

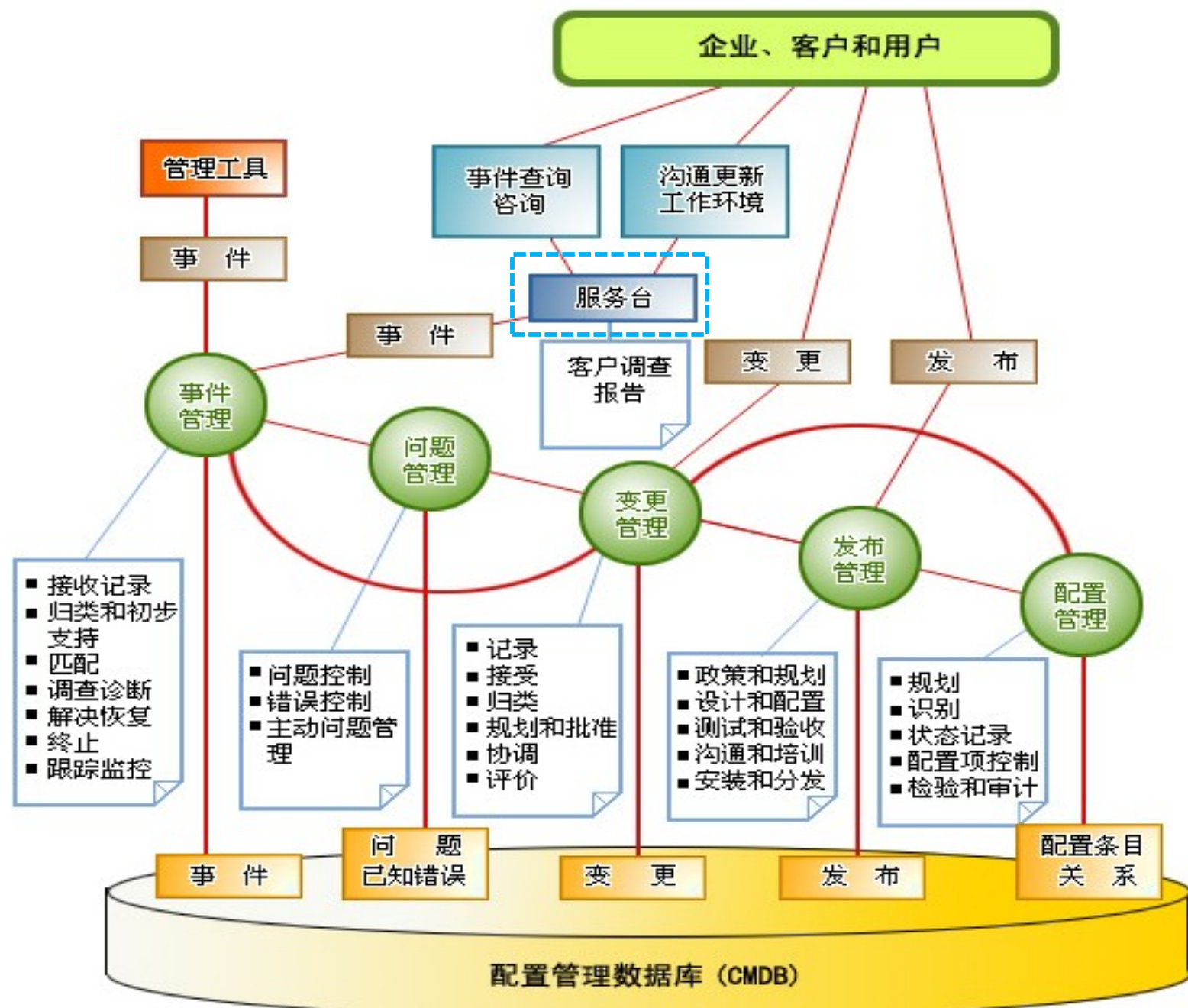
- 1 IT服务管理简介.....●
- 2 IT服务管理流程解析.....●
  - 服务支持
  - 服务交付
- 3 内审知识及审核技巧.....●

➤ 服务支持

- 服务台
- 事件管理
- 问题管理
- 变更管理
- 发布管理

➤ 服务交付

# 服务支持流程关系



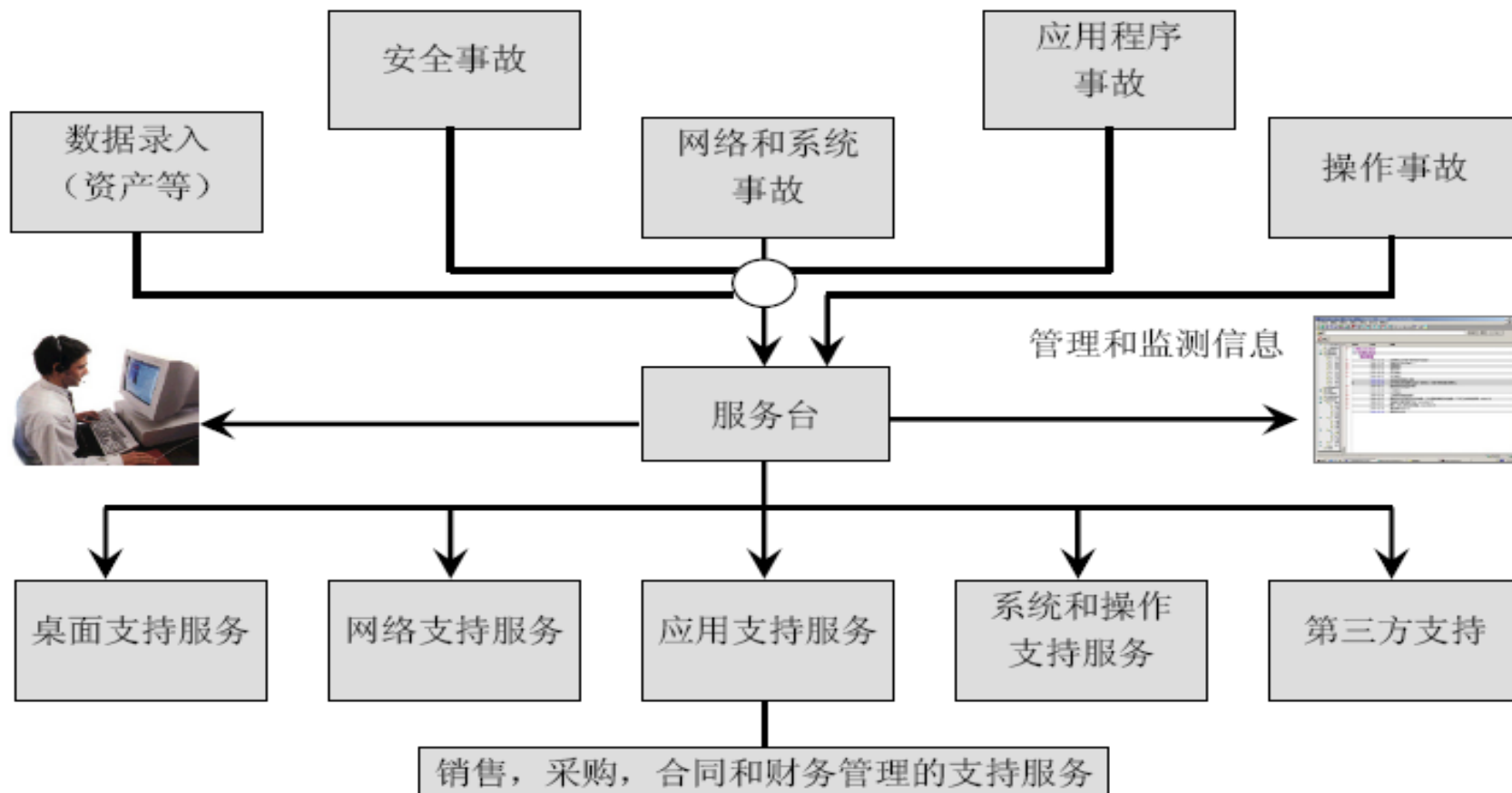


## 定义

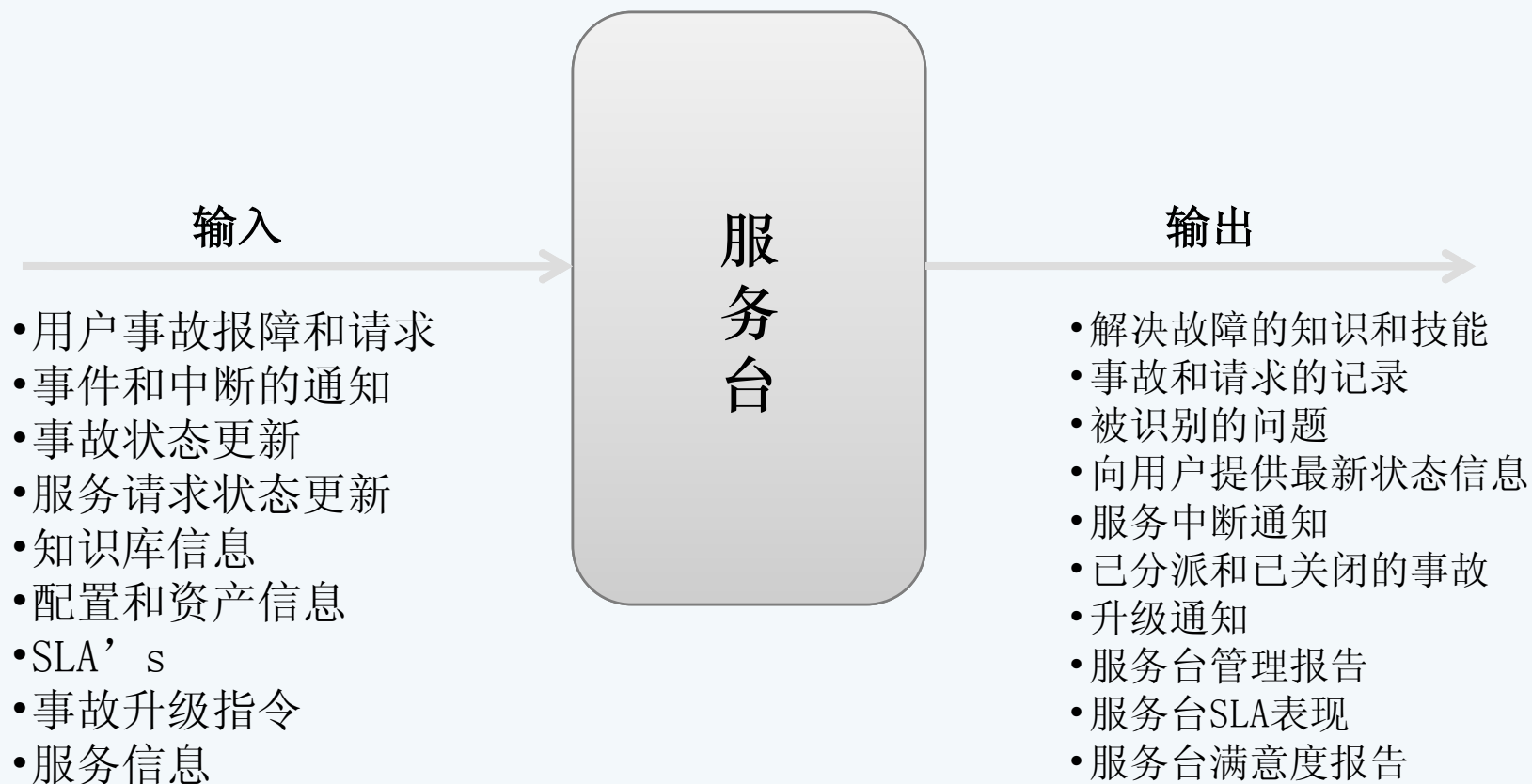
- 报告事件和请求提供用户支持的中心，它主要关注运作层次的用户支持

## 目标

- 为客户和用户提供单一联系点；
- 协调客户（用户）和IT部门之间的关系，为IT服务运作提供支持，从而提高客户的满意度；
- 作为首次联系点，服务台通过截取不相关问题和容易回答的问题减轻了其他IT部门的工作量。







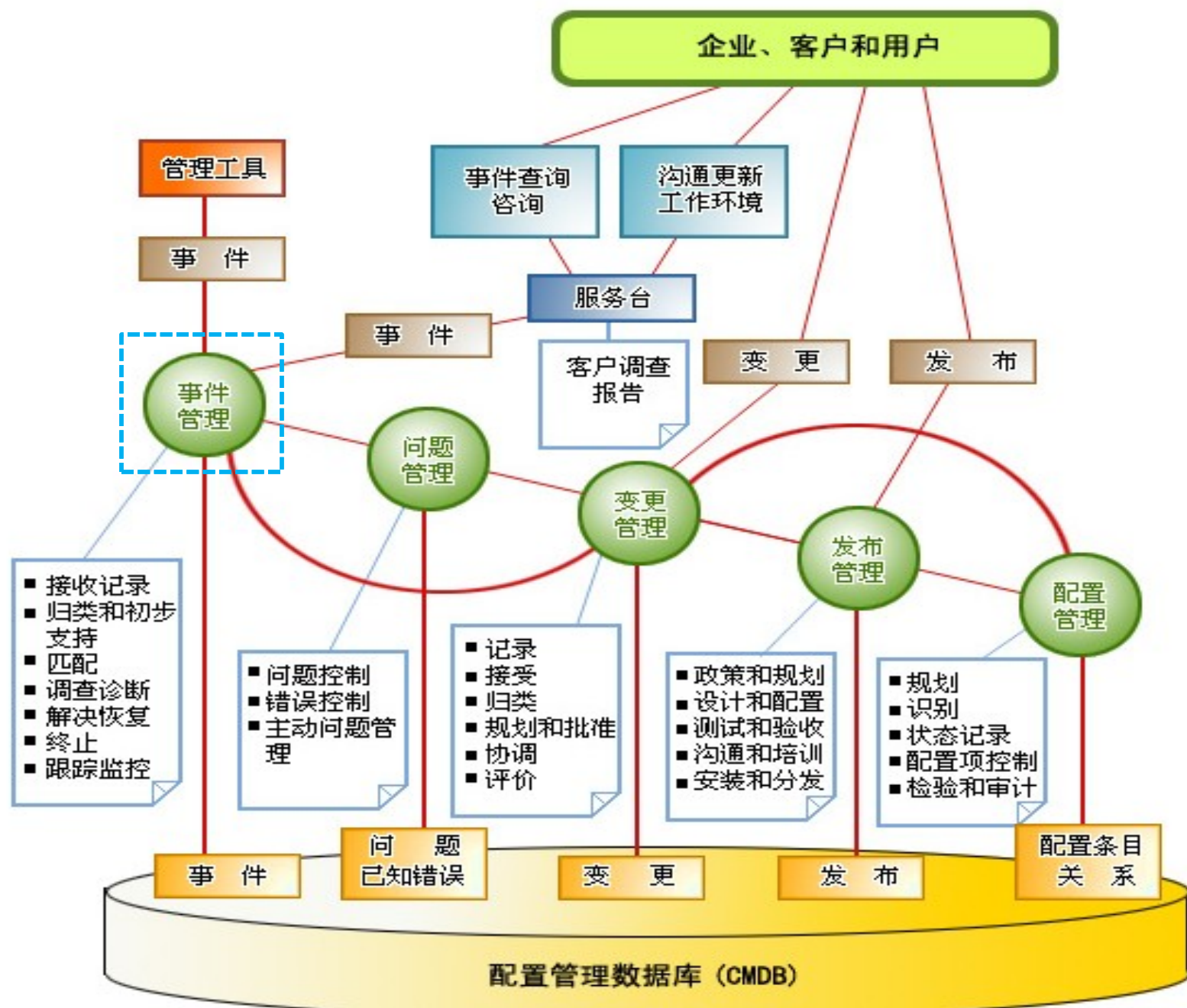
- 集中式服务台 (Centralised Service Desk)
- 本地式 (分布式) 服务台 (Local / Distributed Service Desks)
- 虚拟式服务台 (Virtual Service Desk)

- 平均响应时间
- 达到SLA要求的事故的数量/比例
- 客户满意度
- 成功运用知识库的数量
- 升级和分派的准确性
- 服务台一次解决的呼叫数量/比例



- 服务支持
  - 服务台
  - 事件管理
  - 问题管理
  - 变更管理
  - 发布管理
  - 配置管理
- 服务交付

# 服务支持流程关系



## 定义

- 事件管理是负责记录、归类 and 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的流程。

## 目标

- 事件管理流程的主要目标是根据服务级别协议的要求，在尽可能小地影响客户和用户业务的情况下尽可能快地将服务恢复到“正常状态”。
- 保留事件的有效记录以便能够权衡并改进处理流程，给其他的 service 管理流程提供合适的信息，以及正确报告进展情况。

## 事件

指引起或有可能引起服务中断或服务质量下降的不属于标准操作的事件。  
比如：系统宕机；打印机不工作

## 服务请求

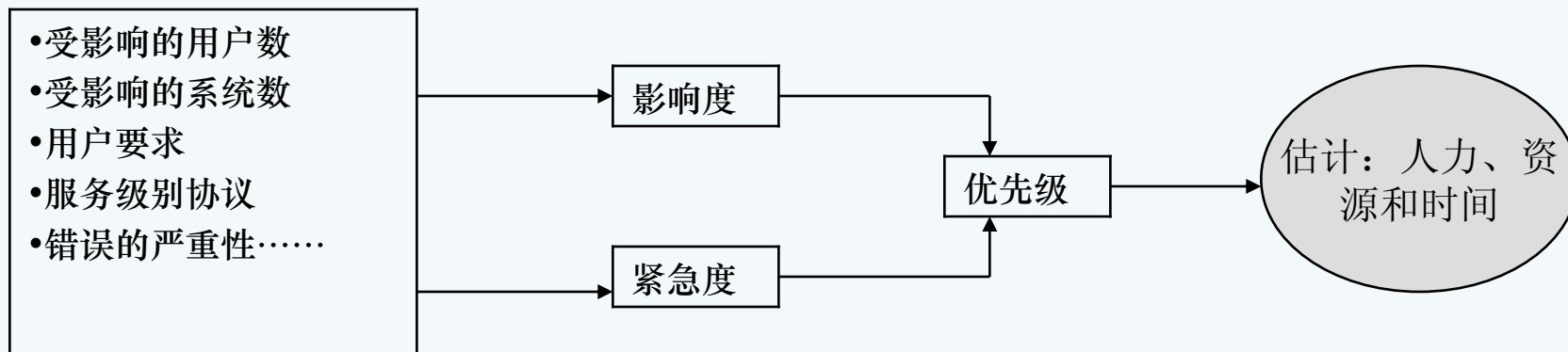
用户想要获得支持、递送、信息、建议或文档的请求，它并不属于基础设施方面的故障  
比如：要求提供文档，提供信息

## 影响度&紧急度

- 影响度——就所影响的用户或业务数量而言，事件偏离正常服务级别的程度。
- 紧急度——解决故障时，对用户或业务来说可接受的耽搁时间。

## 优先级

- 处理事件和问题的先后顺序，他是由影响度和紧急度决定的。





## 影响度

### 紧急度

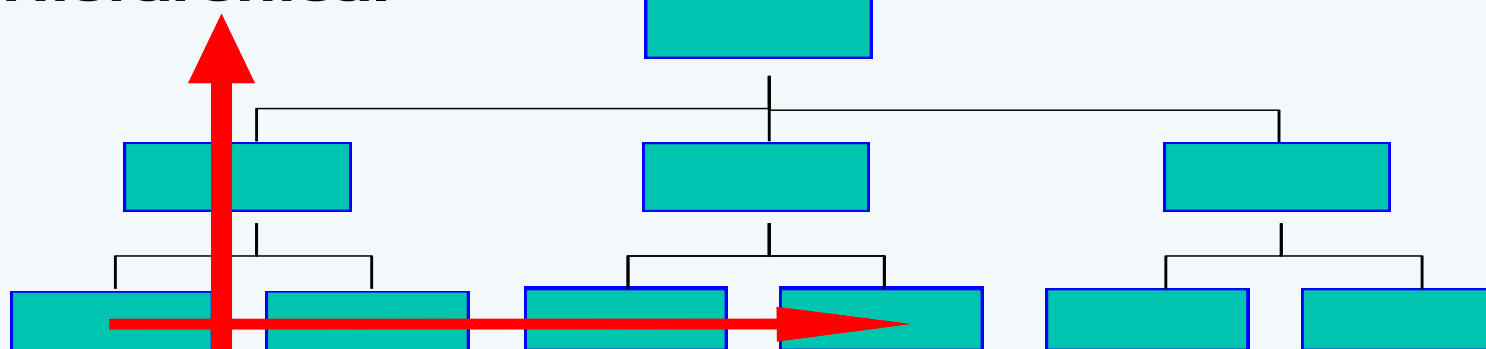
优先级（解决时间）	高	中	低
高	紧急(<1小时)	高(<8小时)	中(<24小时)
中	高(<8小时)	中(<24小时)	低(<48小时)
低	中(<24小时)	低(<48小时)	计划中(已有计划)



## 定义

- 如果某一事件不能在规定的时间内由一线支持小组解决，那么更多的有经验的人员和有更高权限的人员将不得不参与进来，这就是升级。它可能发生在事件解决过程的任何时间和任何支持级别。
- 分类：职能性升级；结构性升级

**Hierarchical**

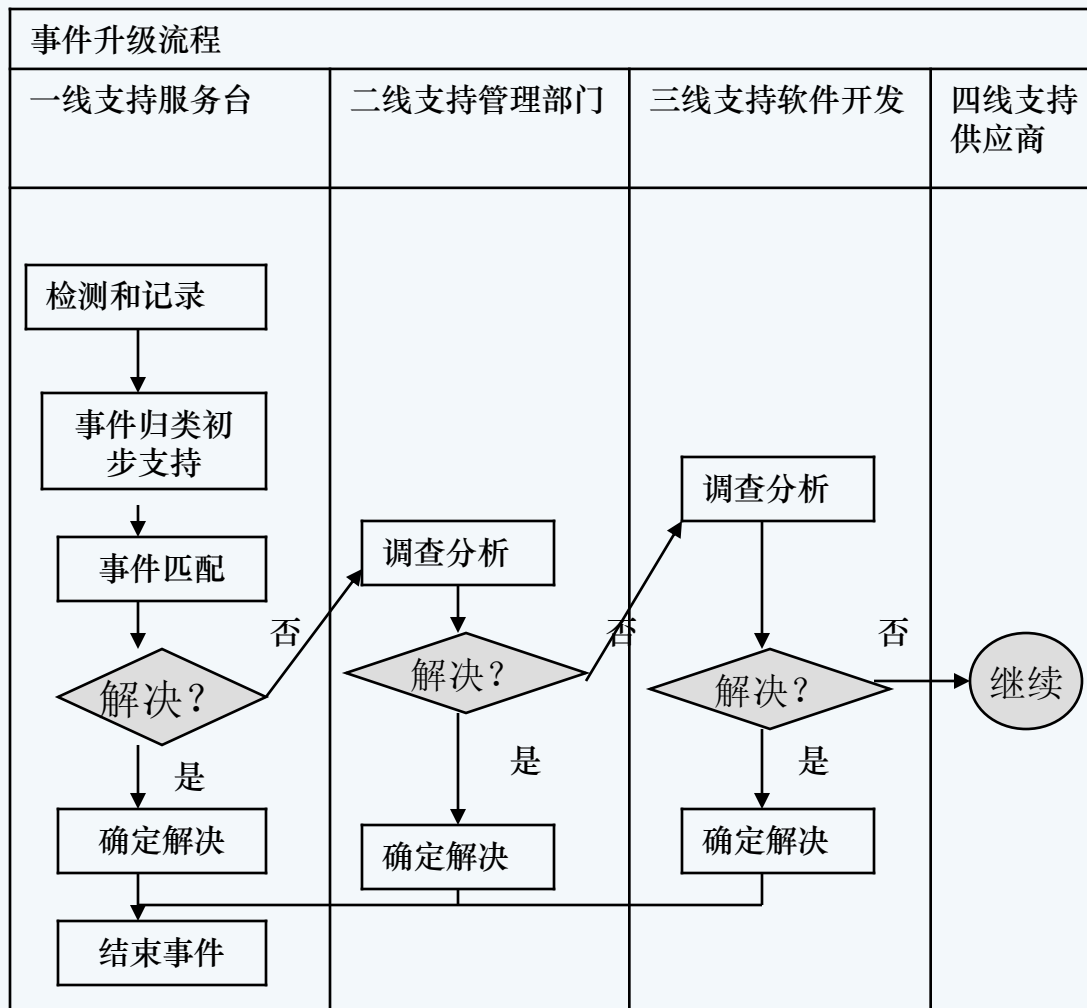


**Functional**

# 概念：一线、二线、N线支持

## 通常设置

- 第1线支持（也称为第1排支持人员）通常由服务台来提供；
- 第2线的支持则由管理部门提供；
- 第3线的支持由软件开发人员和系统结构人员提供；
- 第4线的支持由供应商提供。



# 事件管理——ISO20000的要求

- 应记录所有的事件。
- 应建立程序来管理事件的影响。
- 程序应规定所有事件的记录、优先排序、业务影响、分类、更新、升级、解决和正式关闭。
- 应通知客户，使其了解其报告的事件或服务请求的进展情况，当不能达到约定的服务级别或无法完成约定的措施时应提前告知客户。
- 事件管理所涉及的所有人员应都可以访问相关的信息，如已知错误、问题解决方案和配置管理数据库。
- 应对重大事件进行分类并根据流程进行管理。

## 对整个业务来说

- 更及时地解决事件可减少事件对业务的影响
- 提高用户的工作效率
- 独立的、面向用户的事件监控
- 基于SLA的业务管理信息的可用性

## 对于IT部门来说

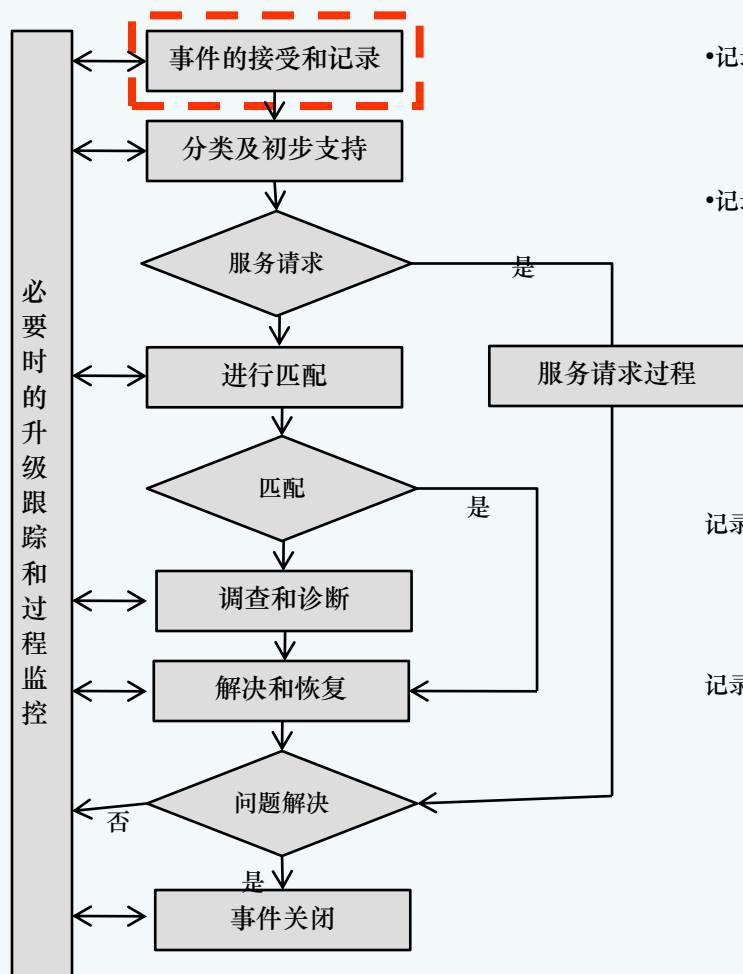
- 改善监控，对于SLA的执行情况可进行更为准确的评测
- 有用的关于服务管理的管理报告和SLA报告
- 更好地和更有效地使用人力
- 避免事件和服务请求的丢失或不正确地记录
- 更准确的配置管理数据库。
- 提高用户和顾客的满意度

## 不实施事件管理的影响

- 由于无人负责监控和升级事件，事件可能无谓地加剧并降低服务的等级，事件得不到解决，用户不断地被迫求助于其他部门
- 专业人员经常会受到用户打来电话的干扰，这意味着他们将不能正常地完成工作。结果是，几个人可能会同时参与到对同一事件的处理工作上，既浪费时间，又可能会得出相互冲突的解决方案
- 与用户和服务相关的管理信息的缺乏



# 流程—事件的接受和记录



## •记录内容（部分）：

- 事件编号（惟一的）；事件类别；
- 记录事件的时间和日期；事件记录人（或组）的姓名（或ID）；
- 有关用户的姓名、部门、电话和工作地点；
- 回复用户的方式（如电话，电子邮件等）；

## •记录方式：

- 分配一个事件索引序号
  - 大多数情况下系统会自动分配一个唯一的事件索引序号。通常，在后续沟通过程中用户可使用通过提供的查询号来查看事件状态。
- 记录基本的诊断信息
  - 时间、症状、用户、处理问题的人、地点以及受影响的服务或硬件等信息；
- 附加事件信息
  - 包括与事件相关的其他信息（例如一个脚本或交谈程序记录）或配置管理数据库中的一些信息（通常以数据库中定义的关系为基础）。
- 警告
  - 如果存在一个具有高影响度的事件，例如某一重要服务器的瘫痪，则应警告其他用户和管理部门。

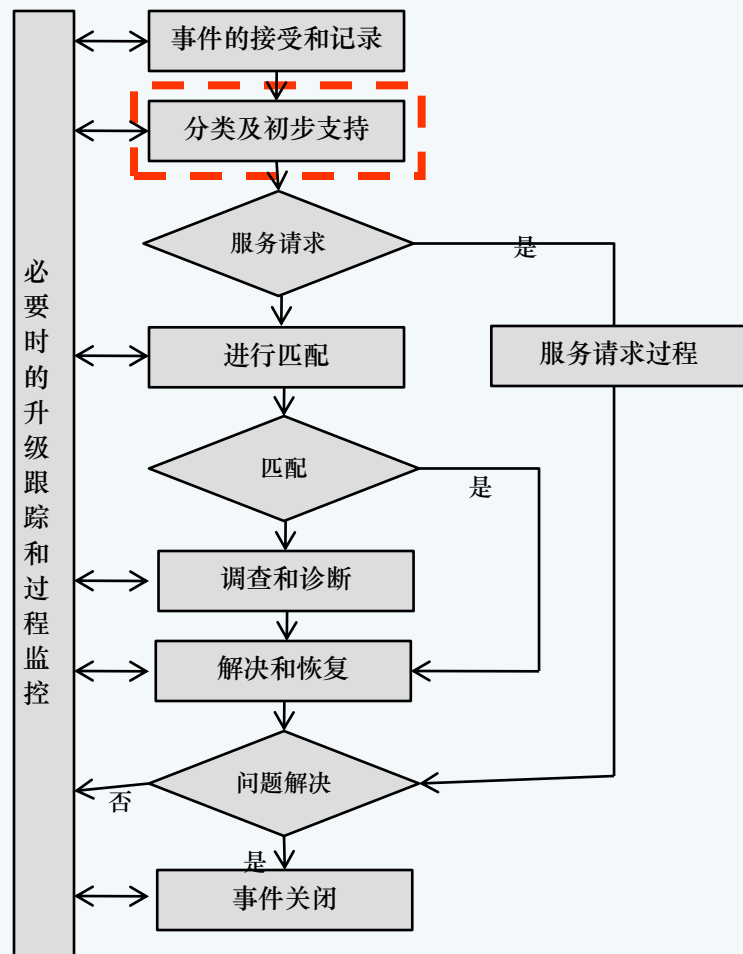
## 记录作用：

已有的事件记录可帮助对新发生的事件进行诊断；  
 问题管理可通过对事件的记录来发现问题原因；  
 如果所有的来电呼叫都被记录下来，那么对某一事件的影响度的判断会容易一些；  
 如果没有事件记录，那么将不能监控经过协商服务级别是否得到履行；  
 避免在解决问题时出现几个人同时解决同样的问题，或在某一事件的处理过程中什么工作都没有做等情形；

## 记录来源：

由某一用户发现  
 由系统发现  
 由某一服务台员发现  
 由另一IT部门的人发现





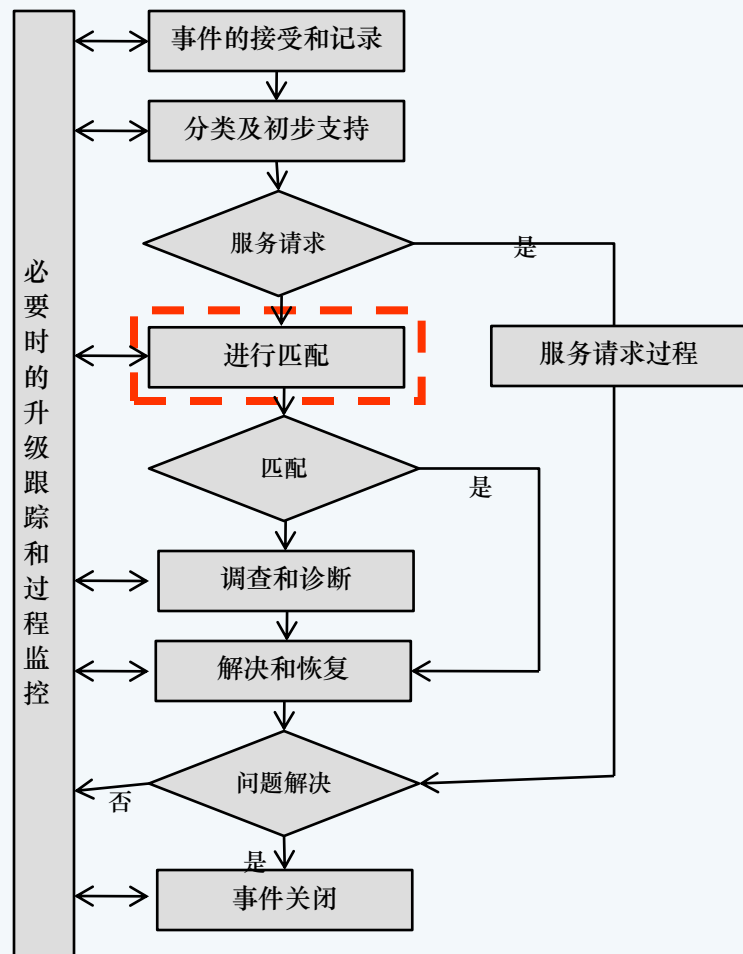
## •类别

- 将事件归入某一类别或某一子类
- 如按事件发生的可能原因分类或按与事件相关的支持小组进行分类。

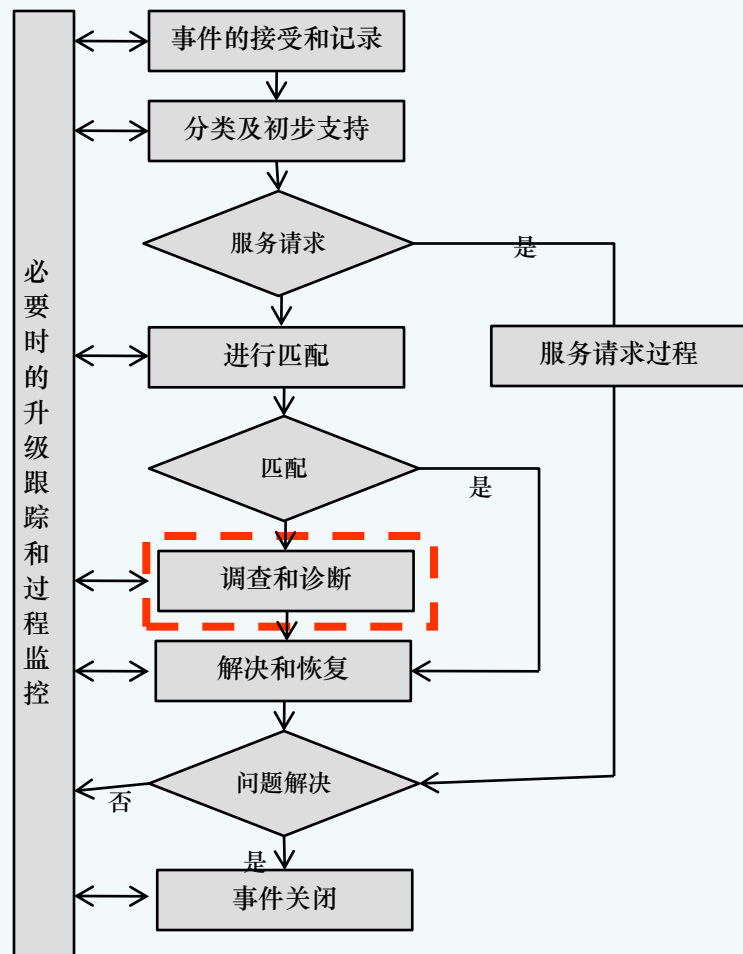
## •优先级 = 影响度 × 紧急度

## •服务

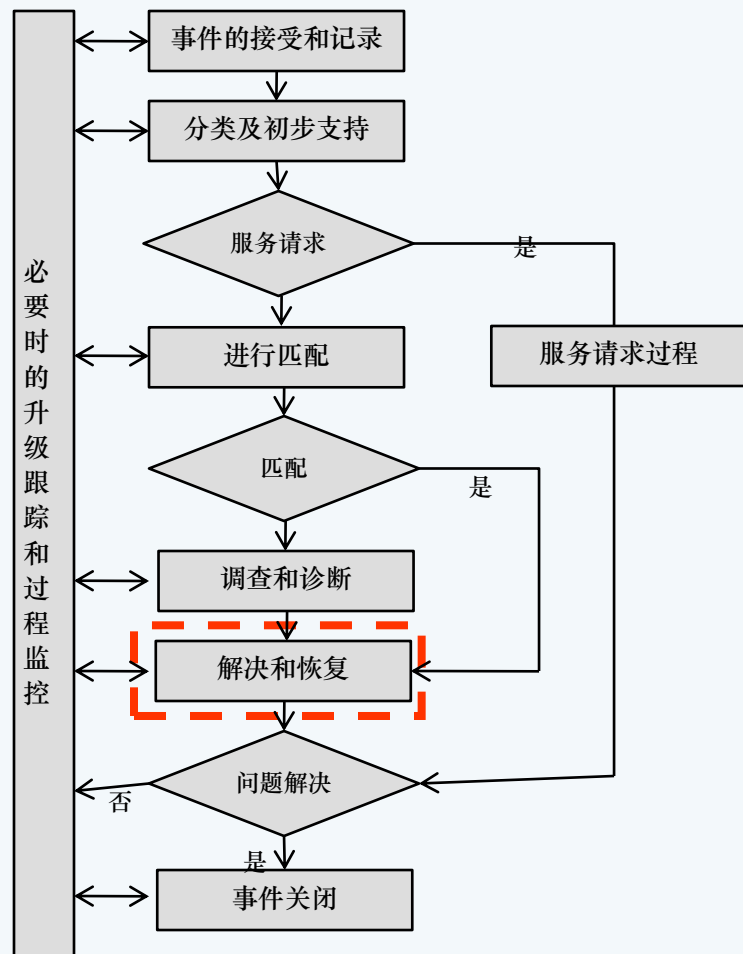
- 按照SLA的有关要求，需要用一個列表来标识与事件相关的服务。
- 这个列表同时也提供了按照SLA对相关服务的升级时间。



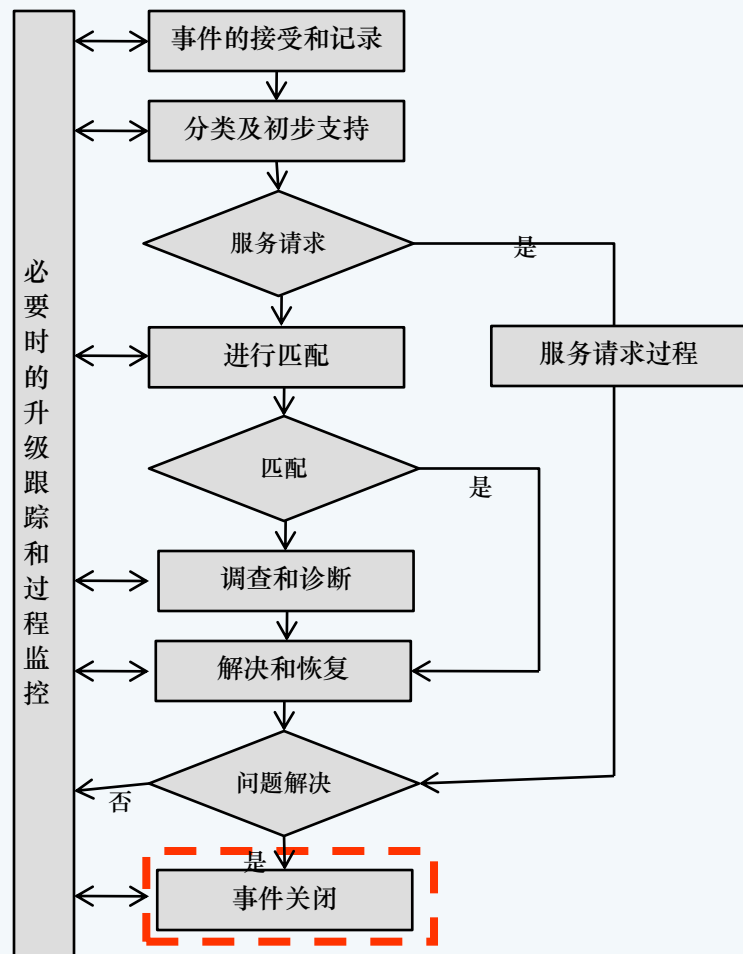
- 对事件进行分类之后，要检查以前是否发生过类似的事件。如果发生过，则查看是否存在解决方案和应急措施。如果新事件与某一问题或某一已知错误具有相同症状，那么可将事件指向这些已知的问题或错误。



- 服务台将那些没有快速解决方法或超过他们专业水平的事件安排给具有更高专业水平和技术能力的支持群体。
- 支持小组将对事件进行调查并尽快加以解决，如不能解决，则将其转交给其他的支持小组。

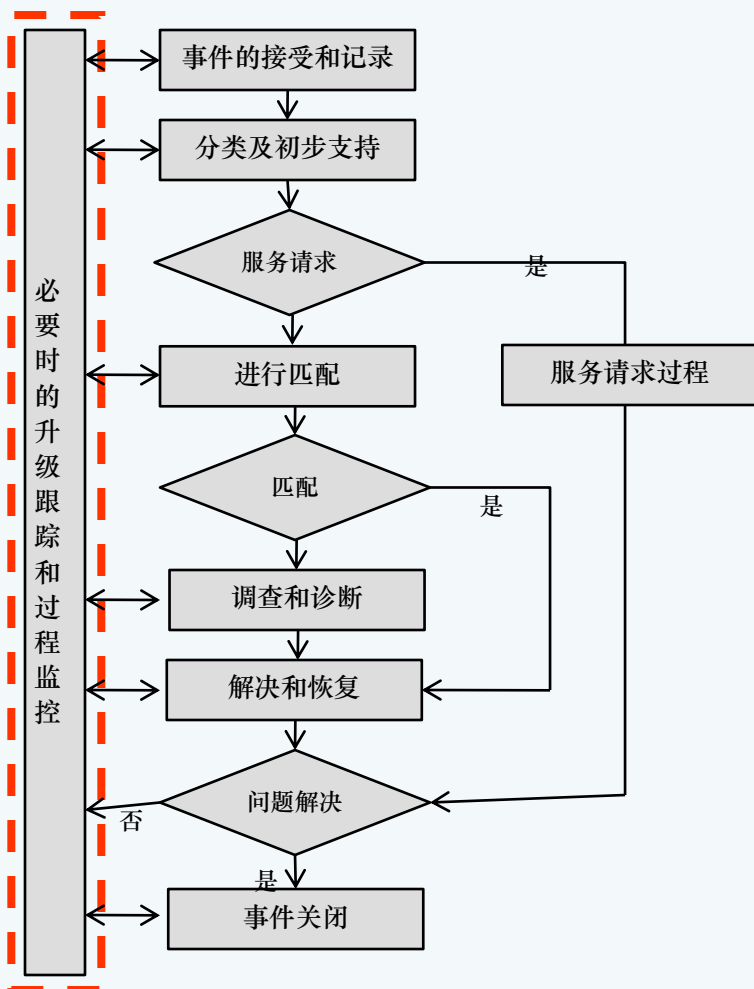


- 成功完成对事件的分析解决之后，负责解决问题的支持小组应在系统中记录故障的解决方法；
- 对某些解决方法来说，必须要向变更管理发送一个变更请求（Request For Change, RFC）
- 如果没有找到解决事件的方法，那么事件依然保持开放（Open）状态。



- 一旦解决方法执行完毕，支持小组要把事件处理情况反馈给服务台。服务台应联系事件的报告人以确认问题的确已经得到解决。
- 如果服务台可以确定问题已经得到很好的解决，那么事件就可以关闭了，否则需要在适当的地方重新开始处理流程。
- 在事件关闭的过程中，必须要对事件的记录进行更新以指明对事件最终的分类和优先级，受影响的服务、用户、客户，以及导致事件发生的配置项等。





- 作为所有事件的拥有者，服务台负责对事件的发展情况进行监控以及通知用户有关事件的状态。
- 用户在某一状态变更后可能作出适当的反馈，如在预期的事件周期内发生的进一步的事件移交安排或变更等。
- 在对事件进展进行跟踪和监控时，可能需要将事件进行职能性升级，转派给其他支持小组来处理，或进行结构性升级，以加强处理事件的力度。





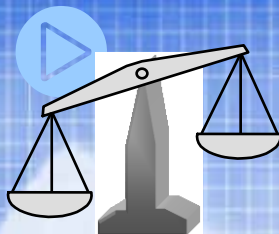
## 支持人员

第一线支持负责记录、分类、匹配、转交、解决和终止事件；其它的支持小组主要参与调查、诊断和恢复工作。



## 事件经理

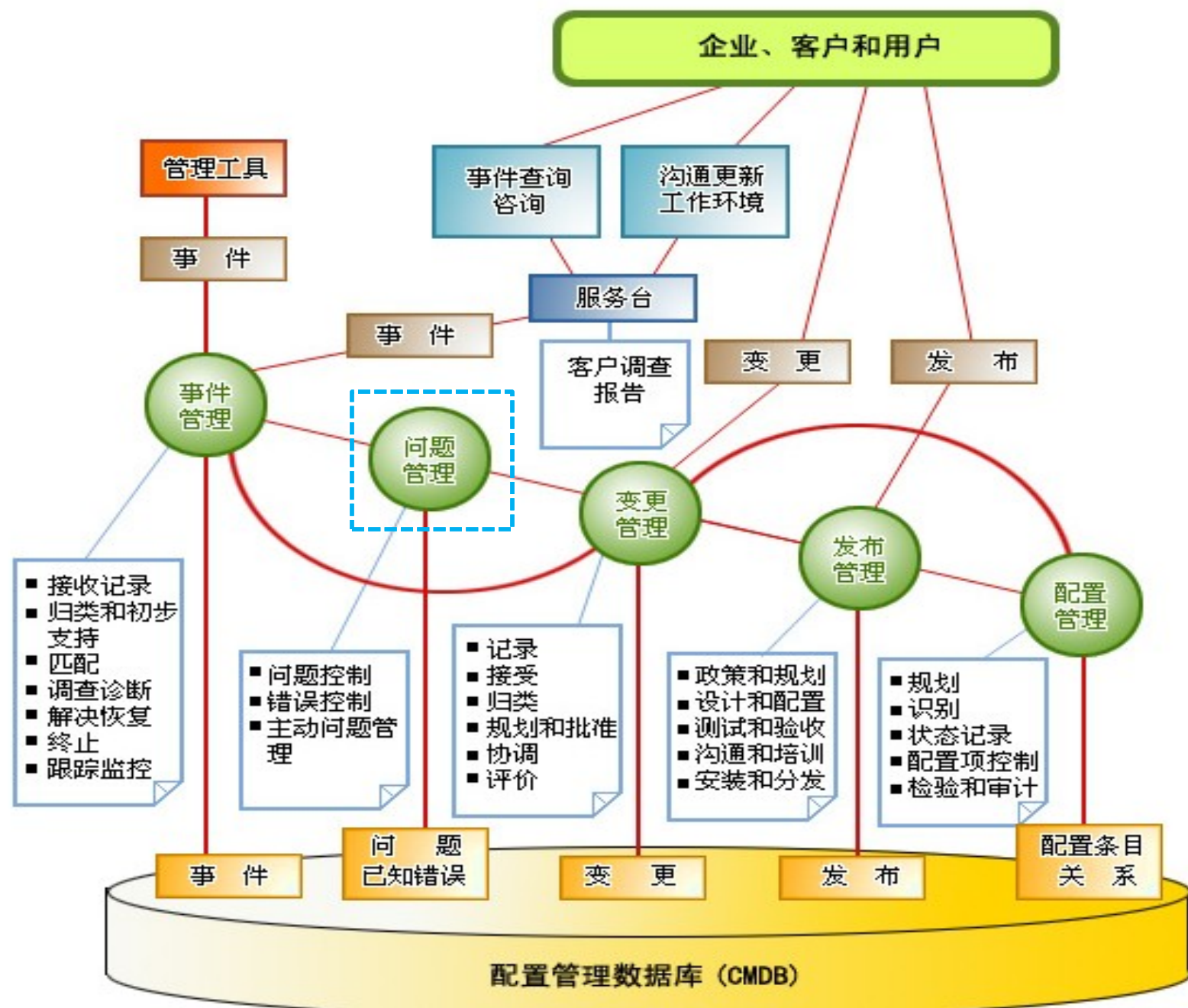
监控处理流程的效果和效率；控制支持小组的工作；为改进工作提供建议；开发并维护事件管理系统；通常指派给服务台经理。



- 事件的总数;
- 平均解决时间;
- 每个事件的平均支持成本;
- 在SLA的目标之内解决的事件数量/百分比;
- 不需拜访用户就解决的事件数/百分比;
- 每个服务台工作站或每个服务台员工平均解决的事件数。

- 服务支持
  - 服务台
  - 事件管理
  - **问题管理**
  - 变更管理
  - 发布管理
  - 配置管理
- 服务交付

# 服务支持流程关系



## 定义

- 通过调查和分析IT基础架构的薄弱环节、查明事件产生的潜在原因并制定解决事件的方案和防止事件再次发生的措施，将由于问题和事件对业务的负面影响减小到最低的服务服务管理流程。

## 目标

- 将由IT基础架构中的错误引起的事件和问题对业务的影响减少到最低程度；
- 查明事件或问题产生的根本原因，制定解决方案和IT事件再次发生的预防措施；
- 实施主动问题管理，在事件发生之前发现和解决可能导致事件产生的问题



# 概念：问题 | 已知错误 | 变更请求





# 概念：问题 | 已知错误 | 变更请求 - 例子



## 已知错误

- 一个已经确定产生根源的问题。这些错误已被确认了一个临时或永久性的解决方案。

## 临时措施

- 是为解决事件的临时性的替代方法或技术。它被用来消除用户对某种已知有问题服务的依赖性。使用临时措施后，用户可以继续使用服务而不会被中断。
  - 例：病毒专杀工具

## 被动问题管理

- 确认事件的根本原因。根据这些原因提出永久性解决方案防止事件再次发生。

## 主动问题管理

- 活动目的是在事件发生之前阻止它们发生。此活动协助鉴别IT基础设施中的缺陷并提出消除这些缺陷的方法。

# 概念：事件管理VS问题管理

	事件管理	问题管理
主要目的		
实施方法		
关注重点		
花费时间		

# 概念：事件管理VS问题管理

	事件管理	问题管理
主要目的	恢复服务	查明根源
实施方法	应急措施	永久方案
关注重点	速度	质量
花费时间	短	长



# 问题管理——ISO20000的要求

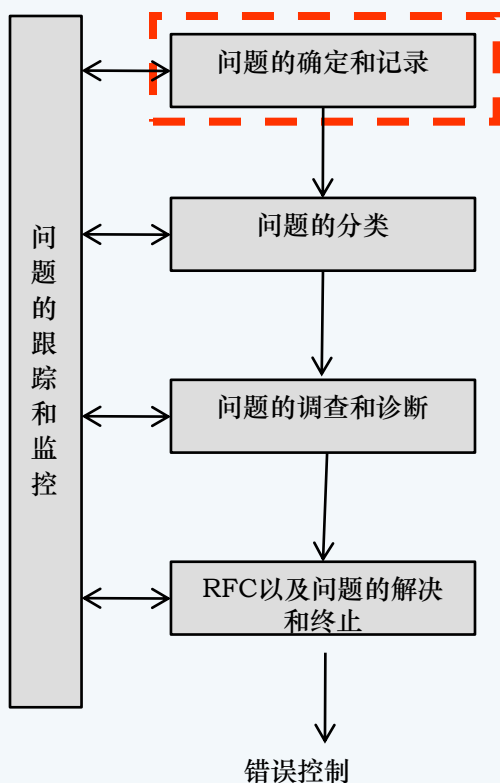
- 应记录识别的所有问题。
- 应建立程序以识别、最小化或避免事故或问题的影响。程序应规定所有问题的记录、分类、更新、调整、解决和关闭。
- 应采取预防措施，以减少潜在的问题，如事故数量和类型的趋势分析之后的后续活动。
- 纠正问题的根本原因所需的变更应提交变更管理流程。
- 应监视、评审问题的解决并报告其有效性。
- 问题管理者有责任确保事故管理者可获得关于已知错误和已纠正问题的最新信息。
- 应记录在这一流程中确定的改进措施，并作为服务改进计划的输入。

# 实施问题管理的好处

- 提高IT服务质量
  - 记录和消除错误
  - 降低事件的数量
  - 为IT基础设施的问题提供永久性解决方案
- 更高的一线解决：
  - 通过获取事件解决方案和临时措施信息，提高一线对事件的首次解决率

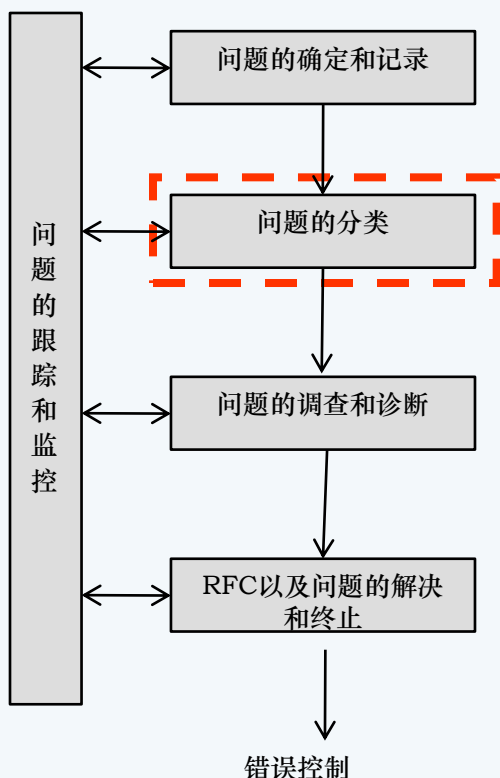
**问题管理流程可以不断改善服务，让服务达到协定的质量标准**

- 问题控制：定义、调查以及诊断；问题控制注重将问题转化为已知错误
- 错误控制：监控并控制已知错误，提出变更请求；错误控制注重于通过变更管理流程在结构上解决已知错误
- 主动性问题管理：通过改进基础设施以及提出变更请求来阻止可避免事件的发生
- 提供信息：对结果和重要问题的报告



## •如何确定问题？举例：

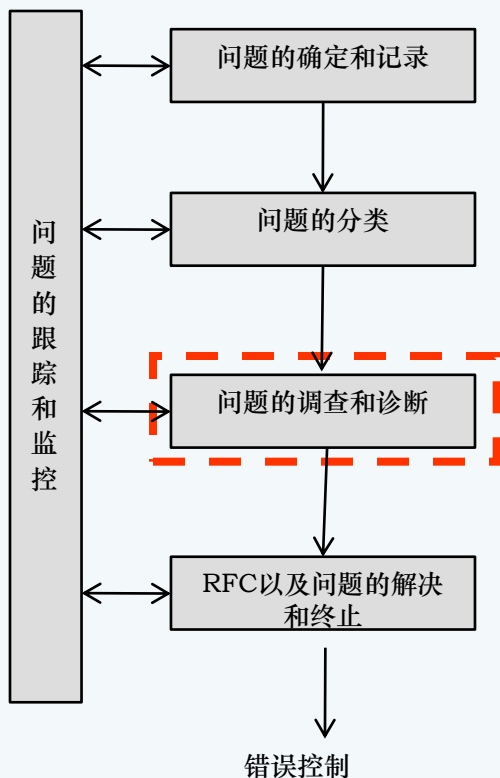
- 对某一事件进行分析表明该事件可能再次发生，或者有大量发生并且加重的趋势。
- 对基础架构进行分析可以找出可能会产生事件的薄弱环节(也可由可用性管理和能力管理来进行分析)；
- 服务级别可能会受到威胁(能力、性能、成本等)
- 记录下来的事件不能与一个现有的问题或已知错误发生关联。



## •如何归类？

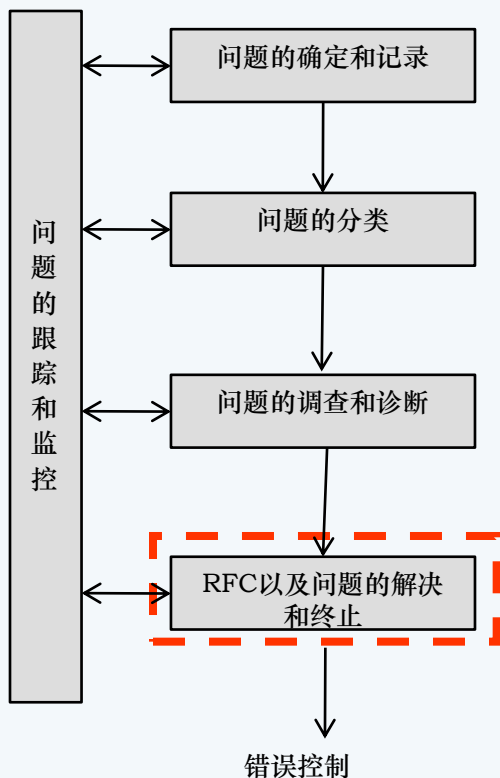
- 类别：确定问题的相关领域，如是硬件还是软件问题；
- 影响度-主要指对业务流程的影响
- 紧急度-也包含多长时间的延期是可接受的；
- 优先级-紧急度、影响度、风险和所需资源的综合考虑。
- 状态-如问题、已知错误、已解决、已关闭但正在进行实施后评审等。



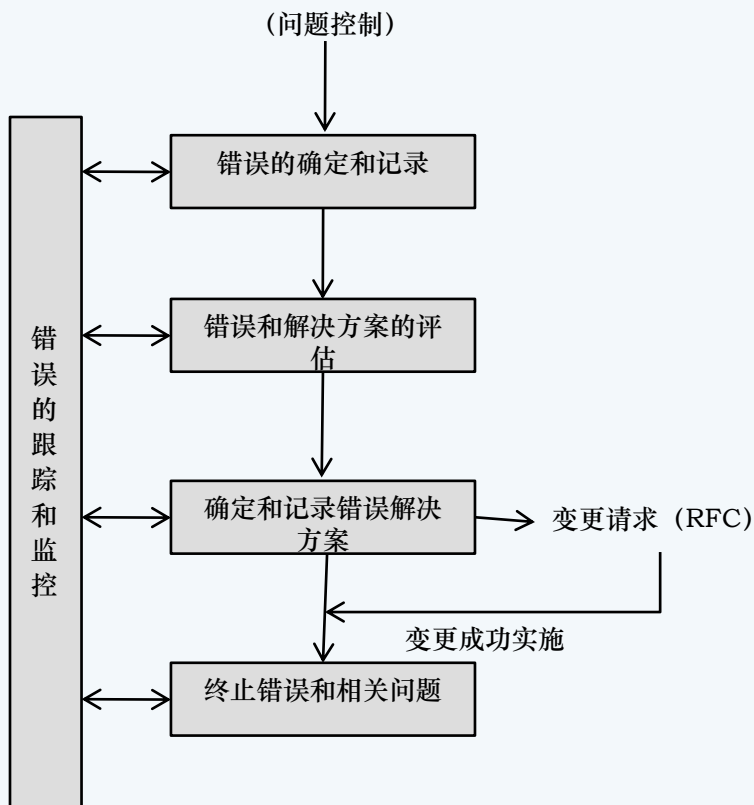


## 调查和诊断

一旦找到问题的根源以及与此问题相关的一个或多个配置项，就可建立配置项和相应事件之间的关联：  
之后如果找到了解决此问题的应急措施，此问题就转变为已知错误。



在解决问题的过程中，如果问题导致了严重的事件，那么找到一个临时修复或紧急修复的方法是非常必要的。但是如果临时修复措施需要对基础架构进行一些改动，那么必须首先提交变更请求(RFC) (这主要是指在找到问题的最终原因之前)。如果特别严重而且不容耽搁，就必须启动紧急变更请求处理程序。



**错误确定和记录：**如果找到错误的根源和与此错误相关的配置，问题转变为已知错误描述。然后开始错误控制

**错误评估和解决方案评估：**根据服务级别协议、处理事件和已知错误所需成本和所可能获得的收益、变更请求的影响度和紧急度等因素来比较不同的解决方案

**确定和记录解决方案：**确定对问题最合适的解决方案，包括确定是需要临时性修复还是永久性解决方案，或者两者都需要。也可能决定不修复此问题，比如考虑到这样做从业务上来看并不划算。

**跟踪和监控：**负责在问题和已知错误的整个生命周期内对其发展情况进行监控

## 目的:

- 是在事件发生之前阻止它们发生。此活动协助鉴别IT基础设施中的缺陷并提出消除这些缺陷的方法。

## 描述:

- 根据对IT基础架构进行的分析，问题管理可以找到可能出现问题的薄弱环节，在事件发生前发现和解决有关问题和已知错误，以尽量减少问题和已知错误对业务的影响。

## 趋势分析:

- 找出IT基础架构中不稳定的组件，分析其原因，以便采取措施降低配置项故障对业务的影响；
- 分析已发生的事件和问题，研究其变化趋势；
- 通过其它方式和途径分析，比如系统管理工具、用户反馈等。

## 制定预防措施:

- 提交变更请求(RFC)；
- 提交有关测试、规程、培训和文档方面的反馈信息；
- 进行客户教育和培训；
- 对服务支持人员进行教育和培训；
- 确保遵守问题管理和事件管理的规程；
- 改进相关的流程和程序。

一些与应急措施和临时修复相关的信息会提供给事件管理流程。这样，服务台可以通过任何受到影响的用户。





## 支持人员

### 被动性职责：

- ✓通过分析事件细节确定并记录问题；
- ✓以问题的优先级为基础对其进行调查和管理；
- ✓提出RFC
- ✓监控已知错误的进展情况；
- ✓为事件管理的应急措施和暂时修复提供建议；
- ✓实行重大问题评审。

### 主动性职责：

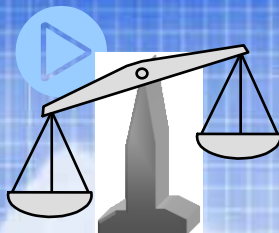
- ✓确认问题的发展趋势；
- ✓提出RFC
- ✓防止问题扩散到其他系统；



## 问题经理

- ✓开发并维护问题控制和错误控制流程；
- ✓帮助提高问题控制和错误控制的效率和效用。
- ✓提供管理信息并运用这些信息主动预防事件和问题的发生；
- ✓对问题管理人员进行管理；
- ✓获取问题管理行为所需的资源；
- ✓开发并改进问题控制和错误控制系统；
- ✓对主动性问题管理的有效性进行分析和评价。

问题管理的难点在哪里？为什么？



- 通过管理和解决问题，使事件的数量减少；
- 解决问题所需的时间减少；
- 与解决故障相关的成本降低。
- 已关闭的问题数量
- 通过“已知错误”解决的事故数量
- 问题管理提出的RFC数量
- 关闭一个问题的平均数量
- 错过目标解决时间的问题数量
- 客户满意度
- 解决一个问题的成本
- 用户宕机总时长

## 例题

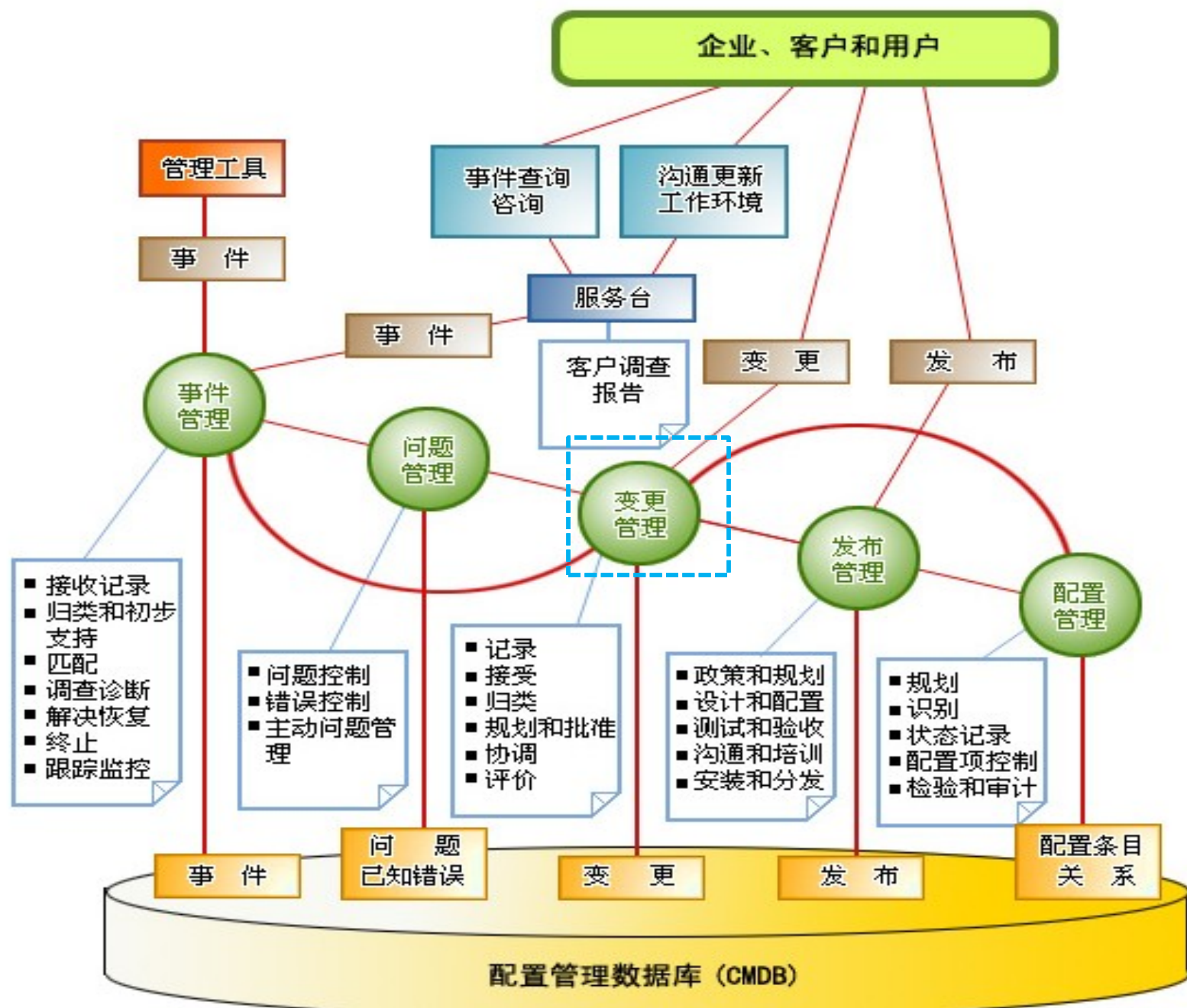
- 1) 你是某个 IT 组织中的服务台人员。有一个用户呼叫电话说它的某个终端设备不能使用了。请问这是一个？
  - A. 事件
  - B. 已知错误
  - C. 问题
  - D. 变更请求
- 2) 一个良好的事件管理流程将可以：
  - A. 确保错误的修改像处理紧急变更一样进行处理
  - B. 快速地诊断事件发生的潜在原因
  - C. 在事件发生后尽快地恢复正常的服务运作
  - D. 以上三项都是
- 3) 下列哪项活动属于事件管理的职责？
  - A. 变更在基础架构中的应用
  - B. 检测事件产生的原因
  - C. 识别事件背后的潜在问题
  - D. 事件的排除

- 1) “已知错误 (Known Error)” 与 “问题” 在 ISO20000 中的不同之处表现在哪些方面？
  - A. 导致已知错误的潜在原因是已知的，而导致问题的潜在原因是未知的
  - B. 已知错误与 IT 基础架构中出现的错误有关，而问题则与其无关
  - C. 已知错误通常某个事件，而问题则不完全是这样的
  - D. 对问题而言，与其有关的配置项已经发现和确认，而与已知错误有关的配置项通常仍未发现
- 2) 以下哪项活动属于主动问题管理？
  - A. 处理变更请求 (RFC)
  - B. 进行趋势分析，发现潜在的事件的问题
  - C. 跟踪所有的事件和服务中断
  - D. 尽量减少由于 IT 环境的变更而造成的服务中断
- 3) 当导致某个问题产生的原因发现后，此问题的状态转变以下哪种？
  - A. 事件
  - B. 已知错误
  - C. 已解决的
  - D. 变更请求



- 服务支持
  - 服务台
  - 事件管理
  - 问题管理
  - **变更管理**
  - 发布管理
  - 配置管理
- 服务交付

# 服务支持流程关系



## 定义

- 为在最短的中断时间内完成基础构架或服务的任一方面的变更，并对其进行控制的服务管理流程。
- 对基础设施进行改变

## 目标

- 确保标准方法和过程可以得到使用，因而变更可以很快地、对服务质量可能影响最小地得以处理。
- 所有的变更都必须可跟踪，换句话说，可以很容易地回答“什么变更了？”这样的问题。

### 范围

- 变更管理流程的范围仅仅包含IT基础设施的变更。
- 变更管理的范围局限于支持IT基础设施运营的相关硬件、软件、通讯设备、文档和规程的变更。
- 应用系统开发、组件选择以及已变更或新的组件版本的发布超出了变更管理流程的范围。

## 变更请求(RFC)

---

- 对一个或多个特定配置项实施变更的正式请求；
- 说明了变更的内容及与变更有关的配置项；
- 包括标准变更和非标准变更两种；
- RFC可以是书面文档或电子文档。

## 标准变更

---

- 变更已经得到全面的定义和批准，属于日常变更，不需要变更管理流程进行单独评估。
- 例如：新建用户帐号、安装PC、更新防病毒软件等。

## 非标准变更

---

- 被管理的基础设施所进行的其他改变。
- 这里的“其他”，相对于标准变更。



## 紧急变更

- 具有绝对优先级的变更，这种变更很重要，必须尽可能地执行。

## 说明

- 在紧急变更发生之前可能没有足够的时间做正常的测试，但是之后，正常流程所有必需的步骤都必须完成以保证任何以前跳过的测试现在都被执行，并且文档(变更记录和CMDB)也得到了更新，以保证“什么变更了”是可记录的。
- 在需要执行紧急变更的情况下，如果有时间，变更经理可以组织一次CAB的紧急会议。这种会议仅有特定的成员需要对其评价，授权，为其分配资源。如果没有时间或者请求发生在工作时间之外，就必须有获取授权的其他方法。
- 紧急变更具有破坏性，且容易失败。
- 紧急变更的数量要尽可能少。

# 概念：变更顾问委员会(CAB)

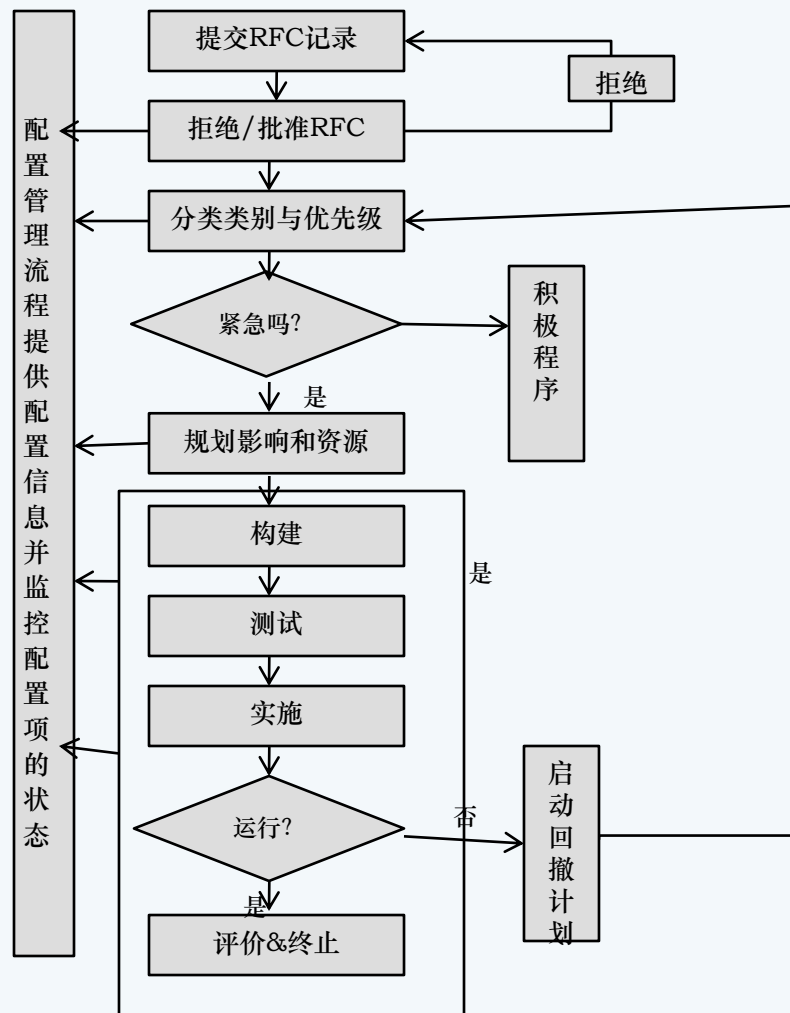
## 定义

- 变更顾问委员会（CAB）是变更的审批机构，对变更进行评估和对变更请求进行优先级排序后批准变更。
- 为确保所有的变更请求被充分的评估，CAB成员应具备全面的技术知识和优秀的业务远景思维。另外，CAB成员应该全面理解客户和用户的需求。

# 变更管理——ISO20000的要求

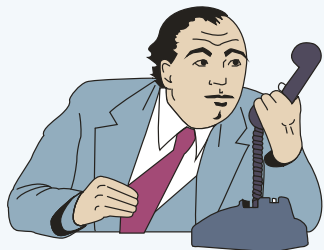
- 应清楚定义服务和基础设施变更的范围，并形成文件。
- 应记录并分类所有要求的变更，如紧迫、紧急、重大和轻微等。应评估变更请求的风险、影响和业务收益。
- 变更管理流程应包括恢复和补救失败变更的方法。
- 应批准并检查更新，并以受控的方式实施。
- 应评审所有变更以确保成功以及实施后所采取的措施。
- 应建立策略和程序，以控制紧急变更的授权和实施。
- 计划的变更日程应作为制定变更和发布时间表的基础。时间表应包括批准实施的所有变更以及建议实施日期的详细信息。应保持时间表并与相关方沟通。
- 应定期分析变更记录，以检测日益增多的变更级别、频繁发生的类型、出现的趋势以及其他相关信息。应记录变更分析所得出的结果和结论。
- 应记录有变更管理所确定的改进措施，并作为服务改进计划的输入。

大多数组织将注意力集中在产品和流程的持续改进上。然而，改进预示着变更，相应地带来一定的风险。为了控制风险，我们需要按照标准流程系统化地执行变更。



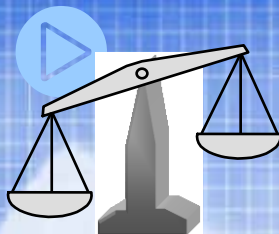
- **记录：** 确保所有的变更资源可以提供给变更请求，并且它们被完整地记录下来。
- **审查：** 过滤变更请求，对其进行验证以备进一步考虑。
- **归类：** 按照类别和优先级对RFC进行分类。
- **规划和批准：** 批准变更；规划和批准开发和实现的过程；确保要求的资源可用；必要时提交CAB。
- **协调：** 协调变更的构建、测试和实施过程。
- **评价：** 判定每个变更是否成功并从中汲取教训以便改进该流程





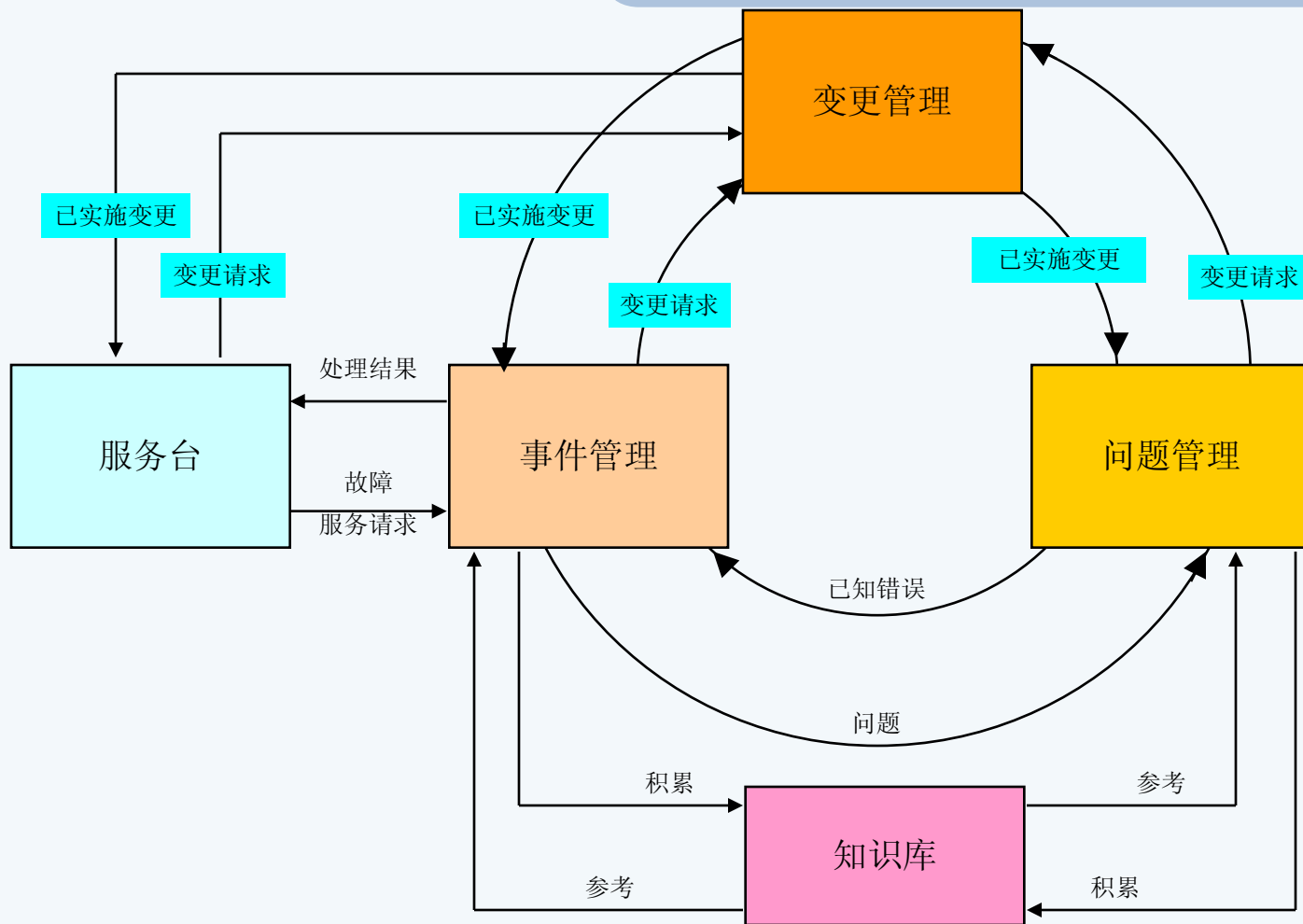
## 变更经理

- 筛选、接受和分类所有的变更请求
- 为所有紧急变更请求和变更请求召开CAB会议
- 为变更获得所需的授权
- 通过服务台发布实施进度表
- 计划和协调变更的实施
- 提交规范、准确的变更报告
- 评审所有已实施的变更，确保达到预期目标



- 每一类变更的数目
- 变更实施的速度
- 引发变更的事件的数目
- 与变更相关的备份数目
- 有资源和时间估计的变更数目
- 失败变更的百分比
- 被拒绝的变更请求的百分比
- 未授权变更数量
- 变更积压数量
- 客户满意度
- 紧急变更数量/百分比
- 未交付预期结果的变更数量/百分比

# 事件管理、问题管理和变更管理之间的关系

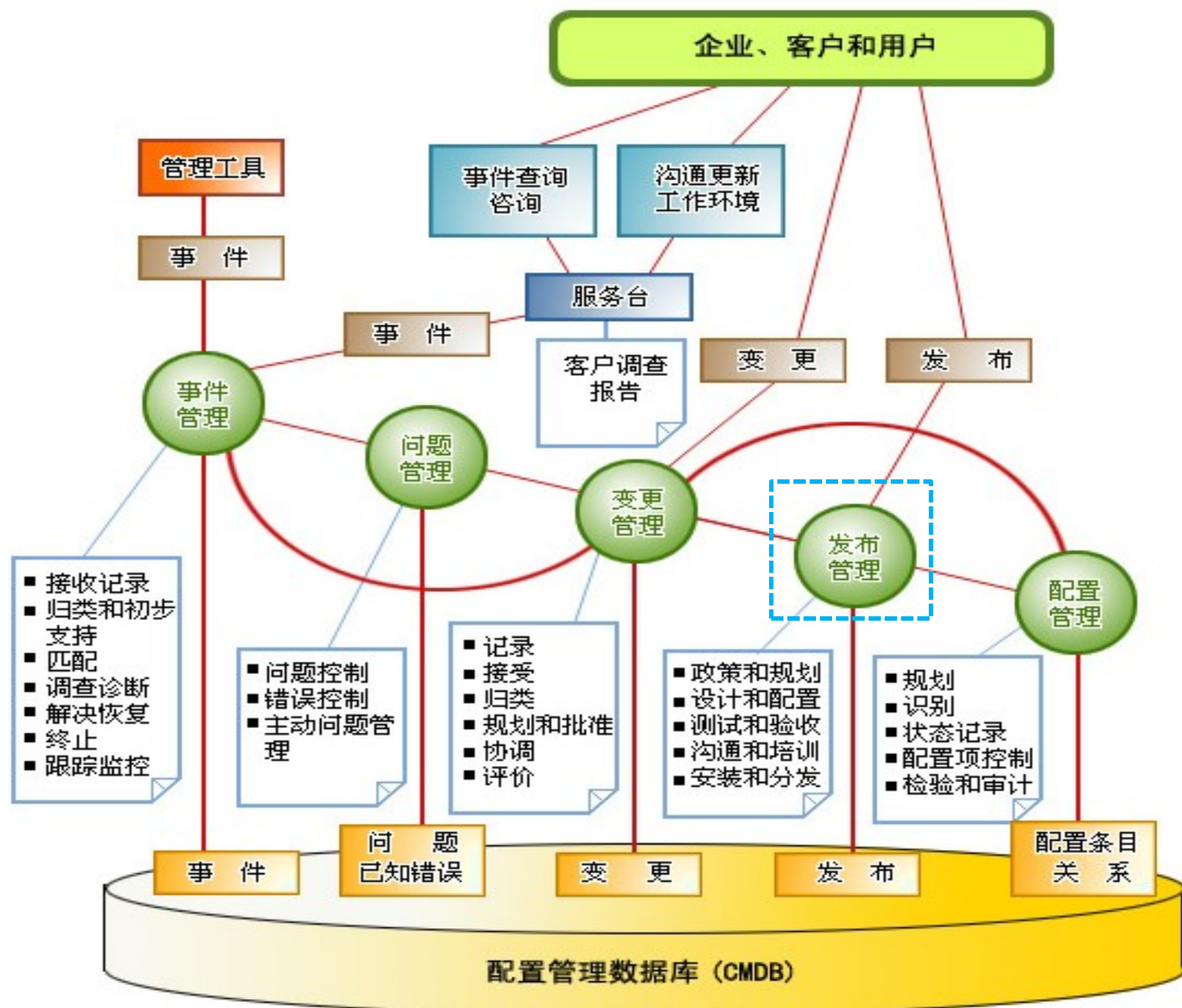


- 1) 当某个软件包的最新版本被安装到某个台式机时，它可能会影响其它软件包。哪个流程负责检查和判断其它软件包是否有必要测试或者重新安装？  
A. 变更管理  
B. IT 服务持续性管理  
C. 问题管理  
D. 发布管理
- 2) 哪个 IT 服务管理流程负责检查变更请求 (RFC) 的合理性、可行性和必要性？  
A. 变更管理  
B. 事件管理  
C. 问题管理  
D. 配置管理
- 3) 以下哪项变更必须经变更管理流程批准后才能实施？  
A. 用户录入数据到数据库中  
B. 改变密码  
C. 给系统增加一位新用户  
D. 将打印机从二楼移到三楼

- 服务支持
  - 服务台
  - 事件管理
  - 问题管理
  - 变更管理
  - **发布管理**
  - 配置管理
- 服务交付



# 服务支持流程关系



## 定义

- 对经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；
- 以前称为软件控制与分发，由变更管理流程控制。

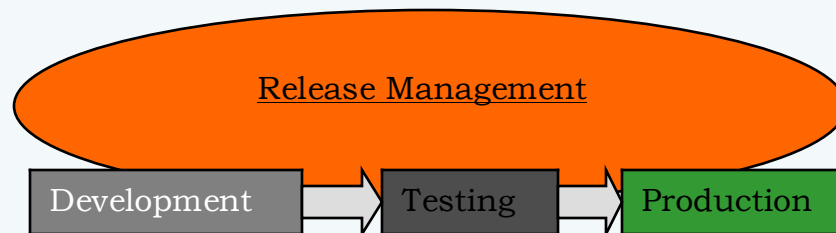
## 目标

- 计划和协调软硬件组件的发布；
- 设计和实施有效的程序来分发和安装IT系统的变更；
- 确保只有正确的、被授权的和经过测试的软硬件版本才能导入实际运作环境；
- 确认所有最终软件库中软件正本的拷贝是安全可靠的，并且在配置管理数据库中得到了更新

## 概念：发布管理(续)

- 范围：

- 负责对软件和硬件进行规划、设计、构建、配置和测试，以便为实际运行环境提供一系列的发布组件。
- 需要发布管理进行控制的组件：
  - 自行开发的应用程序；
  - 外购软件；
  - 工具软件；
  - 供应商提供的系统软件；
  - 硬件和软件的规格说明；
  - 装配指南和文档，包括用户手册。
- 发布管理执行的常见情形：
  - 重大或关键硬件的首次运行，特别是当业务系统对某个相关的软件变更具有较大依赖的情形；
  - 主要软件的首次运行，特别是新的应用程序与其协同软件同时发布的情形；
  - 将一组相关的变更打包成一个个适当规模的单元的单元的情形。



## 概念：发布管理VS变更管理

发布管理	变更管理
关注变更的实施，以及与变更有关的风险	整个变更流程
发布管理是从变更管理中独立出来的	
主要涉及软件方面	IT基础设施的变更
一组变更	单个变更
生产环境的质量	标准的方法和过程可以得到使用

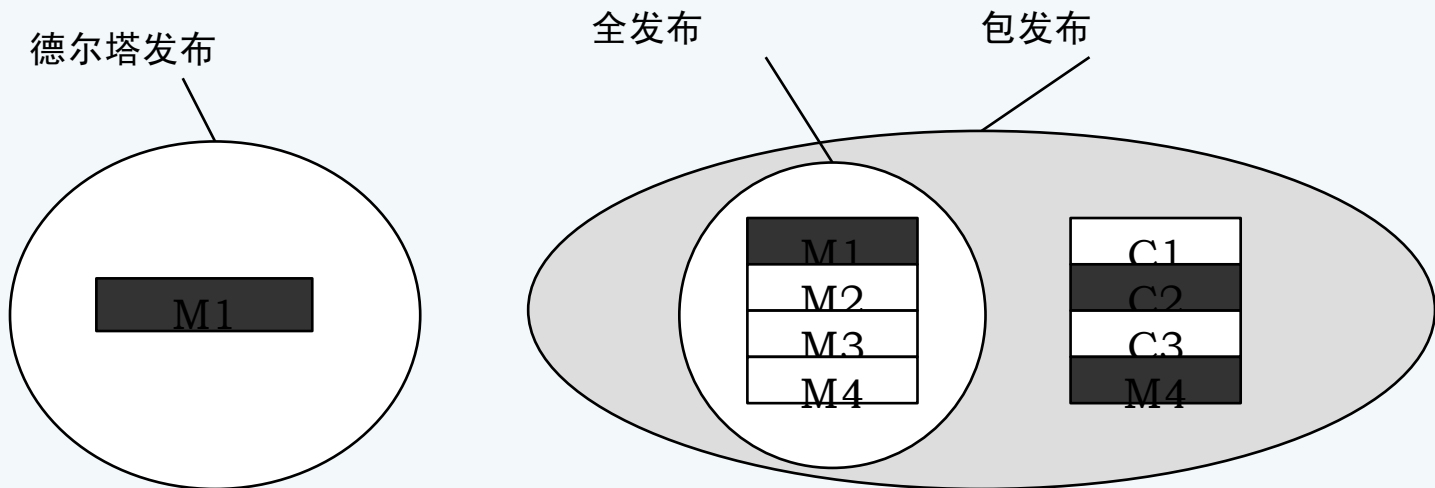
类型	使用情况
重大发布	伴随着重大的功能增强，可以消除多个已知错误
小型软件发布和硬件升级	已知错误的小的改进和修复
紧急发布	临时性修复



## 发布管理涉及的几种环境

- 开发环境
  - 以最终软件库(DSL)中的一个旧有版本为基础开发新的版本。版本的编号随着每一个新版本的出现而递增。软件一般只能在开发环境中进行变更。
- 测试环境
  - 用于版本测试的环境。一般可以分为开发人员用的技术测试区、用户使用的功能测试区和发布构建者使用的实施测试区。也有可能还有供用户和管理部门使用的最终验收测试区。
- 生产环境
  - 信息系统对用户开放的实际运作环境。
- 存档
  - 保留旧版本的软件。这些旧版本一般是不再使用的，但是如果有必要实施针对新发布的撤销计划是可能需要重新起用这些旧版本。

# 概念：发布方案



类型	使用情况	优点	缺点
德尔塔发布	紧急修复；临时修复	迅速	只对部分组件进行测试
全发布	不完全清楚哪些组件会发生变更	软件和硬件会得到彻底测试	周期长，消耗大
包发布	小的错误；新功能	为用户提供更长时间的稳定期	时间上的滞后

# 概念：最终软件库（DSL）

- 最终软件库(Definitive Software library)
  - 定义：最终软件库是一个存储所有软件配置项的最终批准版本(正本)的安全储存库：
  - DSL在物理上可能分布在多个地点，并且由安全的仓库和防火的保险柜组成；
  - DSL中可能包括同一种软件的多个版本，包括存档版本、相应的文档记录和源代码等：
  - 最终软件库(DSL)需要定期进行备份，因为它不仅包括当前的版本，还包括实施撤销计划时需要起用的版本；
  - 如果最终软件库(DSL)分布在多个地方进行管理，则每个地方应当备有一个最终软件库(DSL)的拷贝以应付软件的上线(Rollout)；
  - 发布管理涉及从软件被纳入到最终软件库(DSL)中开始的整个软件生命周期。

## 概念：最终硬件库(DHS)

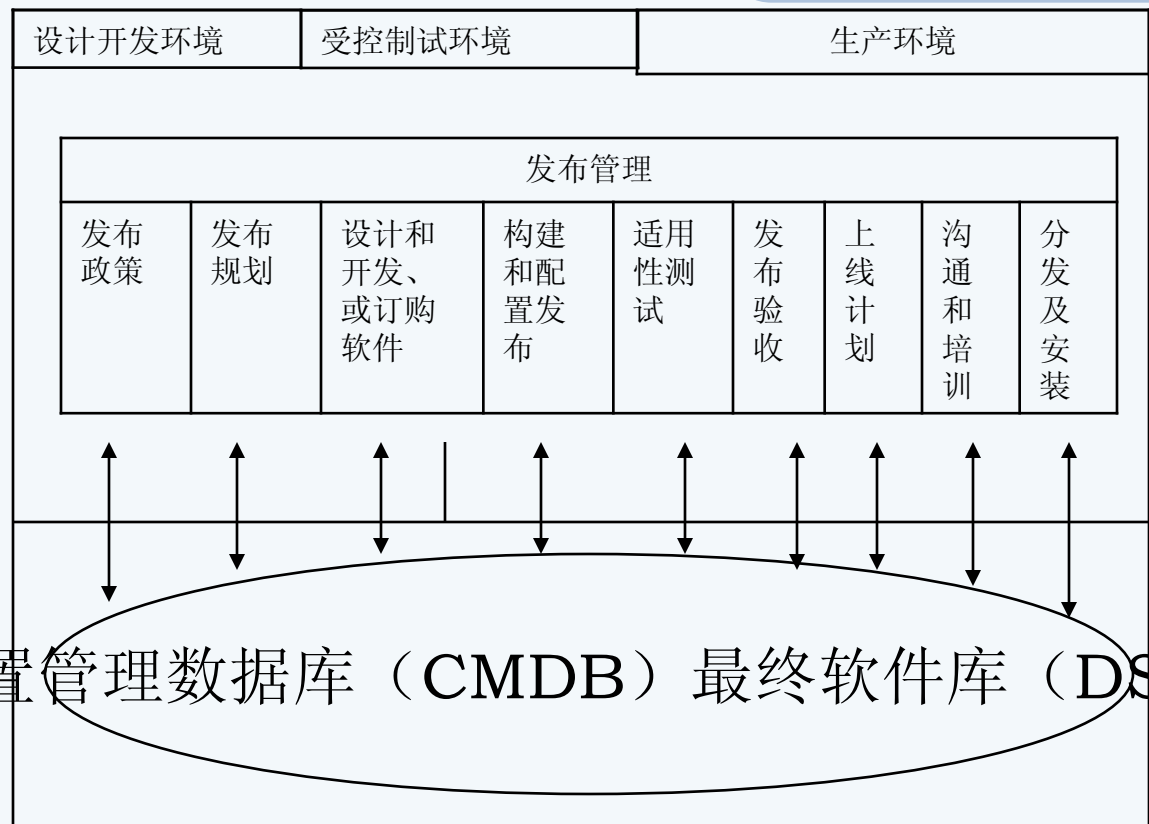
- 最终硬件库(Definitive Hardware Store)
  - 定义：最终硬件库中包含了硬件的备件和库存。
  - 这些备用组件和配件得到与它们在实际运作环境中的对应组件和相同级别的维护：
  - 最终硬件库(DHS)中的硬件可用来替换或修复IT基础架构中相似的配置。
  - 有关这些配置构成的详细信息应该被记录在配置管理数据库(CMDB)中。

- 实施发布管理流程将大大提高IT服务的效率。发布管理的收益有：
  - 减少风险
  - 在合理的事件段，以最小的影响实施发布
  - 减少各自为政
  - 降低非法使用软件的可能性
  - 增加用户在测试发布的参与度
  - 促使软硬件版本的标准化的



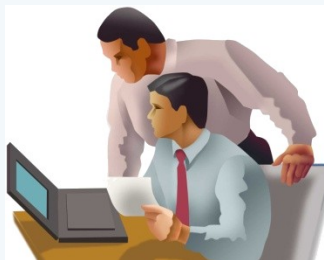
# 发布管理——ISO20000的要求

- 应与相关方协商发布策略并形成文件。发布策略应包括发布类型和频次。
- 服务提供商应根据业务要求对服务、系统、软件和硬件的发布进行策划。应在所有相关方之间就如何启动发布计划达成一致，并经过他们的授权，如客户、用户、操作人员和支持人员。
- 流程应包括一旦发布失败，返回或补救的方式。
- 计划应记录发布的日期及可交付成果，并参见相关的变更请求、已知的错误和问题。应就这些情况与事故管理流程进行沟通。
- 应评估变更要求对发布计划的影响。发布管理程序应包括配置信息和变更记录的升级和变化。应根据既定的流程来管理紧急发布。紧急发布流程应与紧急变更管理流程有接口。
- 应建立受控的接收测试环境，以在分发之前建立并测试所有的计划发布。
- 应设计并实施发布和分发，以确保在安装、处置、包装和交付的流程中保持硬件和软件的完整性。
- 应度量成功或失败的发布。度量应包括发布之后于发布有关的事故。分析应包括对业务、IT运行和支持性人力资源影响的评估，并作为服务改进计划的输入



发布管理流程的主要活动

- 发布政策制定和发布规划
- 发布设计、构建和配置
- 测试和发布验收
- 上线计划
- 沟通、准备和培训
- 分发和安装

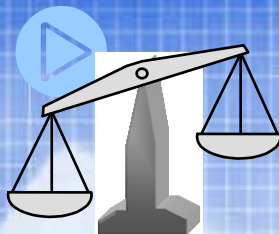


## 发布人员

- 在验收前对发布进行成功的测试
- 和发布经理一起准备首次运行计划
- 确保测试环境和现实环境一致

## 发布经理

- 准备发布计划
- 批准发布的构建和配置
- 作为变更顾问委员会的一员
- 协调最终的发布实施
- 负责与其他团队的沟通，例如用户、服务级别经理和变更经理



- 紧急发布数量/百分比
- 发布导致的错误数量
- 准时发布百分比
- 未经测试的发布数量
- 平均发布成本
- 客户满意度
- 优化的数量
- 从日志文件检测到的缺陷数量
- 测试并发布到生产系统的修复数量
- 返回到开发部门的修复数量
- 部署延迟天数
- 成功的应用构建数量

- 1) 下列哪项活动属于发布管理流程？
  - A. 检查组织内部的电脑上是否使用了非法软件
  - B. 在组织内部的电脑上安装原版软件
  - C. 记录哪些软件版本是可用的
- 2) 下面哪一项不是发布管理流程的目标？
  - A. 评估软件变更的影响
  - B. 与变更管理协商软件发布的具体内容
  - C. 为在组织内部分发软件变更设计和实施有效的程序
  - D. 防止软件病毒进入组织

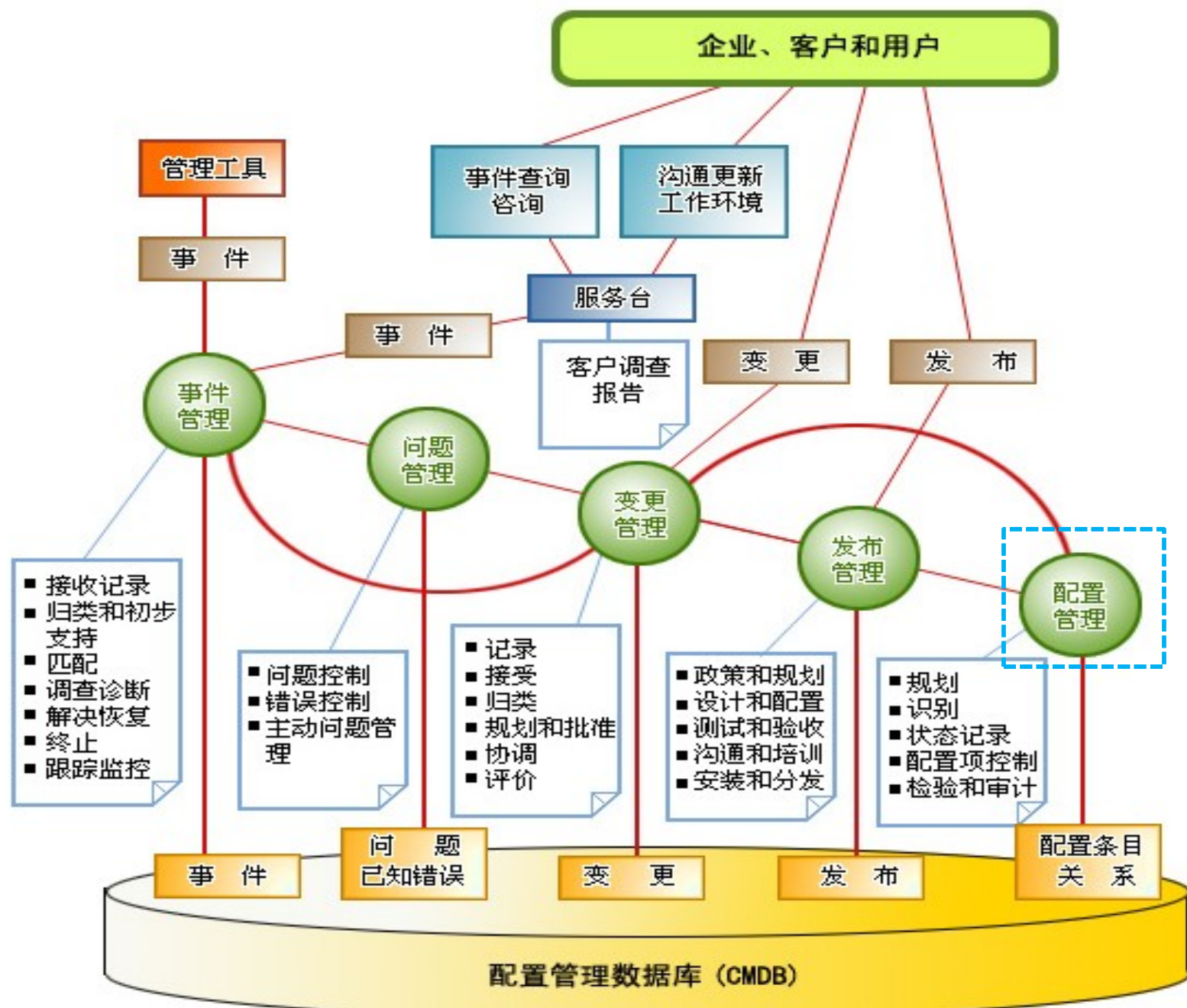


## ➤ 服务支持

- 服务台
- 事件管理
- 问题管理
- 变更管理
- 发布管理
- **配置管理**

## ➤ 服务交付

# 服务支持流程关系



## 定义

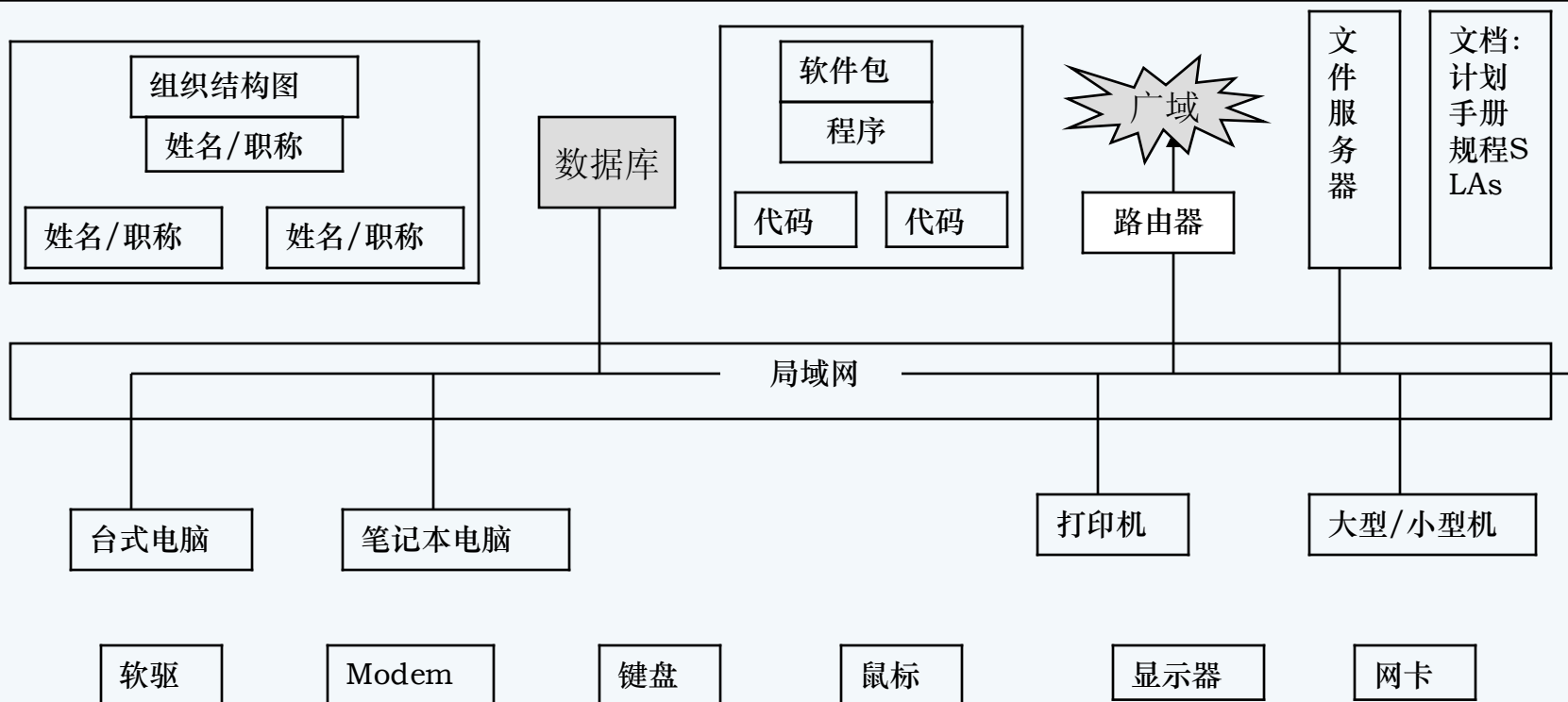
- 指由识别和确认系统的配置项、记录和报告配置项状态和变更请求、检验配置项的正确性和完整性等活动构成的服务管理流程。

## 目标

- 计量组织和服务中所使用的所有IT资产和配置项的价值；
- 为其它服务管理流程提供有关IT基础架构配置的准确信息；
- 为事件管理、问题管理、变更管理和发布管理的运作提供支持。

## 定义

- IT组件以及运用这些IT组件提供的服务被称为配置项（CI）。



## 概念：配置项 (续)

特性	内容
<ul style="list-style-type: none"><li>•服务交付所需要的</li><li>•唯一可识别的</li><li>•可变的</li><li>•可管理的</li></ul>	<ul style="list-style-type: none"><li>•所属分类</li></ul> <div>例如：软件、硬件</div>
	<ul style="list-style-type: none"><li>•关系</li></ul> <div>例如：父子关系</div>
	<ul style="list-style-type: none"><li>•属性</li></ul> <div>例如：编码、型号、存放地址、生产商</div>
	<ul style="list-style-type: none"><li>•状态</li></ul> <div>例如：测试中、使用中、闲置</div>



## 定义

---

- 包括所有与配置项及其状态和相互关系有关的信息的数据库。

## 说明

---

- 所有IT组件、组件的不同版本和状态以及组件之间的相互关系进行跟踪；
- 在其最基本的形式下，一个CMDB可能是由一些纸质表格或一套清单组成。

# 概念：CMDB (续)——分解的层次

第一层

IT设施

第二层

- 分解的层次越多，需要处理的信息越多
- 分解的层次越少，关于IT基础实施的控制和信息也就越少

第三层

软件组件1

软件组件2

第四层

程序1

程序2

程序3

第五层

模块1

模块2

第N层



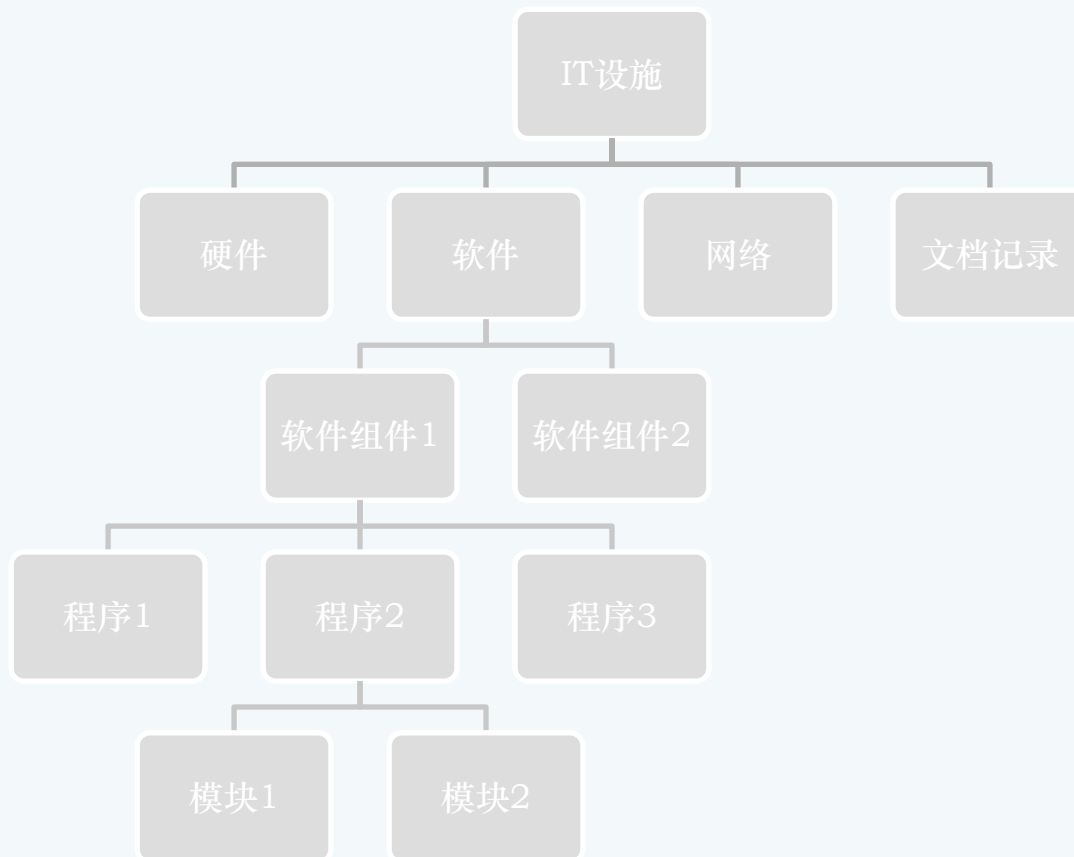
# 概念：CMDB (续)—CI 的关系

物理关系：

构成  
连接  
需要  
.....

逻辑关系：

拷贝  
相关  
被使用  
.....



## 定义

---

- 一个服务或配置项在某一特定时刻的配置状况（“快照”）。

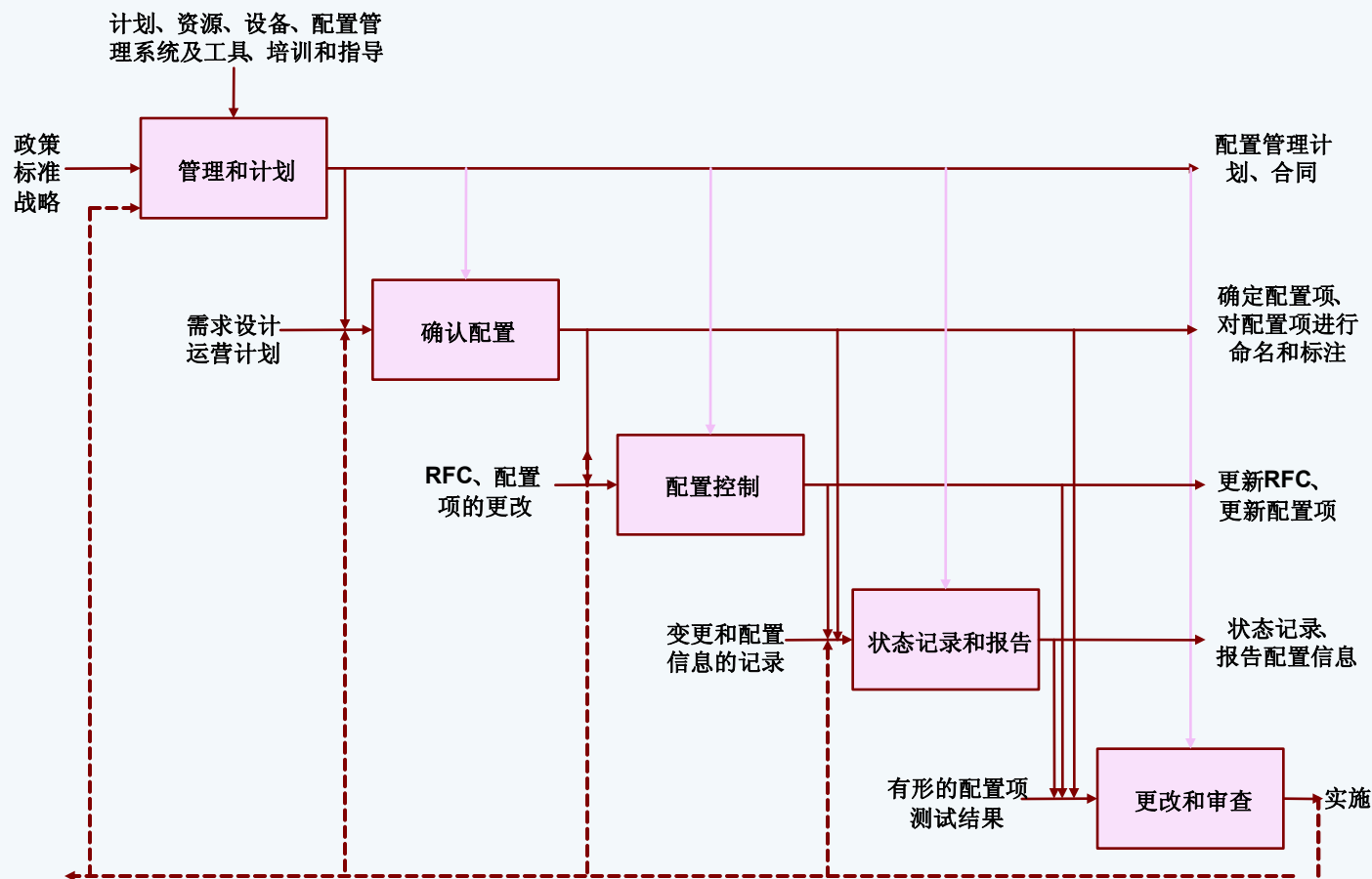
## 作用

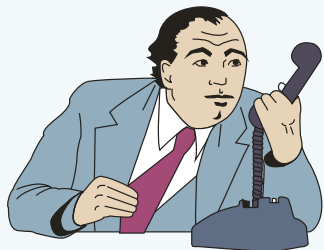
---

- 以后可以按照上述配置重建该产品或系统；
- 可以作为初始状态的一个参考或当前状态的一个对照。

- 在进行配置管理的变更和策划时应采用综合方法。
- 服务提供商应规定与资产财务管理流程的接口。
- 应制定关于配置项及组件定义的策略。
- 应规定每一项目应记录的信息，包括有效的服务管理所需的关系及文档。
- 配置管理应提供服务 and 基础设施组件的识别、控制和追溯版本的机制。控制的程度应充分满足业务需求、失效的风险和对服务的重要性。
- 配置管理应为变更管理流程提供与变更请求对于服务和基础设施配置影响有关的信息。适当时，配置项的变更应是可追溯的和可审计的，如软件和硬件的变更和活动。
- 配置控制程序应确保保持系统、服务和组件的完整性。
- 应在发布到实际运行环境之前建立配置项的基线。
- 数据配置项的主拷贝应控制在安全的物理环境或电子数据库中，并引用到配置记录，如软件、测试产品和支持文件。
- 所有的配置项应能被唯一的识别，并记录在CMDB（配置管理数据库）中。应严格控制对CMDB的更新。应主动管理并验证CMDB，以确保CMDB的可靠性和准确性。需要的人员应可获得配置项的状态和版本、位置、有关的变更和问题以及相关的文档。
- 配置审计程序应包括记录偏差、采取的纠正措施和结果报告的内容。

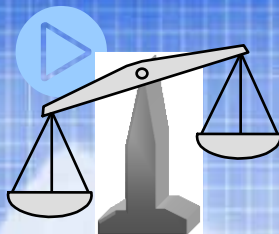






## 配置经理

- ✓就配置管理的范围和详细程度提出相关的变更建议。
- ✓确保配置管理流程在整个组织内得到良好的传达和沟通。
- ✓为该流程提供人员和培训。
- ✓开发识别系统和命名规范。
- ✓开发与其他流程的接口。
- ✓评估现有的系统和实施新的系统。
- ✓规划和实施CMDB的组建工作。
- ✓就流程的有效性、一致性和价值进行报告。
- ✓组织配置审计



- CMDB数据错误导致的变更失败数量
- 闲置许可证数量
- 配置项文档错误导致变更失败所引起的事件数量
- 因为CMDB错误导致违反SLA的数量
- 不精确配置项百分比
- 客户满意度

## 例题

- 1) 可以从哪个数据收集工具提取统计信息用来深入了解 IT 基础设施的结构和组成？
  - A. 能力管理数据库 (CMD) ☐
  - B. 配置管理数据库 (CMDB) ☐
  - C. 最终硬件库 (DHS) ☐
  - D. 最终软件库 (DSL) ☐
- 2) 配置管理数据库 (CMDB) 中的哪个属性有助于查明某个时刻的哪些配置项正在进行维护？
  - A. 购买日期 ☐
  - B. 责任人 (Owner) ☐
  - C. 位置 ☐
  - D. 状态 ☐
- 3) 由于产品本身的问题，用户现有的声卡被一块新的声卡替换。为方便以后参考，需对这块由另外一个制造厂商生产的新声卡进行登记。请问这项工作应由哪个流程负责执行？
  - A. 变更管理 ☐
  - B. 配置管理 ☐
  - C. 事件管理 ☐
  - D. 问题管理 ☐

## 例题

- 4) 某个组织内即将安装一批新的 PC。下列哪项活动不属于配置管理的职责？
- A. 检查有关这些 PC 的相关数据的完整性和准确性
  - B. 检查这些 PC 是否能够正常工作
  - C. 给这台 PC 命名并记录有关这些 PC 的相关数据
  - D. 记录关于这些 PC 的相关数据的状态并确保这些状态的安全
- 5) 一家中型规模的企业决定每半年对其配置数据库进行一次审核 (verification)。请问每隔半年进行一次审核够了吗？
- A. 是的，在一家中型企业中不需要更加频繁地做此类的审核
  - B. 不是的，在每次 IT 基础架构发生变更之后都应该实施审核
  - C. 根据上述信息无法判定
  - D. 取决于 SLA 中规定的协议
- 6) 下列哪项属于配置项？
- A. 呼叫
  - B. 文档
  - C. 事故
  - D. 流程



# 服务支持流程关系

