治理任务

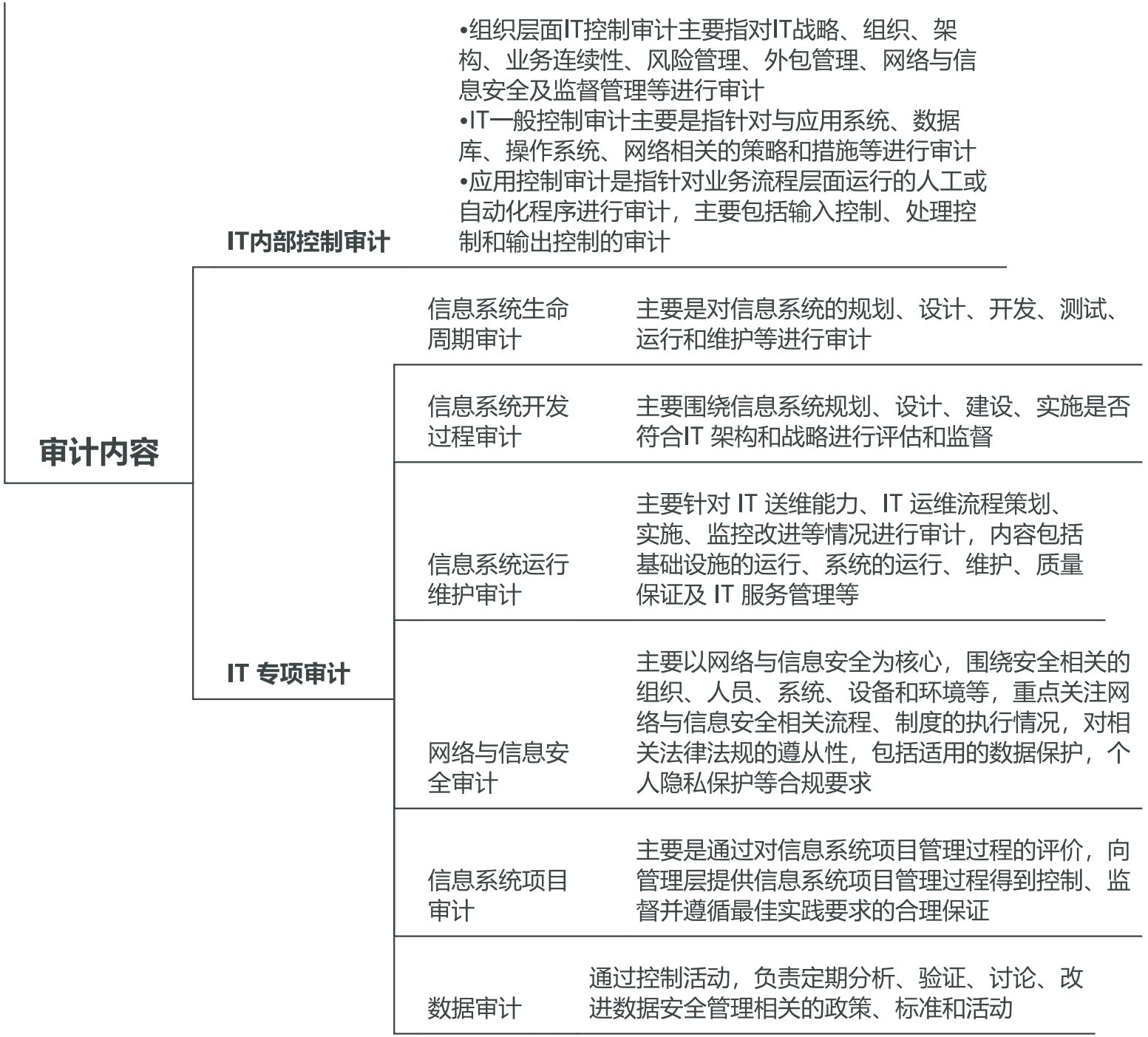
全局统筹	统筹规划 IT 治理的目标范围、技术环境、发展趋势和人员责权利
价值导向	价值导向包括基于实现有效收益，确保预期收益清晰理解，明确实现收益的问责机制
机制保障	机制保障是指组织应对自身 IT 发展进行有效管控，保证 IT 需求与实现的协调发展，并使 IT 安全和风险得到有效的识别、管理、防范和处置
创新发展	创新发展是指利用IT 创新开拓业务领域，提升管理水平，改进质量、绩效和降低成本，确保实现战略目标的灵活性和对环境变化的适应性
文化助推	文化助推是指组织与利益相关者沟通 IT 治理的目标、策略和职责，营造积极向上、沟通包容的组织文化


信息系统治理
IT治理方法与标准
ITSS 中 IT 服务治理
IT 治理通用要求
GB/T 34960.1《信息技术服务 治理第 1 部分：通用要求》规定了IT 治理的模型和框架、实施 IT 治理的原则，以及开展 IT 顶层设计、管理体系和资源的治理要求
IT 治理实施指南
GB/T 34960.2《信息技术服务 治理 第 2 部分：实施指南》提出了 IT 治理通用要求的实施指南，分析了实施 IT 治理的环境因素，规定了 IT 治理的实施框架、实施环境和实施过程，并明确顶层设计治理、管理体系治理和资源治理的实施要求
信息和技术治理框架
治理和管理目标
COBIT 框架介绍了 40 项核心治理和管理目标，以及其中包含的流程和其他相关组件
信息和技术治理解决方案的设计
COBIT 设计指南描述了组织如何设计量身定制的组织 IT 治理解决方案。高效和有效的 IT治理系统是创造价值的起点
IT 治理国际标准
2014 年，ISO/IEC 发布了第二版的 ISO/IEC FDIS 38500, 替换了 2008第一版的 ISO/IEC 38500, ISO/IEC FDIS 38500：2014 提供了 IT 良好治理的原则、定义和模式，以帮助最高级别组织的人员理解和履行其在组织使用 IT 方面的法律、法规和道德义务


IT审计基础
IT 审计定义
根据GB/T 34690.4《信息技 术服务 治理 第 4 部分：审计导则》定义：IT 审计是根据 IT 审计标准的要求，对信息系统及相关的IT 内部控制和流程进行检查、评价，并发表审计意见
IT 审计目的
IT 审计的目的是指通过开展 IT 审计工作，了解组织 IT 系统与IT 活动的总体状况，对组织是否实现IT 目标进行审查和评价，充分识别与评估相关IT 风险，提出评价意见及改进建议,促进组织实现IT 目标
IT 审计范围
IT 审计范围需要根据审计目的和投入的审计成本来确定
IT 审计人员
对 IT 审计人员的要求包括职业道德、知识、技能、资格与经验、专业胜任能力及利用外部专家服务等方面
IT 审计风险
IT 审计风险主要包括固有风险、控制风险、检查风险和总体审计风险

- 2.IT审计
  - 审计方法与技术
    - IT 审计依据与准则
      - •信息系统审计准则（ISACA, 国际信息系统审计协会发布）。
      - •《内部控制一整体框架》报告，即通称的COSO（美国虚假财务报告委员会下属的发起人委员会）报告。
      - •《萨班斯法案》（SOX）。SOX是美国政府出台的一部涉及会计职业监管、组织治理、证券市场监管等方面改革的重要法律。
      - •信息及相关技术控制目标（COBIT）是目前国际上通用的信息及相关技术控制规范
    - IT 审计常用方法
      - 常用审计方法包括：访谈法、调查法、检查法、观察法、测试法和程序代码检查法等
    - IT 审计技术
      - 常用的rr 审计技术包括风险评估技术、审计抽样技术、计算机辅助审计技术及大数据审计技术。
    - IT 审计证据
      - 定义：审计证据是指由审计机构和审计人员获取，用于确定所审计实体或数据是否遵循既定标准或目标，形成审计结论的证明材料
      - 特性：充分性、客观性、相关性、可靠性、合法性
    - IT 审计底稿
      - 定义：审计工作底稿是指审计人员对制订的审计计划、实施的审计程序、获取的相关审计证据，以及得出的审计结论做出的记录
      - 作用：
        - •是形成审计结论、发表审计意见的直接依据；
        - •是评价考核审计人员的主要依据；
        - •是审计质量控制与监督的基础；
        - •对未来审计业务具有参考备查作用。
      - 分类：综合类工作底稿、业务类工作底稿和备查类工作底稿


审计流程
定义
审计流程是指审计人员在具体审计过程中采取的行动和步骤
作用
•有效地指导审计工作；
•有利于提高审计工作效率；
•有利于保证审计项目质量；
•有利于规范审计工作
阶段
审计准备阶段
IT 审计项目从计划开始，到发出审计通知书为止的期间
审计实施阶段
审计人员将项目审计计划付诸实施的期间
审计终结阶段
整理审计工作底稿、总结审计工作、编写审计报告、做出审计结论的期间
后续审计阶段
在审计报告发出后的一定时间内，审计人员为检查被审计单位对审计问题和建议是否已经采取了适当的纠正措施，并取得预期效果的跟踪审计


审计内容
IT内部控制审计
•组织层面IT控制审计主要指对IT战略、组织、架构、业务连续性、风险管理、外包管理、网络与信息安全及监督管理等进行审计
•IT一般控制审计主要是指针对与应用系统、数据库、操作系统、网络相关的策略和措施等进行审计
•应用控制审计是指针对业务流程层面运行的人工或自动化程序进行审计，主要包括输入控制、处理控制和输出控制的审计
IT 专项审计
信息系统生命周期审计
主要是对信息系统的规划、设计、开发、测试、运行和维护等进行审计
信息系统开发过程审计
主要围绕信息系统规划、设计、建设、实施是否符合IT 架构和战略进行评估和监督
信息系统运行维护审计
主要针对 IT 送维能力、IT 运维流程策划、实施、监控改进等情况进行审计，内容包括基础设施的运行、系统的运行、维护、质量保证及 IT 服务管理等
网络与信息安全审计
主要以网络与信息安全为核心，围绕安全相关的组织、人员、系统、设备和环境等，重点关注网络与信息安全相关流程、制度的执行情况，对相关法律法规的遵从性，包括适用的数据保护，个人隐私保护等合规要求
信息系统项目审计
主要是通过对信息系统项目管理过程的评价，向管理层提供信息系统项目管理过程得到控制、监督并遵循最佳实践要求的合理保证
数据审计
通过控制活动，负责定期分析、验证、讨论、改进数据安全管理相关的政策、标准和活动