第8章 信息服务与事件管理

信息安全管理

主讲 李章兵

内容

- 8.1 信息资产管理
- 8.2 信息服务管理
- 8.3 安全事件管理
- 8.4 信息系统审计

8.1 信息资产管理

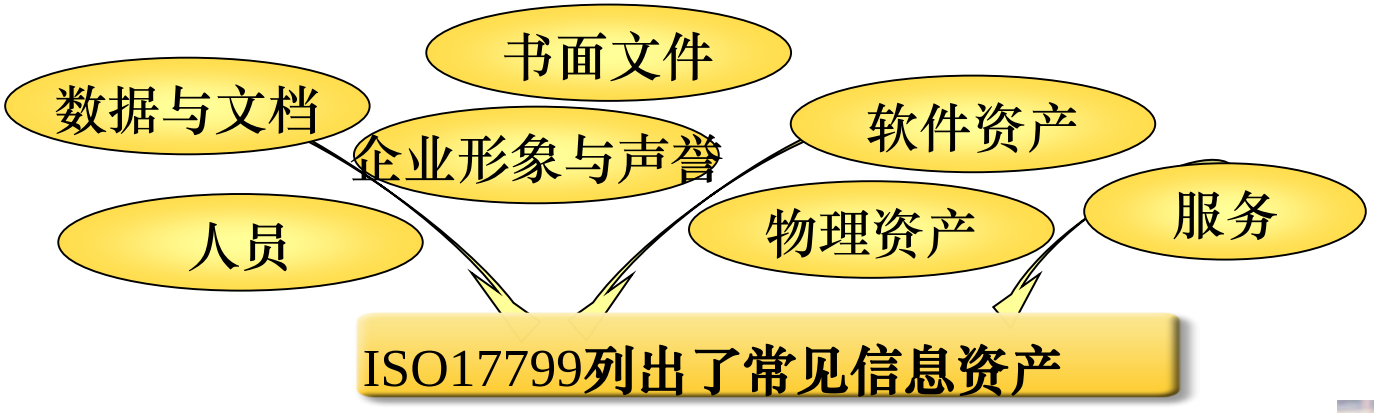
- 1. 信息资产概述
  - 信息
    - 可以理解为消息、情报、数据或知识，它可以以多种形式存在。
    - 信息是一种资产，像其他重要的业务资产一样，对组织具有价值，因此需要妥善保护。---ISO17799
- 信息资产
  - 指对组织具有价值的信息资源，是安全策略保护的对象。(风险评估)
  - 信息资产分类
    - 数据、软件、硬件、文档、服务、人员等。

8.1 信息资产管理

- **1. 信息资产概述**
  - 信息资产分类
    - 数据与文档：数据库和数据文件、系统文件、用户手册、培训材料、运行与支持程序、业务连续性计划、应急安排
    - 书面文件：合同、指南、企业文件、包含重要业务结果的文件
    - 软件资产：应用软件、系统软件、开发工具和实用程序
    - 物理资产：计算机、通用设备、磁介质（磁盘与磁带）、其他技术设备（供电设备、空调设备）、家具、办公场所
    - 人员：各种角色的定义（系统管理员、网络管理员等）
    - 企业形象与声誉
    - 服务：计算和通讯服务，其他技术服务（供热、照明、电力、空调）

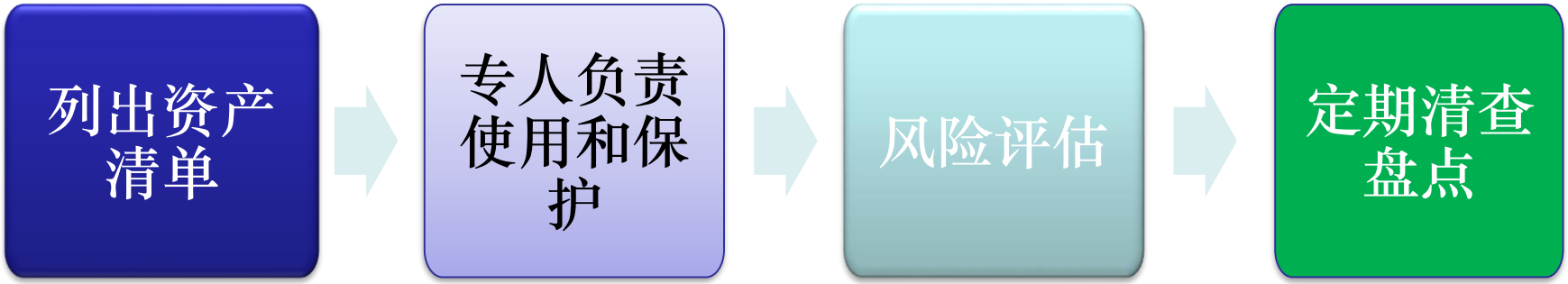
8.1 信息资产管理

- **1. 信息资产概述**
  - 信息资产表现形式
    - 可以是组织中信息设施中存储与处理的数据、程序；
    - 可以是打印出来的或写出来的论文、电子邮件、设计图纸、业务方案；
    - 可以显示在胶片上或表达在会话中的消息。



8.1 信息资产管理

- **2.信息资产保护**
  - 编制资产清单，制定相应控制措施
  - 对于每项资产，组织指定责任人，并赋予职责



8.1 信息资产管理

- **2.信息资产保护**
  - **编制资产清单**
    - 将每项资产的名称、所处位置、价值、资产负责人等相关信息记录在资产清单上。
  - **指定使用和保护的责任人**
    - 责任制：对每一项信息资产，组织的管理者应指定专人负责其使用和保护，防止资产被盗、丢失与滥用。
  - **控制措施**
    - 根据资产的相对价值大小来确定关键信息资产，并对其进行风险评估以确定适当的控制措施。
  - **盘点清查**
    - 定期对信息资产进行清查盘点，确保资产账物相符和完好不损。

8.1 信息资产管理

- **3.信息资产责任**
  - 所有信息和相关设施资产应由组织的指定部门或人员承担责任。
  - 资产责任人应负责
    - 确保与信息处理设施相关的信息和资产进行了适当的分类和标记；
    - 确定并周期性评审访问限制和分类，要考虑到可应用的访问控制策略。
  - 信息资产分类原则
    - 信息应按照它对组织的价值、法律要求、敏感性和关键性予以合理分类。

8.1 信息资产管理

- **3.信息资产责任**
  - 信息的分类保护控制措施
    - 应考虑到共享或限制信息的业务需求；
    - 应考虑到相关的业务影响。
  - 信息分类注意
    - 分类等级要合理
      - 分类等级应考虑分类类别的数目和从其使用中获得的好处。
      - 过度复杂的方案可能对使用不方便、不经济、不实际。
      - 分类标记解释：小心从其他组织获取的信息文件有不同的定义。
    - 信息保存期限
      - 信息的保存有时间期限，其分类可能按照一些预定的策略发生改变。
      - 随时间流逝信息失去一定的敏感性和重要性，原有分类失去了意义。
      - 把分类的安全保护划定得过高会导致不必要的业务开支。
    - 责任人
      - 信息的始发人或指定的所有权人应当承担确定信息类别的责任，以及定期检查这些分类的责任。

8.1 信息资产管理

- **3.信息资产责任**
  - 信息的分类标记
    - 信息的分类标记和安全处理是信息共享的一个关键要求。
    - 应按照组织所采纳的分类机制建立和实施一组合适的信息标记和处理程序。
    - 信息标记与处理实施指南：
      - 信息标记的程序需要涵盖物理和电子格式的信息资产。
      - 对每种分类级别，要定义包括安全处理、储存、传输、删除、销毁的处理程序。
      - 涉及信息共享的与其他组织的协议应包括识别信息分类和解释其他组织分类标记的程序。

8.1 信息资产管理

- **3.信息资产责任**
  - 信息的分类标记
    - 信息标记与处理实施指南：
      - 按照所显示的分类级别，处置和标记所有介质；
      - 确定防止未授权人员访问的限制；
      - 维护数据的授权接收者的正式记录；
      - 确保输入数据完整，正确完成了处理并应用了输出验证；
      - 按照与其敏感性一致的级别，保护等待输出的假脱机数据；
      - 根据制造商的规范存储介质；
      - 使分发的数据最少；
      - 清晰地标记数据的所有拷贝，以引起已授权接收者的关注；
      - 以固定的时间间隔评审分发列表和已授权接收者列表。

8.1 信息资产管理

- **3.信息资产责任**
  - 信息的分类标记
    - 信息标记与处理实施的对象

信息处理程序的实施对象

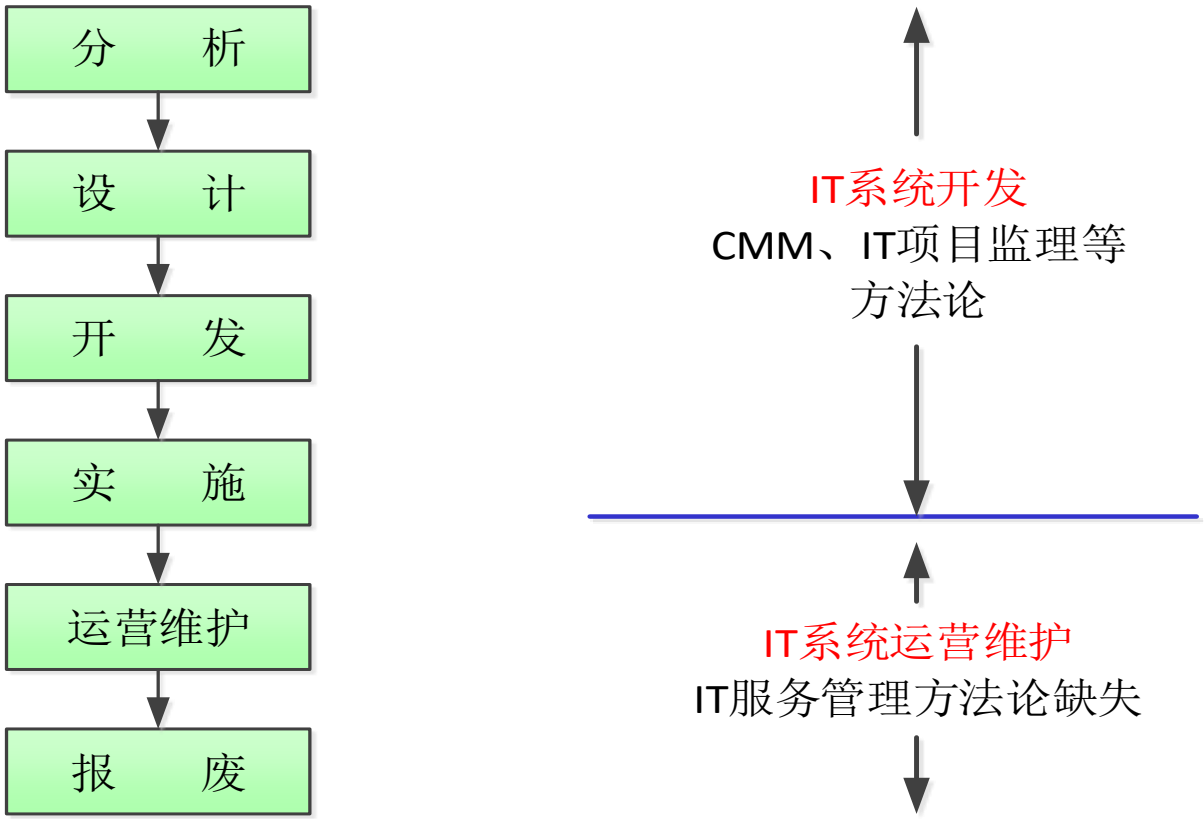
文件	移动计算	邮件	邮政服务/设施
计算系统	移动通信	话音邮件	传真机的使用
网络	通用话音通信		空白支票
多媒体			发票

8.1 信息资产管理

- **4.软件资产许可**
  - 应使用合法软件，严厉打击使用盗版软件行为。
  - 公司应有检测和处理非授权软件措施，例如：
    - 定期检查环境中所安装的软件。
    - 实施技术措施，防止非授权人员安装非授权软件。
    - 对有未授权行为的人员进行教育，提升他们的信息安全意识。

8.2 信息服务管理

- **1. 信息服务管理概述**
  - **IT应用生命周期图**



8.2 信息服务管理

- 1. 信息服务管理概述
  - IT运营管理
    - 帮助企业对IT系统的规划、研发、实施和运营进行有效管理。运营管理是IT生命周期的关键阶段。
      - IT运营阶段非常重要，如果没有任何指南作为管理参考，就有可能造成IT投资的浪费、IT 服务的不可靠、反应速度慢和质量低下。
    - IT应用生命周期中运营阶段的重要特点：
      - 通常时间跨度最长；
      - 业务对IT技术有较强的依赖性，并将受到劣质IT服务质量的负面影响。
        - » 自上个世纪60年代开始，IT如何高效地为人类和社会带来效率便吸引着人们的眼球。“软件危机”、“人月神话”、“软件工程”等词语便成了企业界和IT人关注的焦点。
        - » 在众多专家、学者、企业人士的不断探索中，IT人创造了“OOA&OOD”、“CMM”、“IT项目监理”等我们耳熟能详的方法论。
        - » 在众多的方法论中，一个普遍的缺失是没有一个IT 运营管理阶段（有时又称

8.2 信息服务管理

- 1. 信息服务管理概述
  - IT运营管理
    - IT应用时间分布图

    - 一个服务从开发到上线实施可能只需要一年的时间，却有3到6年甚至更长的时间来运行维护。
    - IT项目生命周期的大约80%时间与IT项目运营维护有关。
    - 运营维护阶段的投资仅占整个IT投资的20%,形成了典型的“技术高消费”、“轻服务、重技术”现象。

8.2 信息服务管理

- **2. ITIL内容体系**
  - **ITIL--IT基础设施库**
    - 上世纪80年代中期，英国政府意识到了IT服务管理问题的严重程度，为填补IT运营指南方面的空白，英国政府中央计算机和电信局CCTA（Central Computer & Telecommunications Agency）深入研究和总结各个组织的实际经验（最佳实践best practice），找出IT运营管理中什么起作用而什么不起作用。
    - CCTA经过几年的深入研究，发布了IT服务管理的最佳实践——ITIL（IT Infrastructure Library，IT基础设施库），可由世界上任何组织免费使用以及利用ITIL开展有关业务。
    - 主要精神为和谐推动及持续改善IT服务，将服务对象视为客户，强调End-to-End的服务。

8.2 信息服务管理

- 2. ITIL内容体系
  - ITIL--IT基础设施库

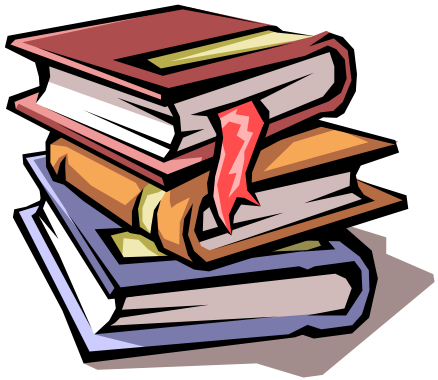
背景	目的	主要精神
• 英国政府意识到了IT服务管理问题的严重程度	• 为填补IT运营指南方面的空白 • 由世界上任何组织免费使用以及利用ITIL开展有关业务	• 为和谐推动及持续改善IT服务 • 将服务对象视为客户，强调End-to-End的服务。

8.2 信息服务管理

- 2. ITIL内容体系
  - ITIL的基本特点
    - （1）开源：公共框架、开源标准
      - » ITIL由世界范围内的有关专家共同开发，任何组织可免费使用以及利用ITIL开展有关业务。
    - （2）最佳实践框架：根据实践而不是基于理论开发的
      - » OGC收集和分析各种组织解决服务管理问题方面的信息，找出那些对本部门和在英国政府部门中的客户有益的做法，最后形成了ITIL。
    - （3）国际标准：事实上的国际标准
      - » 20世纪90年代初期很快在欧洲和其它国家流行起来，目前ITIL已经成为世界IT服务管理领域事实上的标准。
    - （4）以流程为导向，以客户满意和服务品质为核心。
      - » ITIL本质上说来是对IT部门为业务部门提供服务的流程再造。组织在运用ITIL进行内部的IT服务管理时，不仅可以提供用户满意的服务、改善客户的体验，还可以确保这个过程符合成本效益原则。

8.2 信息服务管理

- 2. ITIL内容体系
  - ITIL的核心模块：“服务管理”
    - ITIL将IT服务管理分为十个核心流程和一项管理职能。这些流程和职能又被归结为两大流程组，即“服务提供”流程组和“服务支持”流程组。



8.2 信息服务管理

- 2. ITIL内容体系
  - 服务管理--“服务提供”流程组
    - 服务级别管理：
      - 为签订服务级别协议（SLAs）而进行的计划、草拟、协商、监控和报告以及签订服务级别协议后对服务绩效的评价等一系列活动所组成的一个服务管理流程。
      - 旨在确保组织所需的IT服务质量在成本合理的范围内得以维持并逐渐提高。
    - IT服务财务管理：
      - 负责预算和核算IT服务提供方提供IT服务所需的成本，并向客户收取相应服务费用的管理流程，它包括IT投资预算、IT服务成本核算和服务计费三个子流程
      - 目标是通过量化服务成本减少成本超支的风险、减少不必要的浪费、合理引导客户的行为，从而最终保证所提供的IT服务符合成本效益的原则。
      - 流程产生的预算和核算信息可以为服务级别管理、能力管理、IT服务持续性管理和变更管理等管理流程提供决策依据。

8.2 信息服务管理

- 2. ITIL内容体系
  - 服务管理--“服务提供”流程组
    - IT服务持续性管理：
      - 指确保发生灾难后有足够的技术、财务和管理资源确保IT服务持续性的管理流程。
      - 关注的焦点是在发生服务故障后仍然能够提供预定级别的IT服务，从而支持组织的业务持续运作的能力。
    - 能力管理：
      - 指在成本和业务需求的双重约束下，通过配置合理的服务能力使组织的IT资源发挥最大效能的服务管理流程。
      - 流程包括业务能力管理、服务能力管理和资源能力管理三个子流程。
    - 可用性管理：
      - 通过分析用户和业务方的可用性需求并据以优化和设计IT基础架构的可用性，确保以合理的成本满足不断增长的可用性需求的管理流程。
      - 一个前瞻性的管理流程：通过对业务和用户可用性需求的定位，使得IT服务的设计建立在真实需求的基础上，避免IT服务运作中采用了过度的可用性级别，节约了IT服务的运作成本。

8.2 信息服务管理

- 2. ITIL内容体系
  - 服务管理--“服务支持”流程组
    - 配置管理：
      - 识别和确认系统的配置项，记录和报告配置项状态和变更请求，检验配置项的正确性和完整性等活动构成的过程
      - 目的是提供IT基础架构的逻辑模型，支持其它服务管理流程特别是变更管理和发布管理的运作。
    - 变更管理：
      - 指为在最短的中断时间内完成基础架构或服务的任一方面的变更而对其进行控制的服务管理流程。
      - 目标是确保在变更实施过程中使用标准的方法和步骤，尽快地实施变更，以将由变更所导致的业务中断对业务的影响减小到最低。
    - 发布管理：
      - 指对经过测试后导入实际应用的新增或修改后的配置项进行分发和宣传的管理流程。
      - 又称为软件控制与分发，它由变更管理流程控制。

8.2 信息服务管理

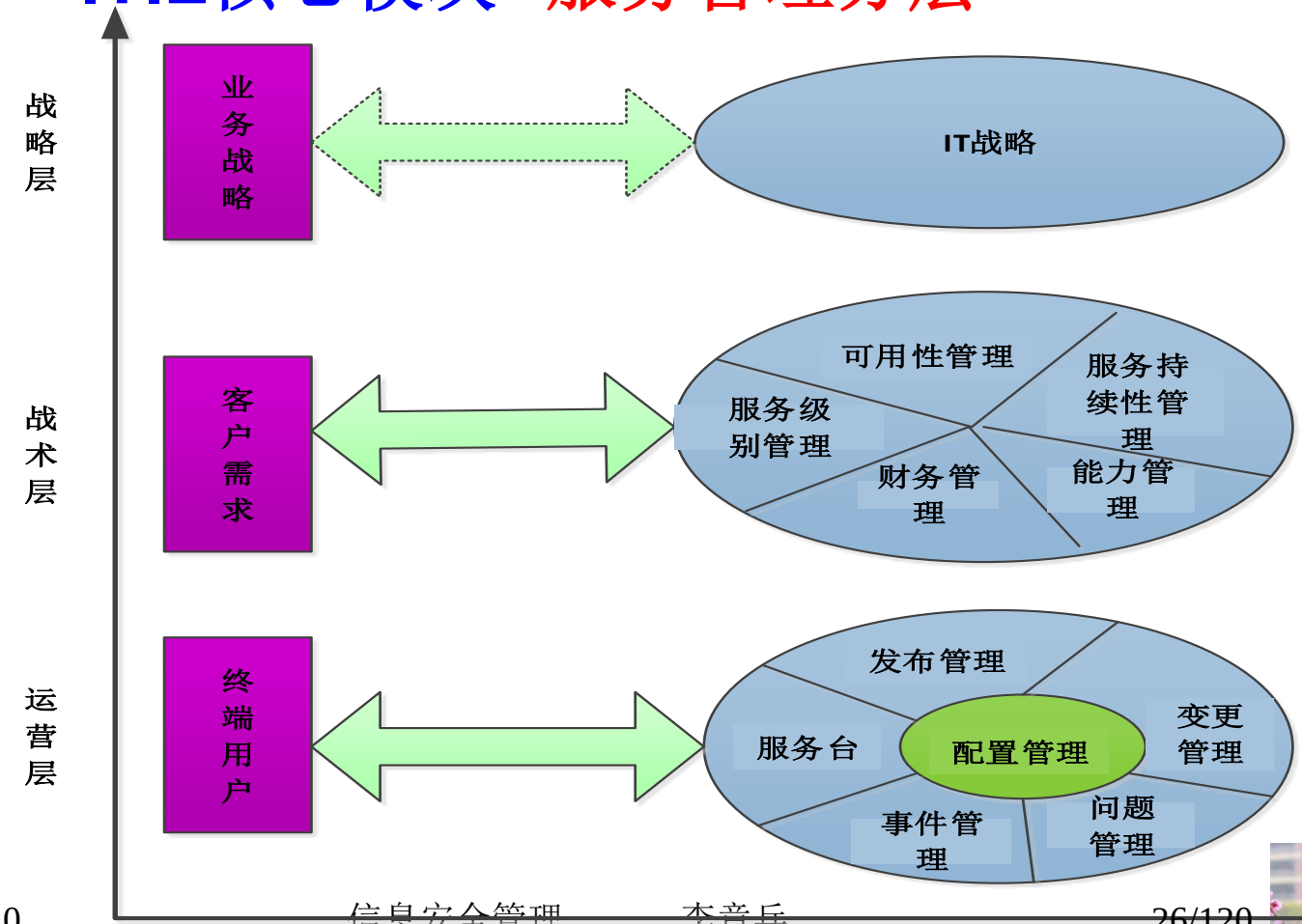
- 2. ITIL内容体系
  - 服务管理--“服务支持”流程组
    - 事件管理：
      - 负责记录、归类和安排专家处理事件并监督整个处理过程直至事件得到解决和终止。
      - 目的是在尽可能最小地影响客户和用户业务的情况下使IT系统恢复到服务级别协议所定义的服务级别。
    - 问题管理：
      - 指通过调查和分析IT基础架构的薄弱环节、查明事故产生的潜在原因，并制定解决事故的方案和防止事故再次发生的措施，将由于问题和事故对业务产生的负面影响减小到最低的服务管理流程。
      - 与事故管理强调事故恢复的速度不同，问题管理强调的是找出事故产生的根源，从而制定恰当的解决方案或防止其再次发生的预防措施。

8.2 信息服务管理

- 2. ITIL内容体系
  - ITIL核心模块--服务管理分层
    - 我们把企业的IT战略属于“战略层”，服务提供称之为“战术层”，把服务支持称之为“运作层”。
    - 战术层：业务部门的客户需求通过服务级别管理与IT部门达成共识；
    - 运营层：业务部门的终端用户通过服务台这一接口统一与IT部门取得联系。

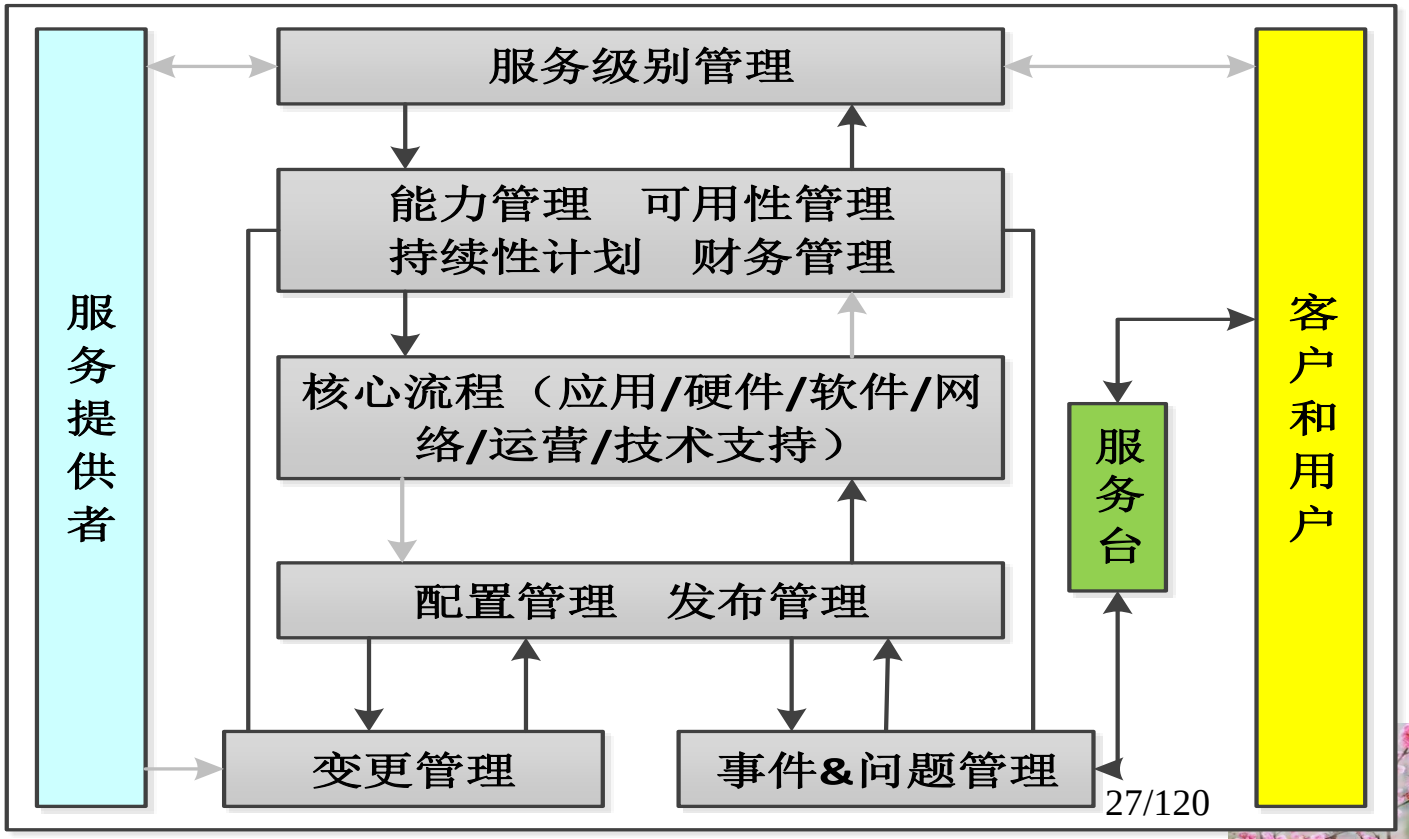
8.2 信息服务管理

- 2. ITIL内容体系
  - ITIL核心模块--服务管理分层



8.2 信息服务管理

- 2. ITIL内容体系
  - 服务管理：服务者和客户关系
    - 用户指直接使用IT服务的人或机构，通常是指业务部门内某个具体的职员；
    - 客户指为IT服务付费的人或机构，通常是指某个具体的业务部门

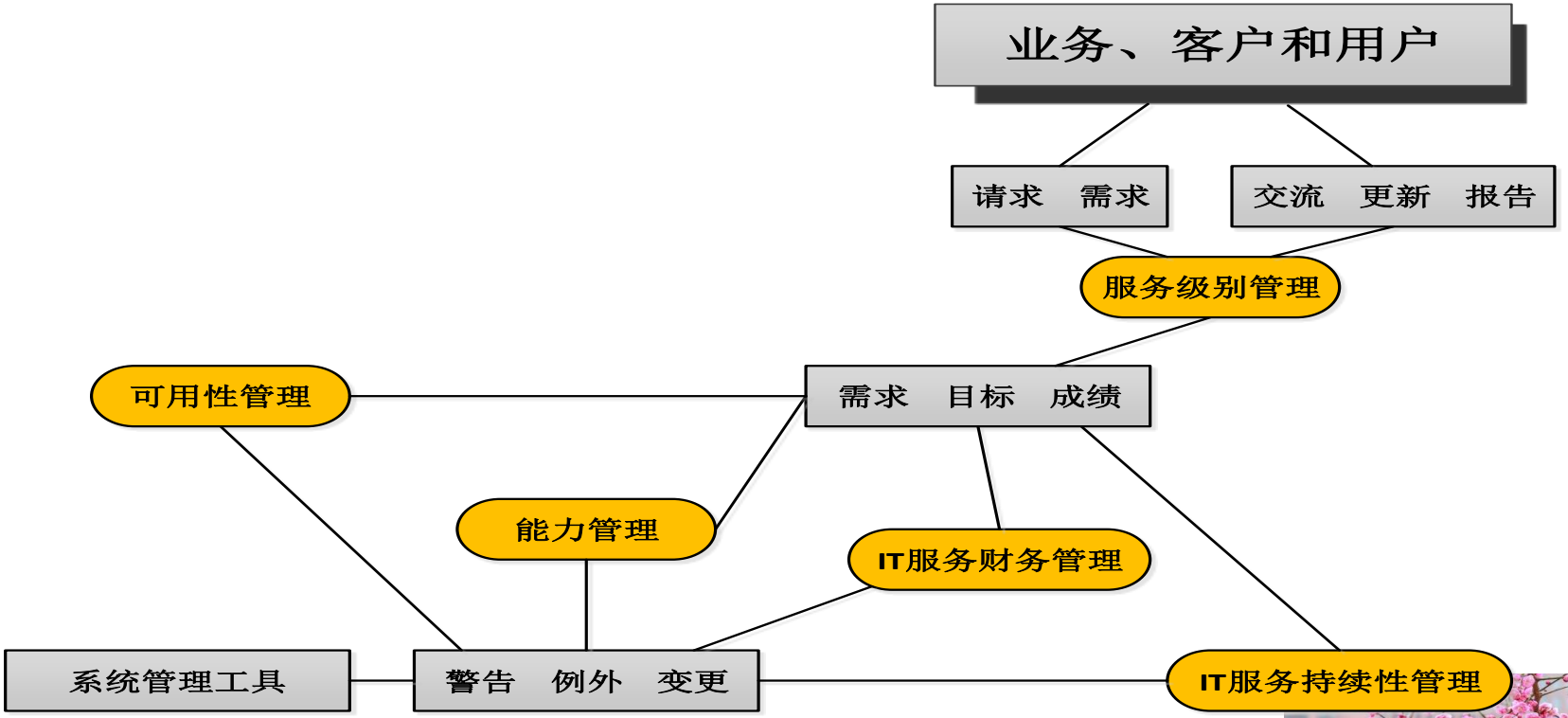


8.2 信息服务管理

- 3.服务提供流程
  - 任务
    - 根据组织的业务需求，对服务能力、持续性、可用性等服务级别目标进行规划和设计。
    - 考虑实现这些服务目标所需要耗费的成本。
  - 服务提供流程设计
    - 主要面向为服务付费的机构和个人客户。
    - 必须在服务级别目标和服务成本之间进行合理的权衡。
      - 必须解决“客户需要什么”、“为满足客户需求需要哪些资源”、“这些资源的成本是多少”、“如何在服务成本和服务效益（达到的服务级别）之间选择恰当的平衡点”等问题。

8.2 信息服务管理

- 3.服务提供流程
  - 服务提供的5个核心流程关系
    - 包括服务级别管理、可用性管理、能力管理、IT服务财务管理、IT服务持续性管理。



8.2 信息服务管理

- 3.服务提供流程
  - 服务级别管理(SLM)——"量体裁衣"的流程
    - 目标
      - 根据客户的业务需求和相关的成本预算，制定恰当的服务级别目标，并将其以服务级别协议的形式确定下来。
    - 真正了解客户的业务需求，服务级别经理须做到：
      - 和业务方（用户和客户）进行全面沟通。
      - 调查用户和客户对当前服务级别的体验，帮助客户分析和梳理那些真实存在却又尚未明确的业务需求。
      - 结合相关的IT成本进一步确定组织对IT服务的有效需求，抑制客户在设备和技术方面"高消费"的欲望，为组织节约成本，提高IT投资的效益。

8.2 信息服务管理

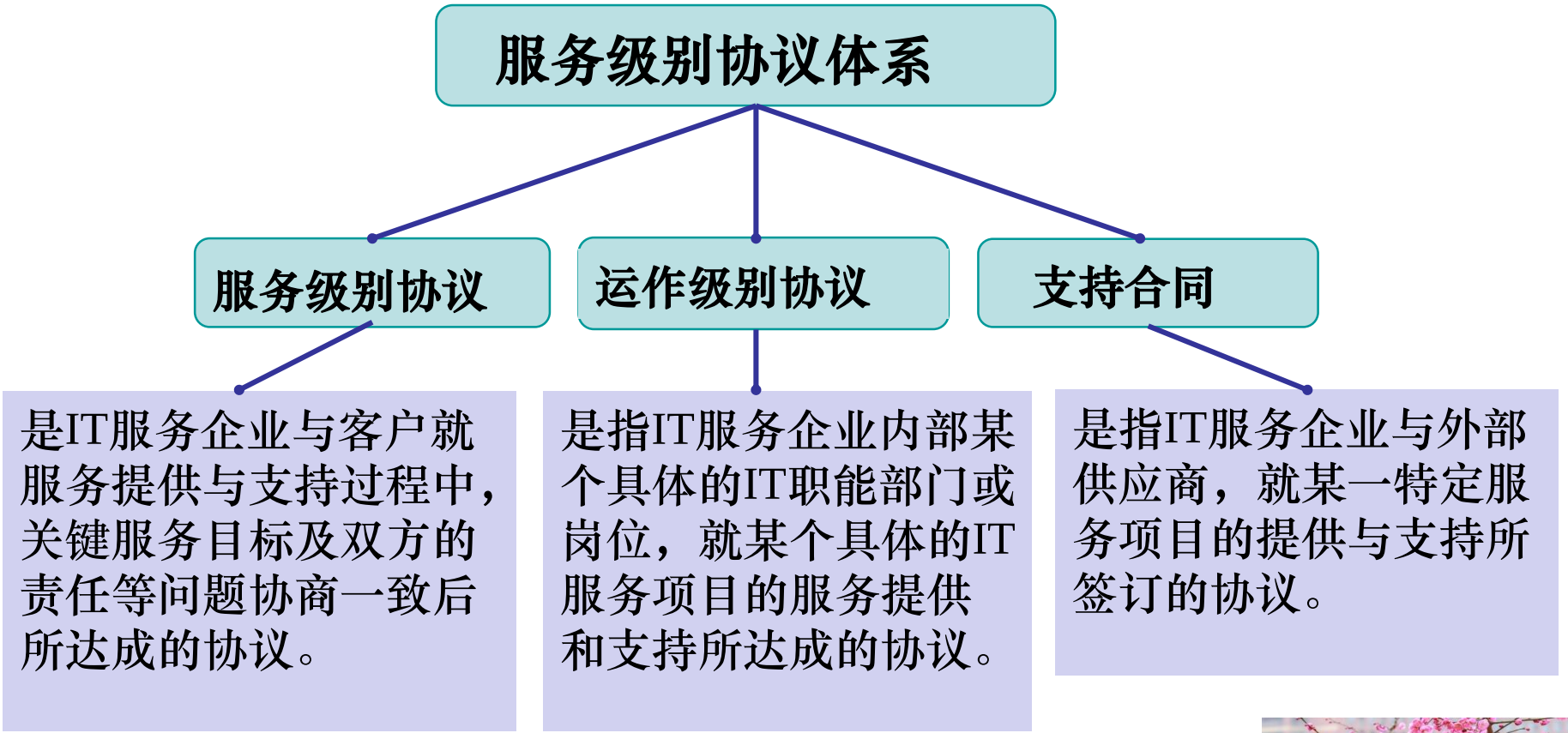
- 3.服务提供流程
  - 服务级别管理--SLM
    - 是IT服务部门面向业务部门（客户）的一个窗口。
    - 解决IT服务部门和用户双方问题最有效的方式。
    - 制定服务级别协议——有效地管理IT服务部门和用户双方的期望。
      - 以一种可以量度的方式来界定他们提供的服务；
      - 服务等级协议是IT外包商的保护性策略。
      - 平衡用户不断攀升的高质量服务期望、满足其需求、抑制其抱怨。
        - » 客户抱怨：“那些家伙拿着我们的钱到底干了些什么？”

8.2 信息服务管理

- 3.服务提供流程
  - 服务级别协议--SLA
    - 是IT服务企业与客户就服务提供与支持过程中，关键服务目标及双方的责任等问题协商一致后所达成的协议。
    - 协议语言：宜采用客户和IT企业都理解、非技术化的语言。便于客户和IT企业之间的沟通，减少双方之间的摩擦；有利于后期的评审与修改。
    - 运作级别协议：指IT服务企业内部某个具体的IT职能部门或岗位，就某个具体的IT服务项目（如邮件系统的可用性等）的服务提供和支持所达成的协议。
    - 服务项目化：签订服务级别协议后，为保证达到约定的服务级别目标，需要将客户的业务需求转化成具体的服务项目，并针对这些项目签订运作级别协议。
    - 支持合同：指IT企业与外部供应商，就某一特定服务项目的提供与支持所签订的协议。如有关通信系统的可用性级别目标，往往需要租用外部供应商的通信线路和设备等。

8.2 信息服务管理

- 3.服务提供流程
  - 服务级别协议--SLA



8.2 信息服务管理

- 3.服务提供流程
  - 服务级别管理--SLM
    - 服务级别管理是个动态的过程，主要有两层含义：
      - 服务级别管理的实施过程是一个循环滚动的过程。
      - 服务级别管理贯穿于整个IT服务运作的全过程。
    - 没有准确了解组织的服务需求，就不能提供令人满意的IT服务。

8.2 信息服务管理

- 3.服务提供流程
  - 可用性管理
    - 指从可用性角度对IT基础架构和IT服务进行设计、实施、评价和管理，以确保持续地满足业务的可用性需求的服务管理流程。
    - 可从两个方面进行衡量，即IT服务的可用性以及单个IT组件的可用性。
    - 可用性一般用IT服务或组件，在某一特定时点或一段时间内，能够正常发挥其应有功能的时间比例来表示。

8.2 信息服务管理

- 3.服务提供流程
  - 可用性管理—意义
    - 企业和机构的业务运作对IT基础架构和IT服务可用性的依赖性增强。
      - 不可用的IT基础架构和IT服务将直接导致这些企业或机构的服务品质的下降或业务运作的中断。
    - 对IT基础架构和IT服务进行可用性管理，是提高保证服务品质、降低服务成本的有效途径。
  - 可用性管理—级别
    - 根据服务级别目标和客户实际的业务可用性需求和体验，用技术指标表述和衡量的服务可用级别。

8.2 信息服务管理

- 3.服务提供流程
  - 可用性管理
    - 服务级别目标和可用性级别目标的确定是一个互动循环的过程。
    - **服务级别目标 VS 可用性级别目标**

服务级别目标是从业务和客户需求的角度进行表述的，采用的是客户易于理解的非技术性语言。

可用性级别目标虽然也是从客户体验的角度进行衡量，但其表述方式更接近于技术指标的层面。

服务级别目标和可用性级别目标的确定是一个互动循环的过程

8.2 信息服务管理

- 3.服务提供流程
  - 可用性管理
    - 目标的实现体现在事前支持、事中支持和事后支持三个方面。
    - 事前支持
      - 可用性管理流程是一个需要持续运作的管理流程，可用性需求分析需要反复进行。
      - 在服务级别需求SLR和服务级别协议SLA被确定和接受之前，需要对业务可用性需求进行分析，以确定IT基础架构是否可以和怎样实现必要的可用性级别。
      - 可用性需求分析时，需要确定服务失效对业务的影响程度，以及为提高可用性级别所需要付出的额外成本。
      - IT基础架构的运作过程可能会出现故障。可用性管理需要定期进行预防性维护管理。维护计划应将停机时间减少到最低，维护活动必须和业务部门进行充分的协调和沟通，尽量减少对业务运作造成的影响。

8.2 信息服务管理

- 3.服务提供流程
  - 可用性管理
    - 事中支持
      - 为尽量减少IT基础架构运作过程的故障，可用性管理需要定期进行预防性维护管理。
      - 对IT基础架构和IT服务的可用性进行监控，可能发现现有的可用性级别不能满足业务运作的需求，或者存在某种迹象表明IT服务可用性有降低的趋势。
    - 事后支持
      - 可用性管理自身是一个反复循环的过程，与服务级别管理也存在一定的互动关系。
      - 可用性管理流程运作的反馈信息可用于积极调整服务级别目标和可用性目标，一定程度上确保制定的可用性级别目标和服务级别目标是可实现的和可操作的。

8.2 信息服务管理

- 3.服务提供流程
  - 能力管理
    - 目标
      - 分析当前的业务需求和预测将来的业务需求，并确保这些需求在制定能力计划时得到充分的考虑。
      - 确保当前的IT资源能够发挥最大的效能、提供最佳的服务品质。
      - 确保组织的IT投资按计划进行，避免不必要的资源浪费。
    - 实施流程的主要围绕问题
      - 维持现有IT服务能力的成本相对于组织的业务需求而言是合理的吗？
      - 现有的IT服务能力能满足当前及将来的客户需求吗？
      - 现有的IT服务能力发挥了其最佳效能吗？

8.2 信息服务管理

- 3.服务提供流程
  - 能力管理：包括三个子流程
    - 业务能力管理
      - 主要关注组织未来业务对IT服务的需求，进行趋势分析和IT战略规划，确保这种未来的需求在制定能力计划时得到充分考虑。
    - 服务能力管理
      - 关注现有的IT服务品质能否达到服务级别协议中所确定的服务级别目标，以支撑业务的正常进行。
    - 资源能力管理
      - 关注IT基础架构中每个组件的执行能力和使用情况，并确保IT基础架构的能力足以支持服务级别目标的实现。

8.2 信息服务管理

- 3.服务提供流程
  - 能力管理：子流程的关系
    - 当业务对IT服务的需求经过业务能力管理子流程处理并正式运作后，就由服务能力管理子流程来确保该项IT服务的品质能够满足约定的服务级别目标的要求，而资源能力管理子流程则负责对支持IT服务运作的各IT组件的能力进行监控和评价，以确保足够的资源能力支持IT服务的运作，并保证现有的IT资源得到最佳利用。

8.2 信息服务管理

- 3.服务提供流程
  - 能力管理：子流程的关系

输入

技术
服务级别
业务计划
业务策略
业务需求
业务量
运作计划
开发计划
项目计划
事件与课题
财务计划
预算

能力管理子过程

- **业务能力管理**
  未来业务需求的趋向、预计，建模、原型、规模、文档。
- **服务能力管理**
  服务性能的监控、分析、优化及报告，建立使用服务的基线，管理服务需求。
- **资源能力管理**
  组件使用的监控、分析、优化及报告，建立使用资源的基线

输出

能力计划
能力数据库
基线
门限与警告
能力与报告
服务级别建议
成本与计费建议
预计变更
服务增进
修正运作计划
审核报告

8.2 信息服务管理

- 3.服务提供流程
  - 财务管理
    - 解决IT投资预算、IT成本、效益核算和投资评价等问题，从而为高层管理提供决策支持。
    - 信息悖论
      - 信息技术对于企业发展具有战略意义；
      - 但有时精良的设备和先进的技术并没有为企业创造实实在在的效益、提升企业的竞争力。昂贵的“系统”常常让他们骑虎难下。
    - IT服务财务管理流程对IT服务项目的规划、实施和运作进行量化管理是一种有效的手段。
    - 战术性的服务管理流程

8.2 信息服务管理

- **3.服务提供流程**
  - 财务管理
    - 负责对IT服务运作过程中所涉及的所有资源进行货币化管理的流程。
    - 包括三个子流程：投资预算、会计核算、服务计费
    - 三个子流程形成了一个IT服务项目量化管理的循环
  - 财务管理--**投资预算**
    - 目的：对IT投资项目进行事前规划和控制。
    - 通过预算，可以帮助高层管理人员预测IT项目的经济可行性，也可以作为IT服务实施和运作过程中控制的依据。

8.2 信息服务管理

- 3.服务提供流程
  - 财务管理--会计核算
    - 目标：量化IT服务运作过程中所耗费的成本和收益，为IT服务管理人员提供考核依据和决策信息。
      - 包括：IT服务项目成本核算、投资评价、差异分析和处理
    - IT服务项目成本核算
      - 核算前先定义成本要素。成本要素是成本项目进一步细分的结果，如硬件可以进一步分为办公室硬件、网络硬件以及中央服务器硬件等。成本要素一般可以按部门、客户或产品等划分标准进行定义。对IT服务部门应该按照服务要素结构来定义成本要素。
    - 投资评价
      - 主要评价指标：投资回报率ROI和资本报酬率ROCE
    - 差异分析和处理
      - IT会计人员需要将每月、每年的实际数据与相应的预算、计划数据进行比较，发现差异，调查、分析差异产生的原因，并对差异进行适当的处理。
      - 需要注意的差异包括成本差异、收益差异、服务级别差异和工作量差异。

8.2 信息服务管理

- 3.服务提供流程
  - 财务管理--服务计费
    - 负责向使用IT服务的客户收取相应费用的子流程。
    - 顺利运作需要以IT会计核算子流程为基础。
    - 意义：
      - 构建一个内部市场并以价格机制作为合理配置资源的手段，使客户和用户自觉地将其真实的业务需求与服务成本结合起来，从而提高了IT投资的效率。
      - 作为成本中心或利润中心，通过向客户收取IT服务费用，可以迫使业务部门有效地控制自身的需求、降低总体服务成本，并有助于IT服务财务管理人员重点关注那些不符合成本效益原则的服务项目。

8.2 信息服务管理

- 3.服务提供流程
  - 财务管理--服务计费
    - IT部门定位：
      - 成本中心或利润中心取决于组织业务的规模和对IT的依赖程度，依靠IT部门—技术支持中心的支持。
      - 利润中心：设立为那些组织业务规模较大且对IT依赖程度较高的组织或IT部门，以真正的商业化模式进行运作。
        - » 作为利润中心来运作的IT部门相当于一个独立的营利性组织，一般拥有完整的会计核算体系。
        - » 管理者可以有足够的自主权去管理IT部门，像管理一个独立运营的经济实体一样。
      - 成本中心：设置那些业务量较小且对IT依赖程度不高的组织或IT部门，运作达到成本控制的目的。

8.2 信息服务管理

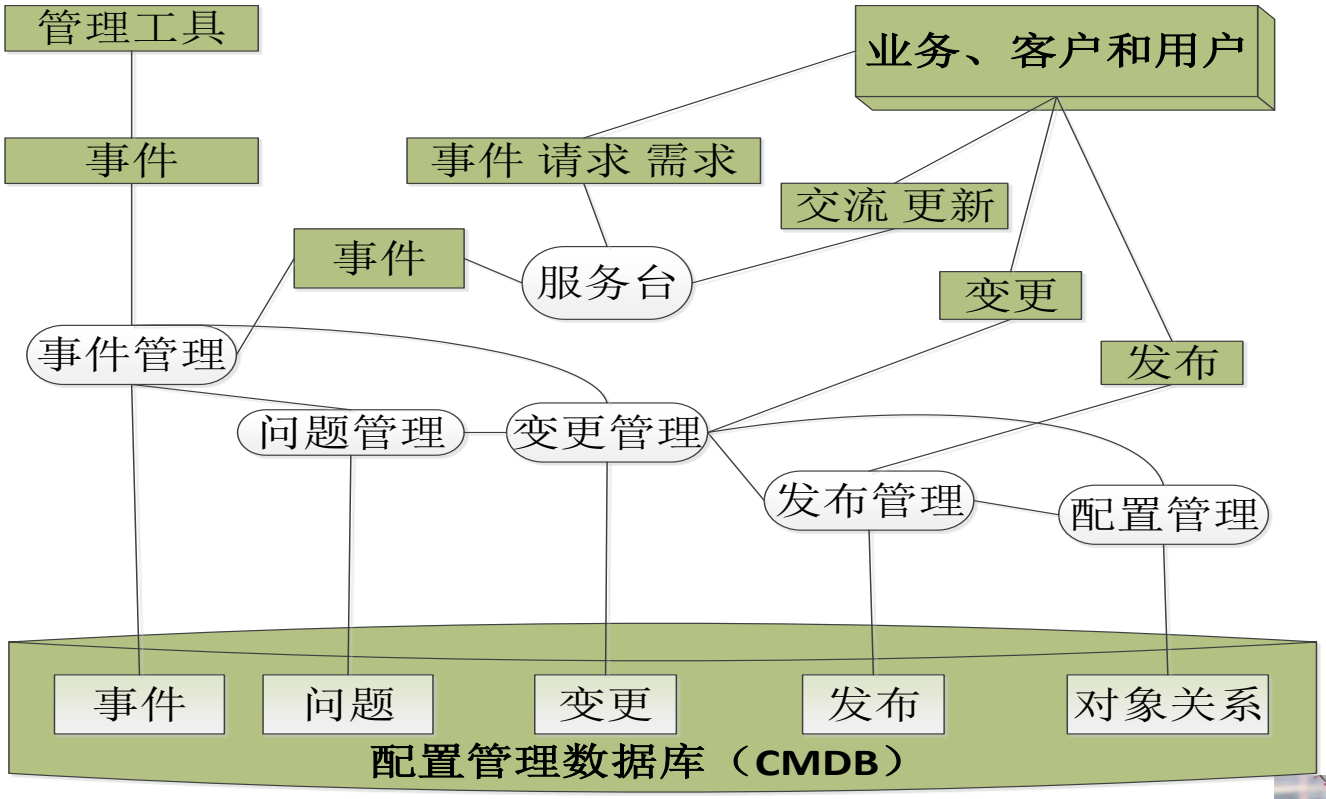
- 3.服务提供流程
  - 业务连续性管理
    - 见后面的章节

8.2 信息服务管理

- **4.服务支持流程**
  - 流程包括：服务台、事件管理、问题管理、配置管理、变更管理、发布管理、补丁管理
    - 主要面向用户（**End-Users**），用于确保用户得到适当的服务以支持组织的业务功能，确保**IT**服务提供方（**Provider**）所提供的服务质量，符合服务级别协议（**SLA**）的要求。

8.2 信息服务管理

- 4.服务支持流程
  - 子流程关系
    - 中心是服务台，重点对象是事件

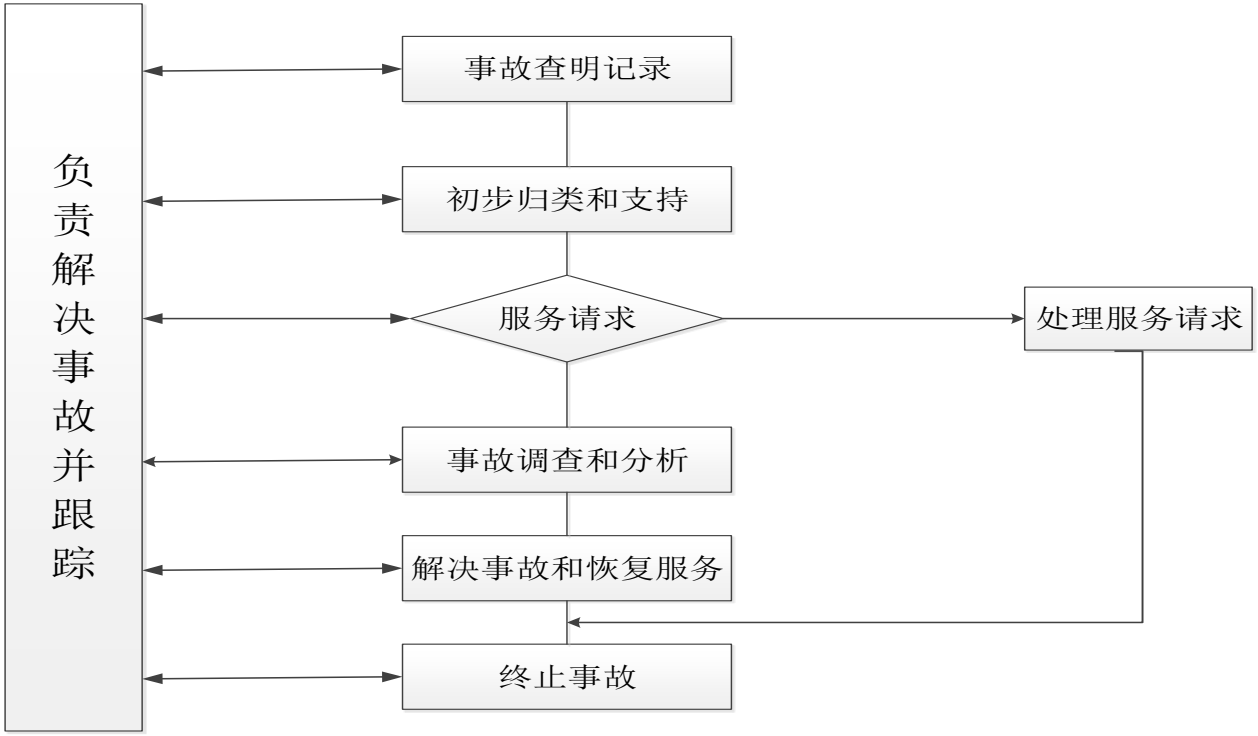


8.2 信息服务管理

- 4.服务支持流程
  - 事件管理
    - 服务台
      - 作用是控制和协调各“服务管理流程”，以提供使客户满意的服务
      - 是事件收集和分发处理的中心--**“流程”控制中心**
    - 事件处理流程
      - 服务台：作为所有事件的责任人，负责监督已登记事件的解决过程。将不能立即解决的事件转移给专家支持小组。
      - 专家组：首先提供临时性的解决办法或补救措施以尽可能快地恢复服务，避免影响用户正常工作。再分析事故发生原因，制定解决方案以恢复服务水平协议所规定的级别。
      - 最后服务台与客户一道验证方案实施效果并终止事件。

8.2 信息服务管理

- 4.服务支持流程
  - 事件管理
    - 事件处理流程图



8.2 信息服务管理

- 4.服务支持流程
  - 问题管理
    - 指负责解决IT服务运营过程中遇到的所有问题的过程。
    - 目标：将由于IT基础架构的错误而导致的问题和事件对业务产生的负面影响减小到最低，以及防止与这些错误有关的事件再次发生。
    - 包括：问题处理、问题控制

8.2 信息服务管理

- 4.服务支持流程
  - 配置管理
    - 指识别和确认系统的配置项、记录并报告配置项状态和变更请求、检验配置项的正确性和完整性等活动构成的过程。
    - 是“物理”控制中心，控制和协调各“IT基础架构组件”，以使服务台能够控制和协调各流程，从而提供让客户满意的服务。
    - 控制中心解决的问题
      - 为什么要控制（Why）
      - 控制的对象是谁（What）
      - 如何控制（How）

8.2 信息服务管理

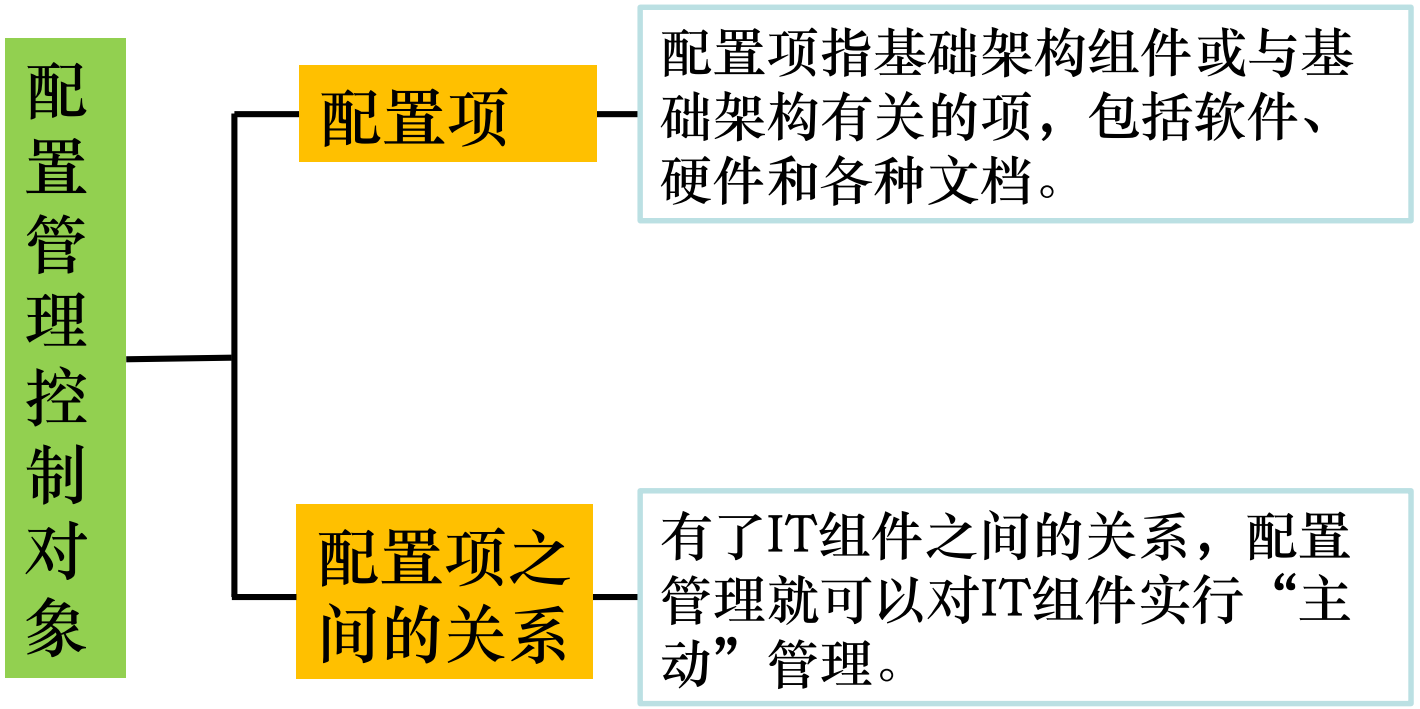
- 4.服务支持流程
  - 配置管理
    - 主要目标
      - 计量所有IT资产；
      - 为其它服务管理流程提供准确信息；
      - 作为事故管理、变更管理和发布管理的基础；
      - 验证基础架构记录的正确性并纠正发现的错误。
    - 实施配置管理的效益
      - 有效管理IT组件
      - 提供高质量的IT服务
      - 更好地遵守法规
      - 帮助制定财务和费用计划

8.2 信息服务管理

- 4.服务支持流程
  - 配置管理--实施效益
    - 有效管理IT组件
      - IT组件是IT服务的基础。每个服务涉及一个或多个配置项。
      - 配置项发生变动或丢失情况、所有人、责任人和应有的状况，流程方便用其它恰当的IT组件替换。
    - 提供高质量的IT服务
      - 协助处理变更、发现和解决问题以及提供用户支持；
      - 减少出现错误的次数，避免不必要的重复工作，从而提高了服务质量，降低了服务成本。
    - 更好地遵守法规
      - 维护IT基础架构的所有软件清单，防止使用非法的软件拷贝和使用包含病毒的软件。
      - 方便审计员发现非法的或有病毒的软件的有关责任人。
    - 帮助制定财务和费用计划
      - 提供所有配置项的完整列表，容易计算维护和软件许可费用，了解软件许可证过期日期和配置项失效时间以及配置项替换成本。有助于财务计划的制定。

8.2 信息服务管理

- 4.服务支持流程
  - 配置管理—控制对象



8.2 信息服务管理

- 4.服务支持流程
  - 配置管理—控制过程(四步)
    - 配置标识
      - 确定配置项的范围、属性、标识符、基准线以及配置结构和命名规范。
    - 配置项控制
      - 在正式建立配置文档后对配置项变更进行控制的各种活动
        - » 注册新配置项及其版本；
        - » 更新配置项记录；
        - » 许可证管理；
        - » 撤销或删除配置项时存档有关记录；
        - » 保护各种配置的完整性；
        - » 定期检查配置项以确保它的存在性和合规性并相应更新配置管理数据库。

8.2 信息服务管理

- 4.服务支持流程
  - 配置管理—控制过程(四步)
    - 配置状况报告
      - 指定期报告所有受控配置项的当前状态及其变更历史，它可用来建立系统基准线、跟踪基准线和发布版本之间的变动情况。
    - 配置验证和评审
      - 指一系列评价和审查以确认配置项是否实际存在，以及是否在配置管理系统中正确地记录了它们。

8.2 信息服务管理

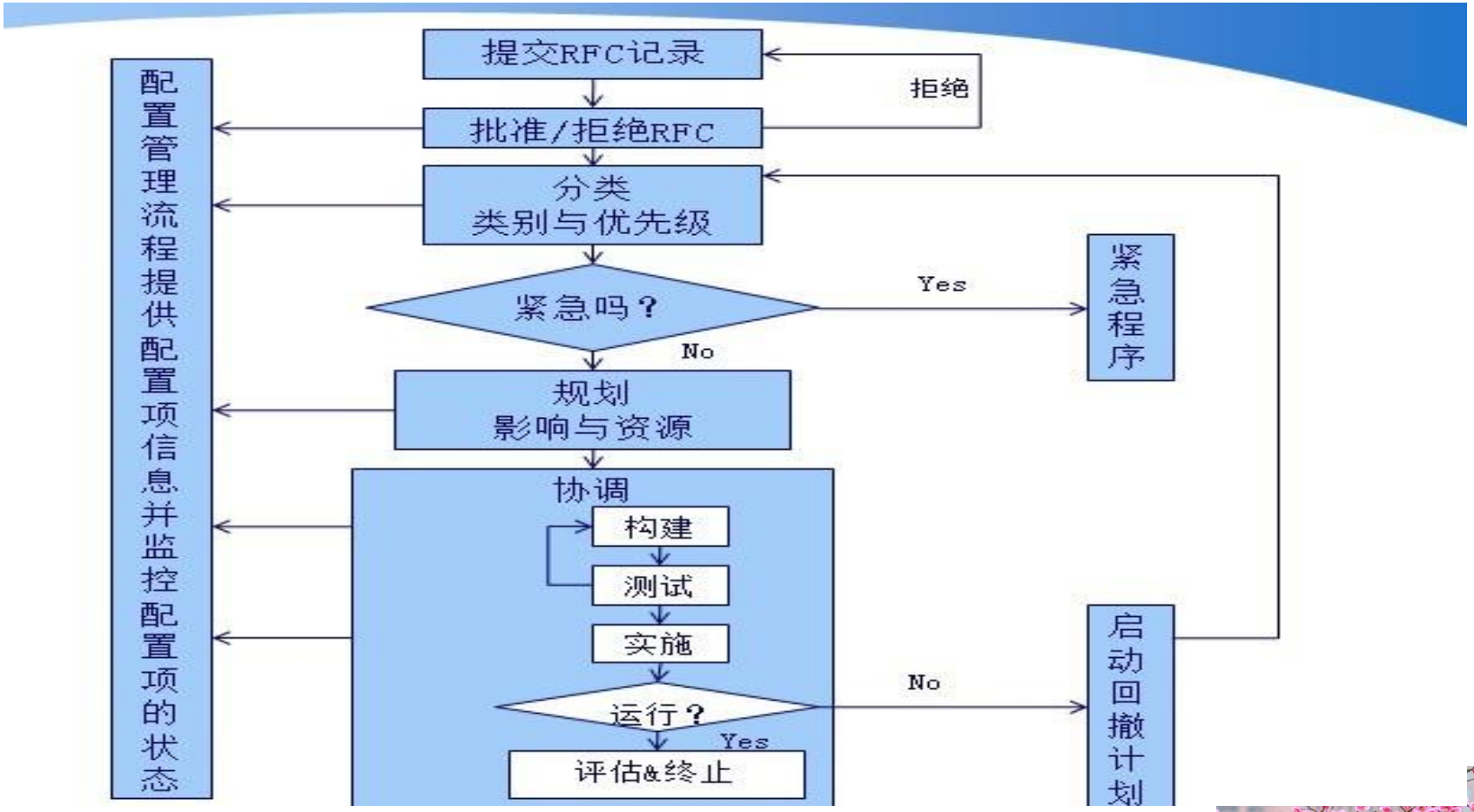
- 4.服务支持流程
  - 变更管理
    - 指在用IT服务的方法来管理与变更有关事件的过程，以减少错误的发生。
    - 目的
      - 标准化的方法和程序用于有效快速处理变更
      - 所有的服务资产变更及它们的配置都被记录在配置管理系统中
      - 优化整体商业风险
    - 范围
      - 服务资产基线及其在整个服务生命周期的配置项

8.2 信息服务管理

- 4.服务支持流程
  - 变更管理---原则
    - 建立组织变更管理文化
    - 变更管理流程与企业项目管理、利益相关者的变更管理流程要一致
    - 职责分离
    - 建立单一节点，减少冲突和潜在问题
    - 防止生产环境中的未授权变更
    - 和其他服务管理进程一致从而可以追踪变更、发现未授权变更
    - 评估影响服务能力的变更的风险和性能
    - 流程的绩效评估

8.2 信息服务管理

- 4.服务支持流程
  - 变更管理---流程



8.2 信息服务管理

- 4.服务支持流程
  - 变更管理
    - 操作系统和应用软件应严格控制变更管理
      - 重大变更的标识和记录。
      - 变更的策划和测试。
      - 对这种变更的潜在影响的评估，包括安全影响。
      - 对建议变更的正式批准程序。
      - 向所有有关人员传达变更细节。
      - 返回程序，包括从不成功变更和未预料事态中退出和恢复的程序与职责。

8.2 信息服务管理

- 4.服务支持流程
  - 发布管理
    - 发布是指经过测试并导入实际应用环境的新增或改进的配置项的集合。
      - 任务：负责计划与实施 IT 服务的变更，并描述各个变更
      - 目标：规范实施变更流程及测试确保应用系统的质量。
    - 发布的规划
      - 对版本的内容、发布的时间阶段、地理位置、业务单位和客户等方面达成一致；
      - 产生和一个高层的发布日程安排；
      - 规划所需的资源级别（包括人员加班）；
      - 在角色与职责上达成一致；
      - 制定失败回退计划；
      - 为发布制定一个质量计划；
      - 规划支持小组和客户对发布的验收。

8.2 信息服务管理

- 4.服务支持流程
  - 发布管理
    - 发布的类型
      - **Delta发布(Delta Release)**
        - » 指仅仅对自上次全发布或 **Delta** 发布以来发布单元中实际发生变化或新增的那些配置项进行发布的方式。
      - 全发布（**Full Release**）
        - » 指同时构建、测试、分发和实施发布单元的所有组件的发布方式。
      - 包发布**(Package Release)**
        - » 指将一组软件配置项以包的形式一起导入实际运作环境的发布方式。

8.2 信息服务管理

- 4.服务支持流程
  - 发布管理
    - 应用软件发布的类型
      - alpha版：α内部测试版。
        - » 可能包含很多BUG，功能不健全，为开发和找BUG用的。
      - beta版：β公开测试版。
        - » 较稳定，用户测试使用，会不断增加新功能。
      - rc版(Release Candidate)：候选版本。
        - » 最终发行版的预览版
      - stable版：稳定版。
    - 商业软件
      - RTM版(Release to Manufacture)：工厂版。
      - OEM版：厂商定制版。
      - EVAL版：评估版。有30-60天使用期限。
      - RTL版：Retail.(零售版)，对外出售。

8.2 信息服务管理

- 4.服务支持流程
  - 补丁管理
    - ITIL补丁管理策略的4个重要阶段
      - 重要阶段1：配置管理
        - » 详细了解现有的IT环境是补丁升级成功的第一步。
      - 重要阶段2：风险评估
        - » 对存在漏洞的系统进行调查和风险评估，并获取补丁程序的信息。
      - 重要阶段3：变更管理
        - » IT部门提出变更请求，企业指定变更管理人对变更请求进行审核和批准。
      - 重要阶段4：发布管理
        - » 尽可能地减小新补丁程序对当前业务和现有IT架构的不利影响，并指导下属部门进行补丁程序的更新操作。

8.2 信息服务管理

- 4.服务支持流程
  - 补丁管理
    - 实施补丁管理策略的目的
      - 提供统一的补丁升级流程，忽视设备或平台间的差异。
        - » 企业可以根据业务的发展灵活地调整该补丁升级流程，增强它保障业务的能力。
        - » 使企业IT架构的补丁升级行为更为规范，升级操作更有把握。
      - 掌握信息资产、漏洞情况和补丁程序信息。
        - » 这些关键信息为补丁升级准确决策，操作人员灵活实施补丁升级操作，提高升级操作的效率和准确率。
      - 提升企业对IT架构的信心。
        - » IT架构是企业处理业务的核心支柱。
        - » 补丁管理策略能够提升IT架构的可用性，增强企业对IT架构的信心。

8.2 信息服务管理

- 4.服务支持流程
  - 补丁管理
    - 实施基于ITIL的补丁管理策略的好处
      - 使补丁升级的流程更具可重复性、可执行性，同时也更为有效。按照业务的需求降低补丁升级的风险。
      - 将企业IT应用中常见的“哪里出问题就去哪里救火”的处置思想改进为更有计划和准备的处置方法。
      - 在一个不断改变的环境中依然能够保证足够的安全性，企业还能定时回顾并改进流程本身。

8.3 安全事件管理

- 1. 安全事件管理概述
  - 信息安全事件(GB/T 20985.1—2017定义)
    - 与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全违规或控制失效。
  - 信息安全事件管理
    - 指采用一致和有效方法处理信息安全事件的行为。
    - 目的是规范突发安全事件的处理，降低其对信息资产造成机密性、完整性、可用性方面的负面影响。
    - 包括信息安全事件分类、报告、处理、分析、总结等内容。

8.3 安全事件管理

- 1. 安全事件管理概述
  - 信息安全事件分类
    - 信息安全事件可分为七类
      - 有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。
    - 信息安全事件分级
      - Ⅰ级：特别重大事件，可能或已造成特别严重损失或影响
      - Ⅱ级：重大事件，可能或已造成严重损失或影响
      - Ⅲ级：较大事件，可能或已造成较大损失或影响
      - Ⅳ级：一般事件，可能或已造成较小损失或影响

8.3 安全事件管理

- 1. 安全事件管理概述
  - 信息安全事件处理
    - 发现、报告、评估、响应和处置信息安全事件并从中汲取经验教训的行动。
    - 处理流程包括
      - 监控、报告、通知、分析、响应、处置和整改流程
  - 信息安全事件响应
    - 为缓解或解决信息安全事件而采取的行动，包括为保护信息系统及其存储的信息并将其恢复至正常运行状态而采取的行动。
  - ITIL安全事件管理
    - 主要包括安全事件监控和安全事件响应

8.3 安全事件管理

- **2. ITIL安全事件监控**
  - 基于合规性或审计目的，跟踪和记录安全数据，实时监控和分析安全事件的发生和可能。
  - 目标
    - 预防内部各业务系统由于权限滥用或者管理不当所导致网络信息安全事件发生；
    - 及时处理由此引发的各类信息安全事件；
    - 降低或者避免突发安全事件造成的经济损失与社会影响，保障网络与业务系统正常运行。
  - 要求
    - 应监视系统，记录信息安全事态。
    - 应使用操作员日志和故障日志以确保识别出信息系统的问题。

8.3 安全事件管理

- **2. ITIL安全事件监控**
  - 安全事件的监控方法与内容
    - 大多通过单一安全控制台，集中地管理安全事故和漏洞，为企业用户提供安全架构的总体视图。
    - 主要包括安全事件的收集、安全事件的归并和过滤、安全事件标准化、安全事件显示和报表
  - 监控意义
    - 安全事件是需要安全运维人员重点关注的内容。
    - 通过安全事件监控，可以帮助企业积极监控整个组织内的IT资源，过滤并关联事件，迅速定位安全威胁，并为安全事件响应提供支持。
    - 使企业用户能够研究网络拓扑，了解受影响的资源的位置并判断问题的真正根源。

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 监控需求
    - 解决因网络规模庞大，监控范围难以覆盖的问题
    - 如何对安全事件进行风险评估、分析
    - 多样的安全事件如何归一化，实现全网监控
  - 监控挑战
    - 如何确保信息系统安全运行
    - 如何降低运维管理成本
    - 如何完善安全事件监控

8.3 安全事件管理

- **2. ITIL安全事件监控**
  - 监控核心问题
    - 如何对采集到的各类安全监控事件进行风险评估，划分出安全风险级别。
    - 做到有效的安全事件风险等级的识别和判定。
  - 监控运转流程
    - 由系统运行时产生的事件的日志生成、采集、分析.
  - 监控目的
    - 安全管理员能够根据事件的风险级别确定事件处理的优先级，按照轻重缓急的策略来协调资源并处理各类安全事件，实现信息系统整体安全风险管理和风险控制的目的。

8.3 安全事件管理

- **2. ITIL安全事件监控**
  - 监控运转流程

安全事件监控数据呈现

安全事件归一化

安全事件关联分析

安全事件管理

安全事件预警

安全事件知识库管理
安全事件数据报表管理

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 监控主要工作
    - （1）综合建立统一管理平台
      - 管理和维护人员可日常操作管理平台，监控安全事件
    - （2）海量安全事件归一化处理
      - 平台收集海量的异构数据转化为统一的数据格式，便于关联分析和风险评估。
    - （3）关联分析
      - 海量安全事件的抽取、降噪、剥离无用信息，降低监控管理的复杂性。
    - （4）安全事件管理
      - 采用一种实时的、动态的管理模型，通过收集、标准化、过滤、归并和关联后，分析来自于不同地点、不同层次、不同类型的信息事件；
      - 帮助发现真正关注的安全风险，提高安全报警的信噪比；
      - 准确实时地评估当前的安全态势和风险,并根据策略作出快速响应。

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 监控主要工作
    - （5）安全事件预警
      - 分析内部预警信息、外部预警信息，提前通告可能发生的威胁，提供各类安全威胁、安全风险、安全态势、安全隐患等信息。提供规则用户设定功能，准确定位安全问题和有针对性地进行响应处理。
    - （6）安全事件知识库
      - 一个集中存放、管理、查询安全知识的环境。
      - 监控积累建立的各类安全事件知识库、安全事件处理方法和应急方案的集合，可以共享和利用。
    - （7）安全事件报表统计
      - 各类安全运行数据的统计、挖掘、分析的呈现；
      - 形式化、标准化的报表报告展现数据结果，满足企业遵从安全法规的建设需求。

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 信息系统监控
    - 检测未经授权的信息处理活动。
    - 通过监视信息系统的日志等信息，记录信息安全事态。
      - 系统管理员和系统操作员的活动应记入日志。
      - 错误和故障日志记录会影响系统的性能。故障应被记录、分析，并采取适当的措施。
      - 日志应定期评审，使用操作员日志和故障日志以确保识别出信息系统的问题。
    - 待分析的日志
      - 管理员和操作员日志
      - 故障日志与审计日志

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 信息系统监控
    - 管理员和操作者日志通常包括内容
      - 事态（成功的或失败的）发生的时间；
      - 关于事态（例如处理的文件）或故障的信息；
      - 涉及的帐号和管理员或操作员；
      - 涉及的过程。
    - 错误和故障日志记录与评审原则
      - 与信息处理或通信系统的问题有关的用户或系统程序所报告的故障要加以记录。
      - 评审故障日志，以确保已满意地解决故障；
      - 评审纠正措施，以确保没有危及控制措施的安全，以及所采取的措施给予了充分授权。

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 信息系统监控
    - 审计日志
      - 应产生记录用户活动、异常和信息安全事态的审计日志；
      - 保持一个已设的周期以支持将来的调查和访问控制监视。
      - 包含入侵者和机密人员的敏感信息，应采取适当的隐私保护措施。

8.3 安全事件管理

- **2. ITIL安全事件监控**
  - **– 信息系统监控**
    - 审计日志

审计日志包含内容

用户ID	对系统尝试访问的记录	系统配置的变化
终端身份或位置	网络地址和协议	特殊权限的使用
防护系统的激活和停用	访问控制系统引发的警报	访问的文件和访问类型
日期、时间和关键事态的细节	对数据以及其他资源尝试访问的记录	系统实用工具和应用程序的使用

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 信息系统监控
    - 监视程序
      - 应建立信息处理设施的监视使用程序，并定期评审监视活动的结果。
      - 必须使用监视程序以确保用户只执行被明确授权的活动。各个设施的监视级别应由风险评估决定。
    - 监视活动的结果评审
      - 监视活动的结果多长时间进行评审应依赖于涉及的风险。
      - 应考虑的风险因素包括：应用过程的关键程度；所涉及信息的价值、敏感度和关键程度；系统渗透和不当使用的经历，脆弱性被利用的频率；系统互连接的程度（尤其是公共网络）；设备被停用的日志记录。

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 信息系统监控
    - 监视活动范围：
      - 授权访问
        - » 例如：用户ID；关键事态的日期和时间；事态类型；访问的文件；使用的程序/工具；
      - 所有特殊权限操作
        - » 例如：特殊权限帐户的使用，例如监督员、根用户、管理员；系统的启动和终止；I/O设备的装配/拆卸；
      - 未授权的访问尝试
        - » 例如：失败的或被拒绝的用户活动；失败的或被拒绝的涉及数据和其他资源的活动；违反访问策略或网关和防火墙的通知；私有入侵检测系统的警报；
      - 系统警报或故障
        - » 例如：控制台警报或消息；系统日志异常；网络管理警报；访问控制系统引发的警报；
      - 改变或企图改变系统的安全设置和控制措施

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 日志保护
    - 记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。
      - 系统日志通常包含大量的信息，如果其中的数据被修改或删除，可能导致一个错误的安全判断。
    - 日志设施被未授权更改或出现操作问题示例：
      - 更改已记录的消息类型；
      - 日志文件被编辑或删除；
      - 超越日志文件介质存储能力的界限，导致不能记录事态或过去记录事态被覆盖。

8.3 安全事件管理

- 2. ITIL安全事件监控
  - 系统时钟支持
    - 时间不准确的审计日志可能妨碍调查，并损害这种证据的可信性。
      - 审计日志可用于调查或作为法律、法规案例的证据。
    - 正确设置计算机时钟对确保审计记录的准确性是重要的。
    - 一个组织或安全域内的所有相关信息处理设施的时钟应使用已设的精确时间源进行同步。

8.3 安全事件管理

- 3. ITIL安全事件响应
  - 安全事件应急响应概述
    - 通常指企业为了应对各种意外事件的发生所做的准备以及在事件发生后所采取的措施。
    - 由应急响应组织根据事先对各种可能情况的准备，在安全事件发生后，响应、处理、恢复、跟踪的方法及过程。
    - 安全事件应急响应是一种被动性的安全体系，是持续运行并由一定条件触发的体系。
    - 补救性的安全事件应急响应是必不可少的。
      - 已发生的安全事件造成企业损失和危害性影响；
      - 并非所有的实体都有足够的实力进行信息安全管理。

8.3 安全事件管理

- 3. ITIL安全事件响应
  - 安全事件应急响应概述
    - 安全事件应急响应的作用
      - 主要表现在事先的充分准备和事件发生后采取的措施两个方面。
    - 应急响应的对象：
      - 泛指针对计算机和网络所处理的信息的所有安全事件；
      - 事件主体可能来自人、故障、病毒与蠕虫或自然灾害等。
    - 安全事件应急响应准备与措施
      - 事先准备：包括信息安全管理培训、制定安全政策和应急预案以及风险分析等，安全技术上则要增加系统安性，如备份、部署安全产品等。
      - 事后措施：包括抑制、根除和恢复等措施，让企业尽可能地减少损失、尽快恢复正常运行。

8.3 安全事件管理

- 3. ITIL安全事件响应
  - 安全事件应急响应具体工作
  - 应急响应的工作需求
    - 制定安全事件响应计划、组建安全事件响应小组、确定团队人员角色等。
    - 建设需求
      - » 如何快速响应突发的安全事件
      - » 如何建全响应措施,降低企业损失
      - » 如何规范响应制度,实现响应专业化管理
      - » 如何统筹全局,建立企业安全事件响应体系

8.3 安全事件管理

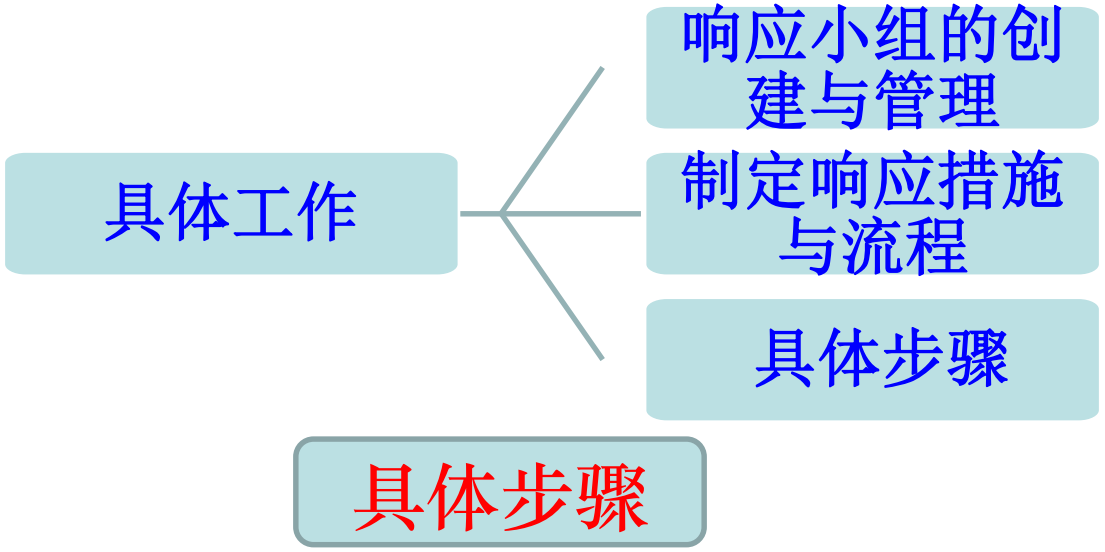
- 3. ITIL安全事件响应
  - 安全事件应急响应具体工作
    - 如何快速响应突发的安全事件
      - 部署的安全设备可能起不到应有的作用,无法全部解决网络中频繁出现的安全事件,企业网络中一旦出挑安全事件时,企业安全管理人员不能及时发现, 也无法及时处理.
    - 如何建全响应措施,降低企业损失
      - 企业安全管理人员无法全面了解整个企业网络中正在发生的内部越权访问和外部攻击,新出现的网络蠕虫病毒造成了较大的损失,甚至造成工作和业务停顿,但无法根除,也缺少必要措施应对.
    - 如何规范响应制度,实现响应专业化管理
      - 在企业网络出现问题的情况下,企业安全管理人员无从下手或者手忙脚乱, 也没有相应的机制、制度指导该如何处理,无法迅速查明真正的原因.
    - 如何统筹全局,建立企业安全事件响应体系
      - 企业各个单位各自为政,对遇到的安全问题无法进行统一考虑,导致同样的安全问题多次出现,同时缺少统一规范的快速处理措施及流程.各自为政的单位的随意性,使得企业无法建立统筹全局的安全事件响应体系.

8.3 安全事件管理

- **3. ITIL安全事件响应**
  - 安全事件应急响应具体工作
    - 企业更多关注自身的核心业务，信息安全工作交由专业安全厂商来完成。
    - 企业的安全外包服务还包括，信息安全咨询与培训服务，企业网站安全检测服务，企业病毒防护清除服务，企业安全评估与加固服务， 定制化、集成化的信息安全外包服务等。
    - 安全事件响应划分为六个阶段: 准备、检测、抑制、根除、恢复、追踪。

8.3 安全事件管理

- **3. ITIL安全事件响应**
  - 安全事件应急响应具体工作



8.4 信息系统安全审计

- 1.信息系统审计概述
  - Ron Weber，1999
    - 信息系统审计是一个获取并评价证据，以判断信息系统是否能够保证资产的安全、数据的完整以及有效率地利用组织的资源并有效果地实现组织目标的过程。
  - 日本通产省，1996
    - 为了信息系统的安全、可靠与有效，由独立于审计对象的IT审计师，以第二方的客观立场对以计算机为核心的信息系统进行综合的检查与评价，向IT审计对象的最高领导，提出问题与建议的一连串的活动。

8.4 信息系统安全审计

- 1.信息系统审计概述
  - 邓少灵，2002
    - IS审计是指对信息系统从计划、研发、实施到运行维护各个过程进行审查与评价的活动，以审查企业信息系统是否安全、可靠、有效，保证信息系统得出准确可靠的数据。
  - 信息系统审计
    - 就是以企业或政府等组织的信息系统为审计对象，通过现代的审计理论和IT管理理论，从信息资产的安全性、数据的完整性以及系统的可靠性、有效性和效率性等方面出发，对信息系统从开发、运行到维护的整个生命周期过程进行全面审查与评价，以确定其是否能够有效可靠地达到组织的战略目标，并为改善和健全组织对信息系统的控制提出建议的过程。

8.4 信息系统安全审计

- 1.信息系统审计概述
  - 信息系统审计界定
    - 指根据公认的标准和指导规范，对信息系统及其业务应用的效能、效率、安全性进行监测、评估和控制的过程，以确认预定的业务目标得以实现。
  - 信息系统审计意义
    - 是保证信息系统质量的重要工具。
    - 是企业信息化发展的必然要求。
    - 信息化建设的效益需要信息系统审计。
    - 信息系统审计有利于维护信息时代的市场经济秩序。

8.4 信息系统安全审计

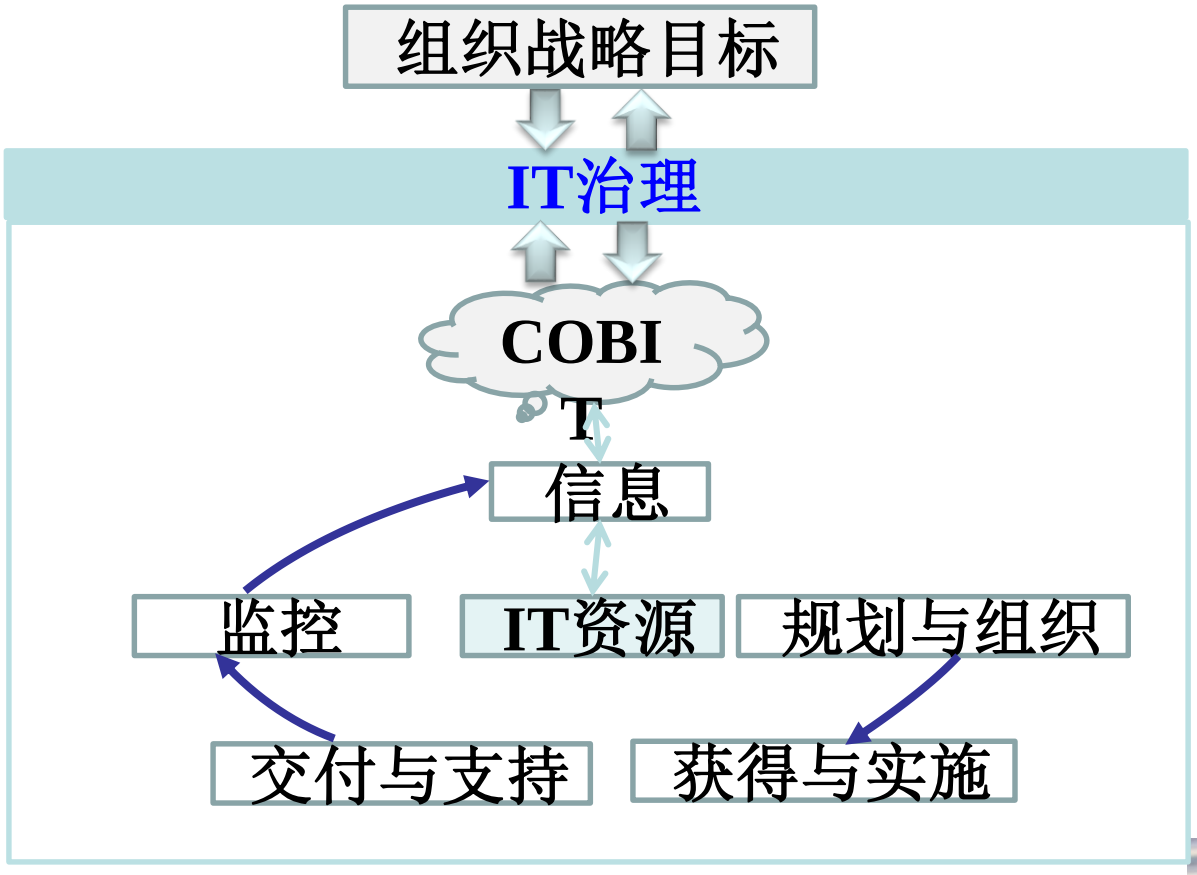
- 1.信息系统审计概述
  - 信息系统审计主要内容
    - 信息系统开发过程审计
    - 信息系统内部控制的评价
    - 信息系统应用程序审计
    - 信息系统数据文件审计

8.4 信息系统安全审计

- **2. 信息系统审计标准COBIT**
  - 审计标准COBIT
    - 由信息系统审计和控制协会（ISACF）于1996年发布
    - 国际通用的信息系统审计标准，为信息系统审计和治理提供一整套的控制目标、管理措施、审计指南等。
    - 把IT划分为4个域，并进一步细分为34个流程：
    - 规划与组织（PO） ⟶ 评估风险
    - 获取与实施（AI） ⟶ 安全审计
    - 交付与支持（DS） ⟶ 确保持续的服务
    - 监控（M） ⟶ 保证系统安全

8.4 信息系统安全审计

- 2. 信息系统审计标准COBIT
  - 审计标准COBIT：模型



8.4 信息系统安全审计

- **2. 信息系统审计标准COBIT**
  - 审计标准COBIT：4个域34个流程

1 规划与组织PO

PO1 制定IT战略规划
PO2 确定信息体系结构
PO3 确定技术方向
PO4 定义IT组织与关系
PO5 管理IT资产
PO6 沟通管理目标与方向
PO7人力资源管理
PO8 确保符合外部需求
PO9 风险评估
PO10 项目管理
PO11 质量管理

2 获取与实施AI

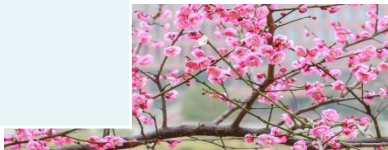
AI1 确定自动化解决方案
AI2 获取并维护应用软件
AI3 获取并维护技术基础设施
AI4 程序开发与维护
AI5 系统安装与鉴定
AI6 变更管理

3 交付与支持DS

DS1 定义并管理服务水平
DS2 管理第三方服务
DS3 性能管理与容量管理
DS4 确保服务的连续性
DS5 确保系统安全
DS6 确定并分配成本
DS7 教育并培训用户
DS8 为客户提供帮助和建议
DS9 配置管理
DS10 问题管理和突发事件管理
DS11 数据管理
DS12 设施管理
DS13 操作管理

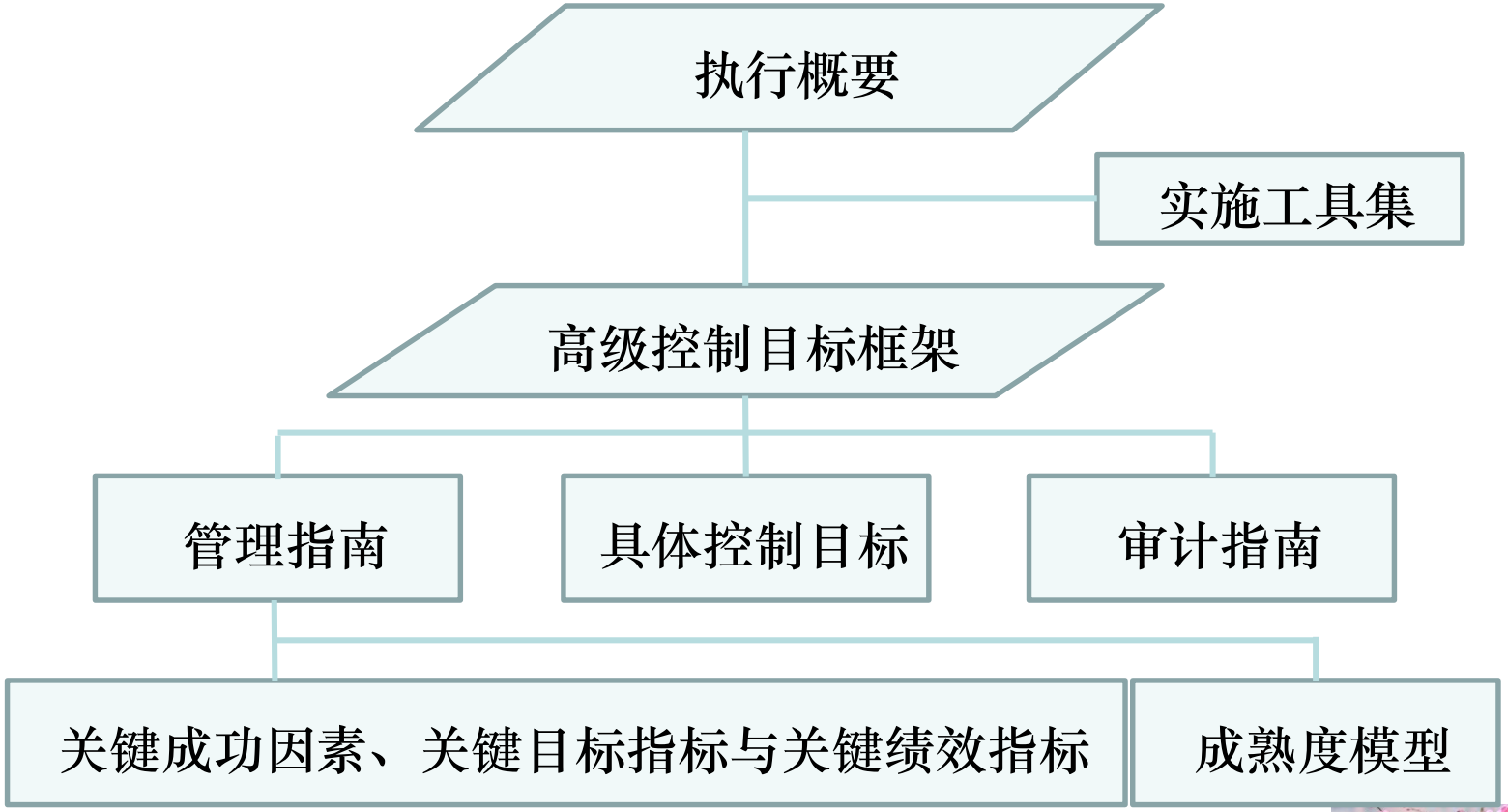
4 监控M

MI 过程监控
M2 评价内部控制的适当性
M3 确保独立性鉴定
M4 提供独立性审计



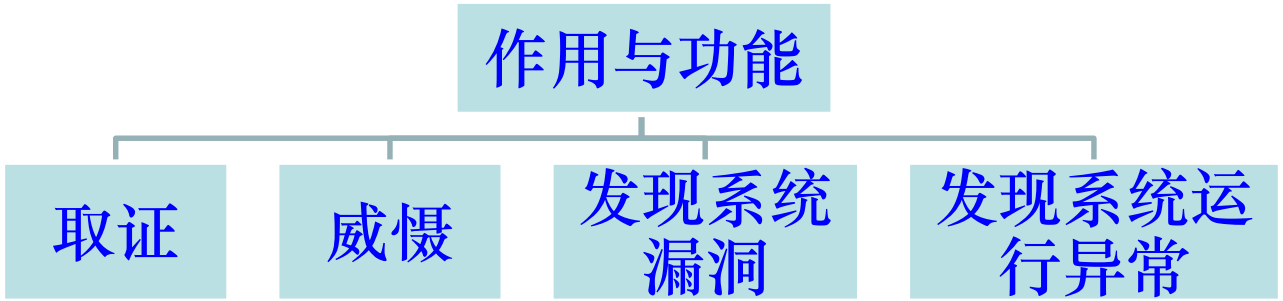
8.4 信息系统安全审计

- 2. 信息系统审计标准COBIT
  - 审计标准COBIT：产品家族分类



8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 是信息系统审计全过程的组成部分，应用于计算机网络信息安全领域，是对安全控制和事件的审查评价。
  - 作用与功能

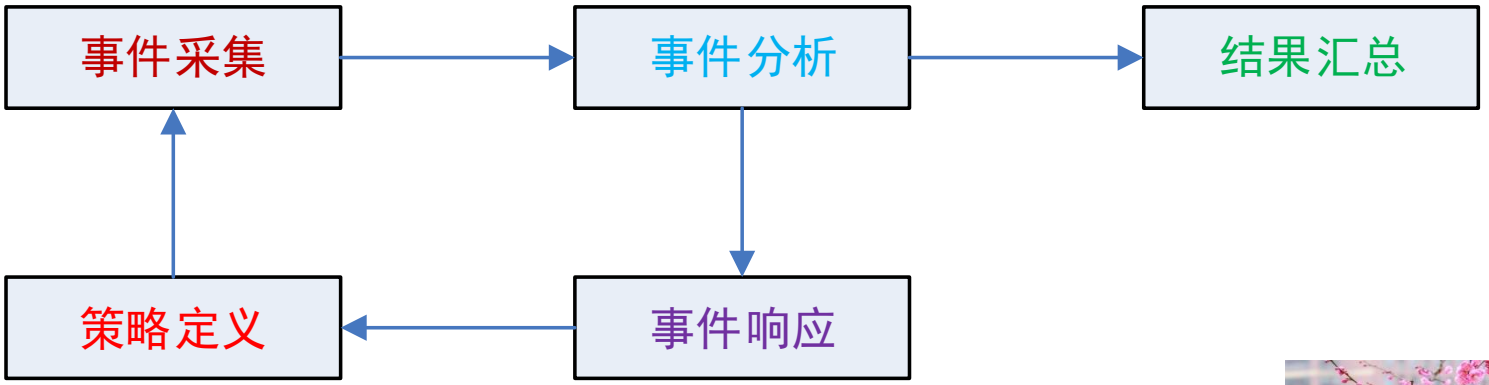


8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 作用与功能
    - 取证：
      - 利用审计工具监视和记录系统的活动情况，并放入系统日志中，可打印输出提供审计报告，对于已经发生的系统破坏行为提供有效的追纠证据。
      - 如记录用户登录帐户、登录时间、终端以及所访问的文件、存取操作等。
    - 威慑：
      - 通过审计跟踪，并配合相应的责任追究机制；
      - 对外部的入侵者以及内部人员的恶意行为具有威慑和警告作用。
    - 发现系统漏洞：
      - 安全审计为系统管理员提供有价值的系统使用日志；
      - 帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞。
    - 发现系统运行异常：
      - 安全审计为系统管理员提供系统运行的统计日志，管理员可根据日志分析网络或系统的安全性，输出分析报告，能及时发现系统的异常行为，采取相应的处理措施。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计策略
    - 规定哪些信息需要采集、哪些事件是危险事件、以及对这些事件应如何处理等。
    - 审计前应制定一定的审计策略，并下发到各审计单元。
    - 事件处理结束后，应根据对事件的分析处理结果来检查策略的合理性，必要时应调整审计策略。
  - 安全审计流程



8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计流程
    - 事件采集阶段
      - 将事件其他各阶段提交的审计策略分发至各审计代理，审计代理依据策略进行客体事件采集。
      - 按照预定的审计策略对客体进行相关审计事件采集；
      - 形成的结果交由事件后续的各阶段来处理。
      - 审计代理：安全审计系统中完成审计数据采集、鉴别并向审计跟踪记录中心发送审计消息的功能部件，包括软件代理和硬件代理。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计流程
    - 事件分析阶段
      - 按照预定策略，对采集到事件进行事件辨析，决定：
        - » 1）忽略该事件；
        - » 2）产生审计信息；
        - » 3）产生审计信息并报警；
        - » 4）产生审计信息且进行响应联动。
      - 按照用户定义与预定策略，将事件分析结果生成审计记录，并形成审计报告；

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计流程
    - 事件响应阶段
    - 根据事件分析结果采用相应的响应行动，包含：
      - a)对事件分析阶段产生的报警信息、响应请求进行报警与响应；
      - b)按照预定策略，生成审计记录，写入审计数据库，并将各类审计分析报告发送到指定的对象；
      - c)按照预定策略对审计记录进行备份；

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计流程
    - 结果汇总阶段
    - 负责对事件分析及响应的结果进行汇总，包含：
      - a)将各类审计报告进行分类汇总；
      - b)对审计结果进行适当的统计分析，形成分析报告；
      - c)根据用户需求和事件分析处理结果形成审计策略修改意见。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计分析方法
    - (1)基于规则库的安全审计方法
      - 将已知的攻击行为进行特征提取，把这些特征用脚本语言等方法进行描述后放入规则库中；
      - 当进行安全审计时，将收集到的审核数据与这些规则进行某种比较和匹配操作(关键字、正则表达式、模糊近似度等)，从而发现可能的网络攻击行为。
      - 方法自身局限性：
        - » 对于特征十分明显的网络攻击行为，效果非常好；
        - » 对于其他非常容易产生变种的网络攻击行为，规则库很难完全满足要求。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计分析方法
    - (2)基于数理统计的安全审计方法
      - 先给对象创建一个统计量的描述，比如一个网络流量的平均值、方差等等，统计出正常情况下这些特征量的数值；
      - 用特征量来对实际网络数据包的情况进行比较，当发现实际值远离正常数值时，就可以认为是潜在的攻击发生。
      - 方法局限性：
        - » 统计量的“阀值”即正常数值和非正常数值的分界点
        - » 阀值的设定取决于管理员的经验，不可避免产生误报和漏报。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计分析方法
    - (3)基于日志数据挖掘的安全审计方法
      - 从系统使用或网络通信的“正常”数据中发现系统的“正常”运行模式，并和常规的一些攻击规则库进行关联分析，并用以检测系统攻击行为。
      - 带有学习能力的数据挖掘方法；
      - 检测准确率高、速度快、自适应能力强等优点。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计分析方法
    - (4)其它安全审计方法
      - 入侵检测分析方法
    - 区别
      - 安全审计是根据收集到的关于已发生事件的各种数据来发现系统漏洞和入侵行为，能为追究造成系统危害的人员责任提供证据，是一种事后监督行为。
      - 入侵检测是在事件发生前或攻击事件正在发生过程中，利用观测到的数据，发现攻击行为。
      - 目的都是发现系统入侵行为，分析方法有很大的相似之处
      - 入侵检测要求有更高的实时性。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计数据源
    - 安全审计系统的输入数据分为三类：基于主机、基于网络和其他途径。
    - (1)基于主机的数据源
      - a)操作系统的审计记录
        - » 由OS的专门审计子系统所产生，目的是记录当前系统的活动信息，并将这些信息按照时间顺序组织为一个或多个审计文件。
        - » 如用户进程所调用的系统调用类型、执行的命令行等
      - b)系统日志
        - » 日志分为操作系统日志和应用程序日志两部分。
        - » 分别由操作系统和应用程序自己生成并维护。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计数据源
    - (1)基于主机的数据源
      - C)WEB服务日志信息
        - » 操作系统审计记录和系统日志都属于系统级别的数据源信息，通常由操作系统及其标准部件统一维护；是安全审计优先选用的输入数据源。
        - » 管理者无法单纯从内核底层级别的数据源来分析判断系统活动的情况；
        - » 入侵攻击行为的目标日益集中于提供网络服务的特定应用程序。
        - » Web服务器的日志信息反应系统活动的较高层次的抽象信息，支持访问日志的特定应用程序。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计数据源
    - (2)基于网络的数据源
      - 输入数据即网络中传输的数据。
      - 通过网络被动监听的方式获取网络数据包，不会对目标监控系统的运行性能产生任何影响，无需改变原有的结构和工作方式。
      - 嗅探工作采用网络用户透明模式，降低了其本身受到攻击的概率。
      - 可以发现许多基于主机数据源所无法发现的攻击手段
        - » 例如基于网络协议的漏洞发掘过程，或是发送畸形网络数据包和大量误用数据包的DOS攻击等。
      - 网络数据包的标准化程度比主机数据源高
        - » 基于TCP/IP协议簇。

8.4 信息系统安全审计

- 3. 信息安全系统审计
  - 安全审计数据源
    - (3)其它数据源
      - a)来自其它安全产品的数据源(防火墙、身份认证系统、访问控制系统等)
      - b)来自网络设备的数据源(网络管理系统等)
      - c)带外数据源(人工方式提供的数据信息)

小结

- 信息资产是指对组织具有价值的信息资源，是安全策略保护的对象。
  - 信息资产分为数据、软件、硬件、文档、服务、人员等。
  - 资产责任人应负责确保与信息处理设施相关的信息和资产进行了适当的分类和标记；确定并周期性评审访问限制和分类，要考虑到可应用的访问控制策略。
- ITIL的核心模块：“服务管理”
  - “服务提供”流程
    - 包括服务级别管理、可用性管理、能力管理、IT服务财务管理、IT服务持续性管理。
  - 服务支持流程
    - 包括：服务台、事件管理、问题管理、配置管理、变更管理、发布管理、补丁管理

小结

- 信息安全事件(GB/T 20985.1—2017定义)
  - 与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全违规或控制失效。
- 信息安全事件管理
  - 指采用一致和有效方法处理信息安全事件的行为。
  - 包括信息安全事件分类、报告、处理、分析、总结等内容。
- 信息系统审计
  - 指根据公认的标准和指导规范，对信息系统及其业务应用的效能、效率、安全性进行监测、评估和控制的过程，以确认预定的业务目标得以实现。
  - 信息安全审计是信息系统审计全过程的组成部分，应用于计算机网络信息安全领域，是对安全控制和事件的审查评价。

作业

- 1. 信息系统生命周期包括哪5个阶段？
- 2.信息资产是什么？怎样分类？责任人有什么责任？
- 3.信息服务的2大流程有哪些内容？
- 4.什么是信息安全事件？什么是安全事件管理？包括什么内容？
- 5.什么是信息系统审计？什么是信息安全审计？包含什么流程？