

第二章 IT 治理

★ 必须的知识点

1. IT 战略、政策、标准和程序对于组织的意义，及其基本要素
2. IT 治理框架(体系)
3. 制定、实施和维护 IT 战略、政策、标准和程序的流程。如:信息资产的保护、业务持续和灾难恢复、系统和基础建设生命周期、IT 服务交付与支持
4. 质量管理战略和政策
5. 与 IT 使用和管理相关的组织结构、角色和职责。
6. 公认的国际 IT 标准和准则(指导)。
7. 制订一长期战略方向的企业所需的 IT 体系及其内容
8. 风险管理方法和工具
9. 控制框架(模型)的使用，如:CobiT, COSO, ISO 17799 等控制模型。
10. 成熟度和流程改进模型(如:C1V1M, CobiT)的使用。
11. 签约战略、程序和合同管理实务。
12. IT 绩效的监督和报告实务
13. 有关的法律、规章等问题(如:保密法/隐私法、知识产权、公司治理的要求)
14. IT 人力资源管理
15. 资源投资和配置实务(如:投资的资产管理回报)

★ 可能的考试重点

公司治理与 IT 治理（概念）

IT 治理中董事会和执行经理层的作用（责任、关键成功因素）

IT 治理最佳实务（结构与关系）

IT 治理中审计的作用（确保 IT 的运用符合组织目标）

IT 战略：IT 战略委员会（职责、作用、组成）、IT 平衡记分卡

信息安全治理

企业架构（结构化方式反映组织的 IT 资产）

业务流程驱动的企业架构

FEA 参考模型

风险管理（原第七章内容，重点）

采购实务

IS 模块交付（内包、外包、混合采购）

采购战略

外包实务和战略（优缺点、风险）

服务水平协议（SLA）

全球化战略和实务

第三方审计报告

能力与发展

服务改进和用户满意度

行业标准/基准

信息系统组织结构

供货商和外包商管理
体系运营和维护（原运维）
应用开发和维护/系统开发和维护

职责分离（重点）

组织结构中不同人员的职责 ★ 需要了解和熟悉

IT 治理审计

查询理解 ★★★★★★★

信息系统安全管理的成果

信息系统安全管理的不同层次

★ 知识点摘要

公司治理

倡导的**公司道德文化**。世界经合组织将**公司治理**定义：“公司内不同群体之间责权利的分配关系，如董事会、管理层、股东和其他利害关系者，这些分配关系清楚地勾勒出公司决策的规则和程序。由此，制定公司目标和确定达成目标和监控绩效的方式。”

公司治理框架中的一个很重要内容是**建立管理和报告业务风险的规则**。该规则要求公司在改进和革新业务活动时**有监控风险的内部控制体系**。同时，公司治理框架又是**保护股东利益**的

董事会和执行经理层监控和保证实务

IT 治理一般关注两方面问题：**IT 增加商业价值和 IT 风险得到控制**。前者通过使 IT 战略与业务**战略保持一致**来达到，后者通过组织内的**职责分工**来达到。

IT 治理是董事会或最高管理层的责任，是企业治理的重要组成部分。

IT 治理的关键因素就是要使 IT 与业务融合，以实现组织的业务价值。

关键的 IT 治理因素包括：

IT 战略委员会

不仅要包括协助董事会承担 IT 治理责任方面提供战略建议，而且要把目光聚集在 **IT 价值、风险及绩效** 上面。这是把 **IT 治理机制集成到公司治理层面** 中去的一种机制。作为隶属于董事会的 IT 战略委员会，其主要职责就是要协助董事会监管组织的 IT 相关事务，保证董事会在掌握充分的内部、外部信息的基础上，作出有效的 IT 治理决策。

执行机构：指导委员会(Steering committees)

风险管理

标准 IT 平衡记分卡

过程管理评价技术。该方法超越了传统的财务评价方法，在**顾客满意度、内部流程和创新能力** 等方。。三个层面：**使命、战略、措施**

IT 平衡记分卡是协助 IT 战略委员会和最高管理层，**保持 IT 与组织业务高度一致的最有效的办法之一**。IT 平衡记分卡的主要目的就是要为管理层建立一套工具，以便于：**管理层向董事会汇报 IT 运营状况；在重要的利益相关者之间对 IT 战略目标达到一致；证明 IT 的价值及有效性；在组织中沟通 IT 的绩效、风险、能力。**

IT 治理是各种关系和流程的架构，用来指导和控制组织达成增值目标，同时还要保证 IT 及其流程的风险与收益的平衡。

IT 治理的目的是指导 IT 工作，确保 IT 绩效满足 IT 目标符合企业目标和预期利润的实现。另外，IT 应该帮助企业开拓商机，实现利益最大化。IT 资源应得到充分的利用，IT 相关风险也应该得到适当控制。

审计在 IT 治理中的作用

在组织内成功实施 IT 治理的过程中，审计扮演的是一个至关重要的角色。审计人员向高级主管提供建议和领导实务，以帮助他们提高 IT 治理的质量和效果。作为监控符合性的一个角色，审计帮助确认组织内实施的 IT 治理符合其初衷。

IT 治理的报告包括了对组织高级管理人员、跨事业、跨职能和跨部门的审计。

IS 审计师在制订审计计划应当考虑到组织的实际状况和员工素质。

IS 审计师依其角色的定义，应该评定 IT 治理相关的如下内容：

- .IS 功能符合组织的使命、理念、价值、目标和战略
- .IS 功能满足业务(效率和效果)的绩效目标
- .法规、环境、信息质量、信托和安全的要求
- .组织的控制环境
- .IS 环境的固有风险

信息安全治理

利用 IT 信息安全应当是 IT 治理中的一个重要的有机组成部分，在这一点上的疏忽将削弱组织机遇来完善业务流程的能力。

包括：信息的完整性、服务的持续和信息资产的保护

IT 治理中越来越关注的领域就是企业架构，所谓企业架构就是通过一种结构化的方式来反映组织的 IT 资产，并有效管理对 IT 投资。企业架构系统而又完整地定义了组织的当前(基准)环境和期望(目标)环境的蓝图。对于信息系统的更新以及开发新系统而言，建立 EA 是必不可少

技术驱动的企业架构是为了澄清现代组织面临的复杂技术选择问题，为组织在做以下决策时
业务流程驱动的企业架构是为了更好地理解组织业务的核心流程及支持流程，了解这两类流程的组成部分及相关支持技术，对现有流程中的不合理部分进行重新设计或改造，从而达到优化流程、降低成本、提高绩效的目的。

企业架构和 FEA 文件主要用来维护和描述技术的符合性，(持续)表述和评估 IS 部门正在管理的技术。IT 治理中涉及 IS 部门管理的方面包括更新战略技术所使用的选择流程和方法。

信息安全治理的 5 个成果 2008 新 P14

战略结盟 strategic alignment 信息系统安全策略和业务战略一致，支持组织的目标 好的
IT 治理可以延伸组织的战略和目标

1. Strategic alignment- Align information security with business strategy to support organizational objectives. To achieve alignment, the following should be accomplished:
 - Security requirements driven by enterprise requirements thoroughly developed to provide guidance on what must be done and a measure of when it has been achieved
 - Security solutions fit for enterprise processes that take into account the culture, governance style, technology and structure of the organization
 - Investment in information security aligned with the enterprise strategy and the well-defined threat, vulnerability and risk profile

风险管理 risk management 管理和执行适当的措施降低风险，使其对信息资源的影响降到一个可接受的水平

2. Risk management—Manage and execute appropriate measures to mitigate risks and reduce potential impacts on information resources to an acceptable level. To achieve risk management, consider the following:
- Collective understanding of the organizations threat, vulnerability and risk profile
 - Understanding of risk exposure and potential consequences of compromise including the regulatory, legal, operational and brand impacts
 - Awareness of risk management priorities based on potential consequences
 - Risk mitigation sufficient to achieve acceptable consequences from residual risk
 - Risk acceptance/deference based on an understanding of the potential consequences of residual risk

价值传递 value delivery 优化安全投资，支持组织目标 日常遵从最佳实务的安全基准、制度化的解决方案的一整套标准

3. Value delivery—Optimize security investments in support of business objectives. To achieve value delivery, consider the following:
- A standard set of security policies and practices, i.e., baseline security requirements following adequate and sufficient practices proportionate to risk
 - Properly prioritized and distributed effort to areas with greatest impact and business benefit
 - Institutionalized and commoditized standards-based solutions
 - Complete solutions, covering the organization and business processes as well as technology based on an understanding of the end-to-end business of the organization
 - A continuous improvement culture based on the understanding that security is a process, not an event

资源管理 resource management 有效和高效管理信息安全知识和设施

4. Resource management—Utilize information security knowledge and infrastructure efficiently and effectively. To achieve resource management consider the following:
- Ensure that knowledge is captured and available
 - Document security processes and practices
 - Develop security architecture(s) to define and utilize infrastructure resources efficiently

绩效衡量 performance measurement 衡量、监控和报告信息安全过程确保目标实现

5. Performance measurement—Measure, monitor and report on information security processes to ensure objectives are achieved. The following should be accomplished to achieve performance measurement:
- A defined, agreed-upon and meaningful set of metrics properly aligned with strategic objectives
 - A measurement process that will help identify shortcomings and provide feedback on progress made in resolving issues
 - Independent assurance provided by external assessments and audits

NOTE: Information security governance, when properly implemented, should provide four basic outcomes: **strategic alignment, value delivery, risk management and performance measurement.**

Strategic alignment provides input for security requirements driven by enterprise requirements.

Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. **Risk management** provides an understanding of risk exposure.

563. 下列哪项 IT 管理最佳实践改进了战略方针

- a. 供应商和合作者风险管理
- b. 有基于客户，产品，市场和流程的知识库
- c. 有能够提供创建和分享业务信息的组织结构
- d. 领导层在业务需求和技术部门之间的协调

答案： d

注释：领导层在业务需求和技术部门之间的协调是**改进 IT 战略方针**的最佳实践。供应商和合作者风险管理是**风险管理**的最佳实践。提供基于客户，产品，市场和流程的知识库是 IT **价值交付**的最佳实践。

信息系统战略

战略规划 从信息系统角度看，战略规划是组织为了**利用信息技术来完善其业务流程**而确定的发展方向及**长期**的计划。应当确保这些计划与组织的总体目标保持一致。**组织的结构和程序确保 IT 支撑和扩延组织的战略和目标**

指导委员会

高级管理层应当组建一个计划或指导委员会，监督其信息系统的职能和业务活动。处于组织高层的信息技术指导委员会是确保信息系统部门与公司宗旨和目标协调的一种机制。委员会应当包括来自高级管理层、用户部门和信息系统部门的人员。**每个成员应当在其负责的领域内有权做出决定**。主要职责是对信息系统项目进行审查，一般**不涉及**日常运营。

政策和程序

为了使政策能够被有效地执行，制定的**政策必须清晰和准确**。与组织的总体性目标和方向有关的政策的制订、开发、记录、推广和控制的责任应当**由管理层**承担，通过制定政策来为组织创造一种积极的控制环境。

根据公司总体政策采用**自顶向下**的方法来开发部门政策是较好的选择，因为它确保了各级政策的一致性。不过，有些组织选择先制定较低层次的政策，这样做的目的是为了节约成本，因为通常这些政策都是基于风险评估的结果而建立和实施的。公司的高层政策是对已有的运营政策的综合，这种方法叫做**自底向上**的方法。这种方法可能更实用，但是容易造成政策的不一致和相互矛盾。

管理层应当**定期审查**所有政策。政策也需要不断更新，反映新的技术和经营过程的重大变化，利用信息技术提高生产效率和获取竞争效益。

信息系统审计师要理解政策并对政策进行符合性审查是审计工作中的重要环节

信息安全政策

构建技术烈组织的安全架构的第一步。政策常常根据组织需要的工具和步骤的不同阶段来设定。

安全政策必须要在**控制水平和生产效率之间**保持平衡。换言之，控制成本不能超过控制所带来的受益。**组织文化**在设计 and 实施安全政策方面起到了重要的作用。安全政策必须经过**高级管理层批准**，并以书面的形式与**所有员工**和相关的服务提供商沟通。

程序

程序是详细的文件，根据组织的政策而制定并体现其精髓。程序必须清晰和准确，使接受者易于准确地理解。**程序记载了业务流程及其内在控制**，程序一般由**中层管理人员**制定，是政策框架下的具体化措施。

一般来说，**程序比相关政策更加易于变化**，它们必须反映业务重点和环境的不断变化。因此，经常审查和更新程序对于保持其相关性、可用性是很重要的。审计师审查程序是为了识别、评价并进一步测试业务流程中的控制，评估在程序中所建立的控制是否达到了必要的控制目标，并使业务流程高效和务实。当运营实务与书面程序不一致、或书面程序根本不存在时，管理层和审计师很难识别控制和确保其在持续起作用。

受程序控制的人员了解程序是最重要的。保存、分发和管理 IT 程序的配置方法和**自动化**机制是关注重点。

风险管理

风险管理是确定组织在实现其业务目标的过程中所使用的信息资源的脆弱性和面临的相关威胁的过程,如果存在风险,就需要确定针对风险采取控制措施,在基于组织信息资源价值的前提下(**成本效益考虑**),将风险降低到组织可接受的水平。

风险管理包括识别、分析、评估、处理、监控和沟通 IT 过程的风险影响。有了明确的风险喜好和风险承受能力,就可以设计风险管理战略和进行责任分工。根据风险类型和对业务的影响程度,管理层和董事会可以选择:

- .避免风险,如选择不从事风险巨大的业务或活动
- .降低风险,如制订并实施保护 IT 体系的控制
- .转移风险,如,与合作伙伴分担风险或将风险转移给保险公司
- .接受风险,如,正视风险的存在并控制其发生
- .消除风险,如尽其可能转移风险源

风险能够被转移、降低、接受或避免。

如果**控制的成本超过了安全收益**(这也称为**控制过度**),组织就可以选择接受风险而不是榨加成本来保护系统。

建立风险管理程序 risk management program 2008 新

第一步、确定风险管理程序的目标,确定成本和效益,CEO 或董事会制定基调

第二步、给不同的人或团队分配建立、实施风险管理程序的职责

建立风险管理程序必须考虑整个 IT 环境

风险管理过程

.风险管理的第一步要对那些具有脆弱性,易受威胁,需要保护的信息资源或资产**进行识别与分类**。分类的目的是为进一步的调查进行**优先级排序**,以确定适当的保护级别(基于资产的价值简单分类);二是为了确保安全保护标准模型得以实施(根据危险程度和敏感程度分类)。

.风险管理的第二步是评价与信息资源相关的威胁和脆弱性,及其发生的可能性。脆弱性是信息资源的固有特性。

.一旦各种风险要素被一一确定之后,把它们结合起来考虑就可以形成对风险的总体评价。结合这些风险要素的通用方法是对每一个威胁计算其对资产脆弱性的影响,把这些影响累计起来就形成了对总体风险的度量。

一旦风险被确定,就可以评价组织中的现有控制或设计新的控制措施将风险降低到一个可接受的水平。这些控制通常是作为风险对策来部署,可能是行动、设备、程序或技术。

实施控制后剩下的、没有被有效控制的风险就叫做**剩余风险**。管理层可以把剩余风险作为衡量某一区域是否需要进一步采取控制以降低风险的度量指标。组织的可接受风险水平应当由管理层决定。**成本考虑**

IT 风险管理需要在多种层面上进行综合分析,在各个层面(**运行层面/项目层面战略层面**)识别、评估和管理 IT 风险是组织中不同的个人与集体所要承担的职责,但这些职责又不能完成隔绝开来考虑,因为**某一层面的风险可能会影响其他层面的风险**。**运营层面、项目层面、战略层面**

进行风险管理时,各种**复杂方法与软件包的使用不能取代业务常识与职业审慎**在风险管理时的重要作用。

风险分析方法

定性

定性风险分析方法使用文字或文字分级来描述风险的影响和发生可能性。财务、管理半定量

半定量风险分析方法采用描述性的风险分级与数字分级相结合的方法。无法使用定量定量，

定量风险分析方法使用数值描述风险的可能性和影响，使用的数据来自不同方面。概率与期望值(Probability And Expectancy)、年预期损失方法(ALE, Annual Loss Expectancy Method)

不可预知的灾难事件也会发生 C 要谨慎的估计最坏事件发生的可能性。

信息系统管理实务：人事管理、采购实务、变更管理、财务管理、质量管理、安全管理、绩效优化。

然而，在信息化社会中，信息系统在许多方面已经与业务融为一体，对组织而言，信息系统变得越来越重要。信息系统审计师必须认识到一个管理良好的信息系统部门对于实现组织的目标是不可或缺的因素。

人事管理 人力资源管理

人事管理涉及员工的聘用、晋升、保留和终止政策和程序的制定与执行。这些管理活动与信息系统的职能密切相关，其有效性将会影响到员工的行为表现和对信息系统职责的履行。

临时雇员和第三方雇员可能引入不可控风险

缺乏对保密要求的了解可能导致对总体安全环境的损害

交叉培训是指培训一个以上的人员从事一项特定作业或程序，这样做的好处是降低了对某个员工的依赖程度，并可以作为接替计划的一部分，它可以在员工缺勤情况下提供备用人员，保持业务持续性。但同一个人了解系统所有部分后的风险不小。

通过强制休假(Required Vacations)确保每年至少一次由日常履行某个工作职责之外的人代行该职责。这样做减少了进行不正当或违法行为的机会。使日常履行某个工作职责之外的人代行该职责，也可以发现潜在的不合规行为。

解雇政策应当为组织的计算机资产和数据提供充分的保护。

采购实务 sourcing practice

组织应该评估 IS 职能以确定最适当的实现 IS 职能的方式，可以考虑下列问题：

IS 是组织的核心部门吗？

该部门有达成目标和目的所特有的知识、方法和员工，而这些都是难以替代的资源。

这些 IS 职能能否外包给其他组织，而成本、质量和风险均有更佳的体现？

组织是否拥有管理第三方、或远程、跨国执行 IS 和业务职能的经验？

完成上述采购战略，IS 指导委员会检查并批准该战略。

外包实务是组织根据协议，将部分或全部信息系统部门的职能转交给外部实体。大多数信息系统部门则利用提供商的各种各样的信息资源，因此，需要制定外包流程来有效地管理这些协议。

不同的组织有不同的 IT 外包目标。需要管理层重新考察其依赖的控制架构是否能控制外包所带来的风险。

因为服务提供商一般对于时间与成本非常敏感，因此很少发生项目失控、时间延期的情况。

合同条款适当考虑到合理的偶然/例外事件。保护本机构自有数据的完整、保密和有效，同时**清晰地建立数据所有者关系**。

外包实务要求管理层能够积极管理外包关系和外包的服务。IS 审计人员**定期检查合同和服务情况**以确定没有出现新问题。

IS 审计人员还可以检查承包方成文的流程和他们的质量计划(包括 CMM、ISO 等标准)的执行情况。这些质量计划要求定期的审计以确定流程达到了**质量标准**。

外包不仅仅是一个成本决策的问题，它是一种**对管理具有重大控制影响的战略决策**。服务提供商在**企业文化和人力资源方面与组织的兼容性**是管理层不应忽略的一个重要事项。

应当把**服务水平协议 SLA 看作是一种控制手段**。当外包服务提供商来自境外时，还需考虑**跨国界的法律问题**。

IS 审计师可以要求外包服务提供商定期提供第三方审计报告，对服务提供商实施的控制进行鉴证，这些控制**应涉及数据的机密性、可用性和完整性的各方面**。

行业标准/基准为组织确定在相似的信息处理环境下提供的服务水平提供了一个参考依据和对照比较的标准。**供应商的服务必须符合其客户信赖的标准**。

变更管理

项目实施的整个过程都应该**获得用户的反馈**，包括确认业务需求，对新的或变更后的功能进行培训和测试等。

财务管理实务

IT 用户的**计费机制(Chargeback)**，组织中采用的针对 IT 服务的内部收费方式)

这种收取方式是信息系统部门 and 用户部门的共同责任，它可以作为信息系统部门和用户的一种工具，**来衡量信息处理设施所提供服务的效果和效率**。

信息系统预算应当与 IT 的**短期计划及长期计划**结合起来考虑。

质量管理

质量管理是信息系统基于部门的流程得到有效控制、评价和改善的手段。

坚持并遵守已制定的流程要求及相关流程管理技术是衡量信息系统组织的效果和效率的关键。

质量管理体系是文件化的体系，它基于一系列文件、手册和记录。突出标准是 **ISO9001 质量管理体系**。

信息系统审计师应当关注业务职能和流程**是否正式成文（最新的文档）并被遵照执行**，是否产生了预期结果。因为开发和实施流程管理技术会产生成本，信息系统审计师最关心的是明确定义并正式成文的、与 IT 相关的关键的业务流程。为此，信息系统审计师可以建议实施一个流程完善程序，排定所需采取的行动的顺序，制定实现所需的行动计划，投入实施该计划所需的资源。

该标准要求**保留一系列必备的质量记录**，用以表明系统的存在性和功效，并且在内部和外部审计时需要接受审查

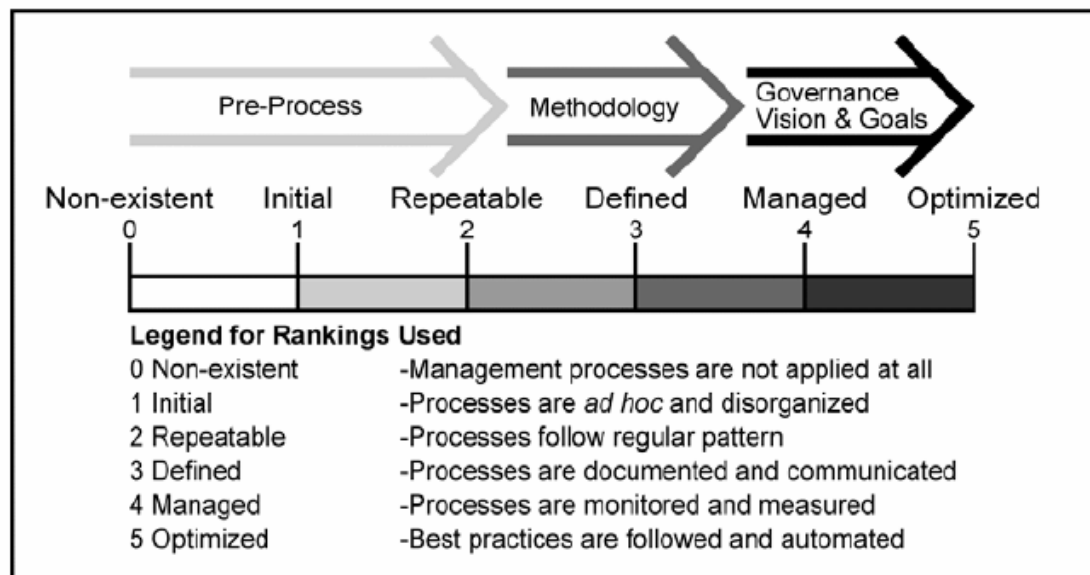
信息安全管理

信息安全管理在确保组织所控制的信息和信息处理资源受到适当的保护方面起着重要作用，它领导和促进整个组织范围内的 IT 安全程序的实施，信息安全管理主要包括了安全方策略的制定、组织与人员的安全管理、访问控制、支持组织关键业务流程的业务持续计划和灾难恢复计划等内容。制定合理的信息安全管理程序的一个重要前提就是要应用风险管理原则来评估 IT 资源的风险，并将这些风险降低到管理层可以接受的水平，并监视剩余的风险。

IT 治理的不同层次：????

IT 治理成熟度模型 IT Governance Maturity Model

Control Objectives for Information and related Technology(COBIT)



Nonexistent

There is no senior management oversight of IT-related activities to ensure that the enterprise's IT goals add value to the organization and to ensure that IT-related risks are appropriately managed.

Initial/Ad Hoc

There is a realization that more formalized oversight of IT is required and it needs to be a shared management responsibility requiring the support of top management.

Regular governance practices such as review meetings, creation of performance reports, and investigation into problems take place, but rely mostly on the initiative of the IT management team, with voluntary or co-opted participation by key business stakeholders, depending on current IT projects and priorities. Problems identified are tackled on a project basis with teams formed as necessary to undertake improvements.

Repeatable but Intuitive 可重复的/直觉

The concept of IT governance does not exist formally and oversight is based mostly on management's consideration of IT-related issues on a case-by-case basis. The governance of IT depends on the initiative and experience of the IT management team, with limited input from the rest of the organization.

Upper management is involved only when there are major problems or successes. The measurement of IT performance is typically limited to technical measures and only within the IT function.

Defined Process

An organizational and process **framework has been defined** for oversight and management of IT activities and is being introduced to the organization as the basis for IT governance.

Specific procedures for management covering key governance activities have been developed. These include regular target-setting, **reviews of performance**, assessments of capability against planned needs, and project planning and funding for any necessary IT improvements.

Previous informal but successful practices have been institutionalized and the techniques followed are relatively simple and unsophisticated.

Managed and Measurable

Target-setting has developed to a fairly sophisticated 老练的; 精密的 stage with relationships between outcome goals in business terms, and IT process improvement measures now well understood. **Real results have been communicated to management in the form of a balanced scorecard.** The enterprise's management team is now working together for the common goal of maximizing IT value delivery and managing IT-related risks. There have been regular assessments of IT capabilities and projects have been completed that have delivered real improvements to IT's performance. Relationships among the IT function, its users in the business community and external service providers are now based on service definitions and service agreements.

Optimized

?The IT governance practices have developed into a sophisticated 老练的 approach using effective and efficient techniques. There is true transparency of IT activities, and the board feels in control of the IT strategy.

?IT activities have been optimally directed toward real business priorities, and the value being delivered to the enterprise can be measured and steps taken on a timely basis to correct significant deviations or problems.

?The balanced scorecard approach has evolved into one that is focused on the most important measures relevant to the enterprise's overall business strategy. The effort spent on risk management (and on IT management activities generally) has been streamlined through adoption of standardized and, where possible, automated processes.

?The practice of continuous improvement of IT capability is embedded in the culture and this includes regular external benchmarking and independent audits providing positive assurance to management.

?Overall, the cost of IT is monitored effectively and the organization is able to achieve optimal IT spending through continuous internal improvements, the effective outsourcing of selected services and effective negotiation with vendors. When dealing with external business partners or service providers, the organization is able to demonstrate first-class performance and demand best practices from others.

绩效优化

优化是指在无须对信息技术基础设施追加额外投资的情况下, 将信息系统的**生产力提高**到可能达到的最高水平。制定和更新**绩效评价**指标是第一步。

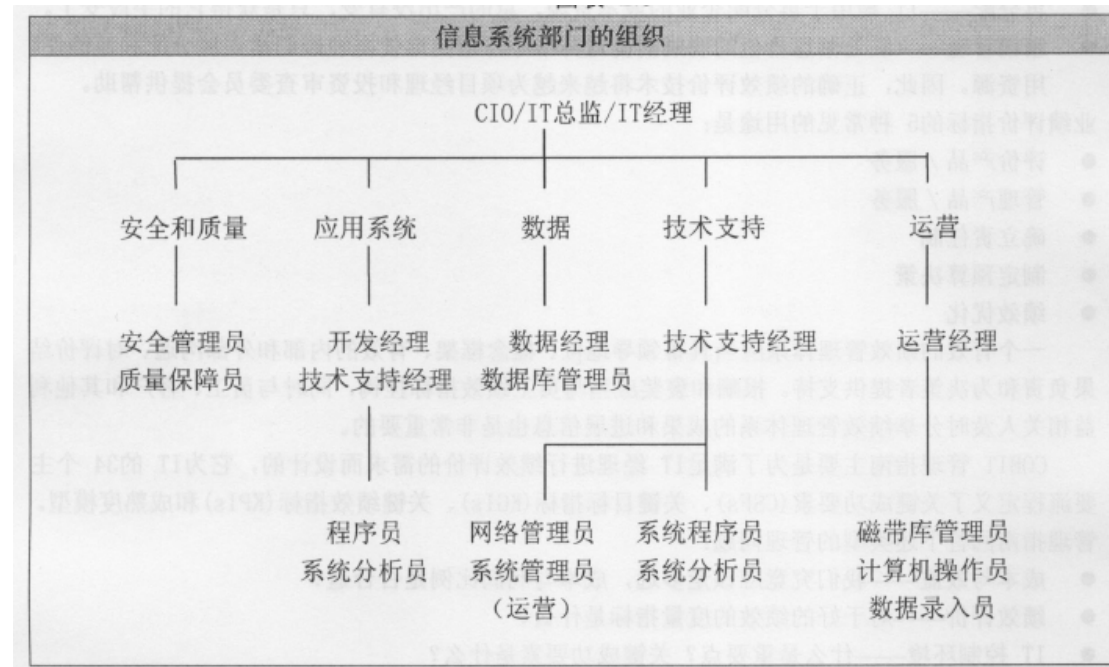
业绩评价指标的 5 种常见的用途是:

- .评价产品/服务
- .管理产品/服务
- .确立责任制
- .制定预算决策

.绩效优化

绩效考评了一个组织 IT 所有的环节

信息系统组织结构和责任 ★★★



需要了解各个环节人员的主要职责、存在风险和控制要点

每个员工都应有一份组织结构图，它提供了清晰的部门层次和授权。另外，工作描述为信息系统部门员工提供了其任务和职责清晰的指引。信息系统审计师应当在被审计方的**现场观察**和**确定工作描述和结构是否充分**。必须审查的职位：系统开发经理(System Development Management)、帮助台(Help Desk)、最终用户(End User)——负责与业务应用系统有关的具体操作、**数据管理员**——负责数据资产管理和大型 IT 环境下的**数据结构设计**

需要由专门的人员管理**供货商 vendor**和**外包商**，

体系运营和维护

运营经理(Operations Manager)负责计算机操作人员的管理，包括准确有效地运行**信息处理设施(IPF)**所需的所有员工(比如，计算机操作员、资料库管员、日程安排人员和数据控制人员)。IPF 包括计算机、外设、磁性介质及其存储的数据。IPF 是一项主要的资产投资。管理控制可以被细分为**物理安全控制**、**数据安全控制**和**处理控制**三类。

▲ **资料库管理员**：资料库管理员(Librarian)负责登记、发布、接收和保管 IPF 保存在计算机磁带和/或磁盘上的**所有程序和数据文件**。根据组织的大小，资料库管理员可以是某个全职人员或某个数据控制组兼职成员。由于该职位非常关键

▲ **数据录入(Data Entry)**人员从事一项关键的信息处理活动。数据被成批录入或在线录入。**部门经理**负责确保数据在录入系统时是合法的、准确的和完整的。

系统管理 系统管理员(Systems Administrator)

增加和配置新的工作站

设置用户账号

安装系统级软件

执行预防/保护/修复病毒传播的程序
分配海量存储空间

安全管理员(Security Administration)

必须首先得到管理层的支持，**管理层要明确承诺对信息安全管理**的责任，并要理解和评价安全风险，制定和强制执行一套书面政策，清晰地说明应当遵循的标准和程序。在信息安全管理体制中，安全管理员(Security Administrator)是一个重要的职位，其职责应当在政策中明确定义。为了提供充分的职责分工，该职位应当是一个全日制职位，。来预防对**组织资产(包括数据、程序和设备)的非法访问**。向 IPF 主管直接报告。
定期审查和评估安全政策，向管理层提出必要的修改意见

质量保证(Quality Assurance 人员执行

两种不同的任务:

.**质量保证(QA, Quality Assurance)**。帮助信息系统部门确保其人员遵守了规定的**质量过程**。

比如，QA 可以帮助确保组织制定程序和文档符合标准和命名惯例。

.**质量控制(QC, Quality Control)**。负责进行测试和审查，验证并确保软件不存在缺陷并**满足用户的预期**。它可以在应用系统开发的各个阶段进行 **无论如何都不能让个人对自己完成的工作进行质量检查**

数据库管理员(DBA, Database Administrator)

是一个组织的数据保管员，其职责主要是定义和维护公司数据库系统的数据结构。DBA 必须理解该组织、用户数据和数据关系(结构)要求，对保存在数据库系统中的**共享数据的安全负有责任**；DBA 负责公司数据库的**设计、定义和正确的维护**；DBA 通常向 IPF 主管直接报告其工作。**实施数据库定义控制、访问控制、更新控制和并发控制**。DBA 拥有建立数据库控制的工具和绕过这些控制的能力，DBA 也能访问所有数据，包括生产数据。通常无法禁止或完全预防 DBA 对生产数据的访问。DBA 活动需要得到管理层的审批。检查性控制、职责分工。

系统分析员(Systems Analysts)

是基于**用户需求**来设计系统的专家 **程序规格说明书**:

安全构架师(Security Architects)

安全构架师(Security Architects)评估安全技术、设计安全的网络拓扑结构、访问控制、标识管理和其他安全系统、还要建立安全策略(或安全政策)和安全需求。

(安全)政策、需求和(网络)体系图

应用组成员(Applications Staff Members)

负责开发和维护应用系统。管理层必须确保他们不能访问生产程序，只能在测试环境

系统组成员(Infrastructure Staff Members)

负责维护包括操作系统在内的系统软件。该职能可能需要给予他们**无限制地访问整个系统的权限**。信息系统管理人员必须密切监督他们的活

网络管理员(Network Administrators)

负责管理网络基础设施中的关键组成部分(路由器、交换机、防火墙、网络分段、运行管理、远程访问,等等)。**不应当赋予局域网管理员应用系统编程**的责任,但是可以使其承担最终用户

职责分工 ★★

信息系统审计师必须获得足够的信息以了解各种工作职位、责任和授权之间的关系,从而**评估职责分工是否充分**。职责分工可以避免因为某一个人**负责多个关键的职位**而造成不能在日常的业务活动中及时地发现其错误的情况。职责分工是威慑和预防欺诈或恶意行为的一种手段。需要分开的职责包括:

.资产的管理

.授权和批准

.交易的记载

兼职情况下为避免潜在的风险,就需要对这些岗位增加**补偿控制(Compensating Control)措施**。补偿控制是一种内部控制,当职责不能被适当地分开时,用于减少存在或潜在的控制弱点的风险。职责分工的目的是通过适当的补偿控制减低或消除业务风险。对于不同的组织,也能确定风险的影响和发生的可能性。**工作描述也指明了组织中职责分工的程度**
可以兼职的: 系统开发和维护、网络管理和网络安全

控制措施

数据所有者有责任决定对数据的**使用者授予**什么级别的**访问授权**,对重要数据的访问必须加以限制,所采取的控制措施必须能保护组织的所有信息资源。为达到这样的目的,组织首先要**对其信息资产进行分类**。组织应当**基于其安全策略和通用的实践标准**(如:职责分工、最小授权原则)来决定其访问控制的决策。**实施控制措施不能以中断正常的业务流程为代价**

用户授权表格又可称为用户访问控制列表(Access Control List)

针对缺乏职责分工的补偿控制 ★★★

审计踪迹(Audit Trails)。审计踪迹是所有设计优良的系统的基本组成部分,它通过提供追踪一项交易的详细“地图”来帮助信息系统部门、用户部门和信息系统审计师**跟踪交易流的来龙去脉**,使得用户部门和信息系统审计师能够建立自起点到终点的实际交易的全过程。

核对(Reconciliation)。控制总计(Control Totals)和平衡表(Balancing Sheets)来完成**例外报告(Exception Reporting)**。例外报告应当由主管层来处理,并且需要证据,**交易日志(Transaction Logs)**。

监督性审核(Supervisory Reviews)。监督性审核可以通过**现场观察和问询**来进行。

独立性审核(Independent Reviews)。独立审核是为了对错误或故意违反操作程序的行为进行补偿控制。在不能进行有效职责分工的小型组织中尤其重要

审计 IT 治理

被审核的各种文档应当被进一步进行评估,从而确定:

它们是否**如实反映了管理层的思想**,并得到了**授权**。

它们**是否适用于当前状况**,并能得到**及时最新**。

确保在恰当的周期内对**合同遵循性**进行审核