



2013年CISA考试知识点变化总结讲义

马 庆 汇哲科技资深讲师

CISA/CIA/CCSA/CBCP/Security+/TCBC

关于我们

上海汇哲信息科技有限公司（简称“汇哲”或“SPISEC”），长年致力于信息安全意识、管理、技术、审计、认证等方面的培训和实践研讨，始终以信息安全的共享交流、学习指导、职业规划。SPISEC为信息安全行业内综合的培训服务模式，重于实践和服务质量的精细、实用，及永久。其讲师均具备信息安全十年以上工作经验，五年以上培训经验，自身长年致力于信息安全培训和服务行业，具备较强的专业培训水平和丰富的培训经验。SPISEC专业、强大的后续服务团队专为学员解决考试、认证、工作实践等问题。并结合多年培训经验，以培训为基础、服务为保障、实践为目的，为业内企业和个人、业内第三方合作伙伴提供优质的培训服。

SPISEC于2008年开始在业内陆续组织多场专业知识学习讲座和研讨，并持续发布多期专业原创文档和学习形式期刊、书籍。SPISEC至今为27000多名会员提供免费的学习指导服务，其中为3000多名会员直接提供考试辅助、职业规划、学习计划梳理等服务，会员现分布央企、国企、金融、电、移动、能源、制造、IT等多个行业。

<https://www.spisec.com/>

2013年CISA考试大纲

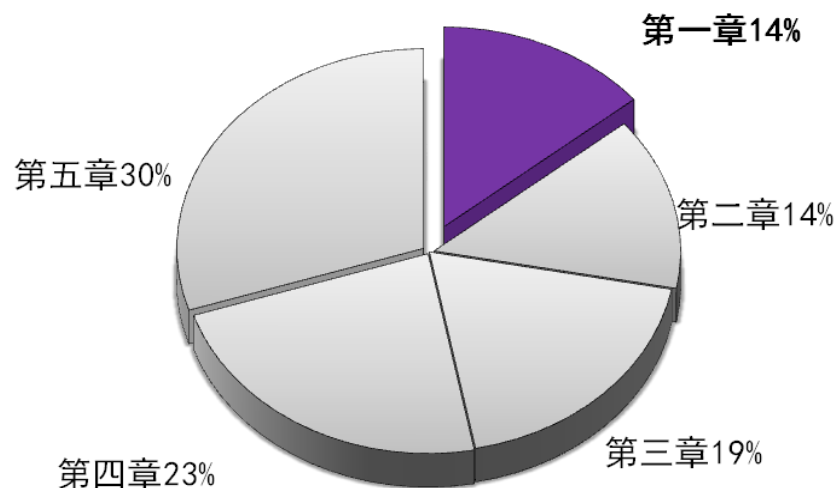
第一章 信息系统的审计流程

第二章 IT治理与管理

第三章 第三章信息系统的购置、开发与实施

第四章 信息系统的操作、维护与支持

第五章 信息资产的保护



第一章信息系统的审计流程

➤ 增加内容

1.2.3 审计计划—审计规划

1.3.5 审计准则、指南、工具和技术（程序）的关系

1.3.6 信息技术保证框架（ITAF）

1.4 风险分析

➤ 变化内容

1.2.4 法律法规对信息系统审计规划的影响

1.5 内部控制

1.5.1 信息系统控制

1.5.2 COBIT5 可免费下载参考《COBIT5.0实施指南中文版》，《COBIT5.0企业IT治理和管理业务框架中文版》，《COBIT5.0过程推动中文版》

1.6.1 审计分类

第二章IT治理与管理

➤ 增加内容

2.3.3 IT平衡记分卡

2.5 成熟度和流程改善模型

2.9.2 外包实务—第三方服务交付管理—云治理

2.9.5 质量管理

➤ 变化内容

2.3.1 IT治理最佳实践

2.3.2 IT治理/战略委员会

2.9.7 绩效优化

2.12.10 计划演练--业务连续管理最佳实践

第二章IT治理与管理

➤ **删除内容**

2.2 公司治理

2.3.4 信息安全治理—有效的信息安全治理

➤ **删除小节内标题但保留内容**

2.10.3 职责分离—访问数据（目录删除内部标题）

2.3.4 信息安全治理—有效的信息安全治理（目录删除内部标题）

2.9.2 外包实务—目前外包治理方法（目录删除标题）

2.9.2 外包实务—第三方服务交付管理（目录删除内部标题）

2.3.3 IT平衡记分卡

➤ 为了把平衡记分卡应用于IT，使用三层结构描述四个方面的问题：

- 使命

- 成为首选的信息系统供应商
- 经济、有效地交付IT应用系统和服务
- IT投资能获得一个合理的业务回报
- 抓住机遇应对未来挑战

- 战略

- 开发良好的应用系统与运营
- 建立用户伙伴关系和良好的客户服务
- 提高服务水平，优化价格结构
- 控制IT费用
- 为IT项目赋予业务价值
- 提供新的业务能力
- 培训和教育IT职员，追求卓越
- 为研究和开发提供支持

- 度量

- 提供一套稳定的指标（如KPI）指导面向业务的IT决策

- 来源

- 最终用户人员（按部门）
- COO
- 流程所有者

注：2013年新增知识点

2.5 过程改进模型和成熟度

- **COBIT流程评估模型 (PAM)使用COBIT4.1, 被用于改善IT流程审查的严格和可靠性, 模型作为参考文件用于绩效评估一个组织目前IT流程成熟度并且定义执行评估的最低要求以确保: 输出是一致的, 可重现的, 可代表被评估流程, 与ISO/IEC15504-2一致, 使用流程能力和流程绩效指标以确定流程属性是否获得。注: 2013年新增知识点**
- IDEAL模型—用于指导企业计划和实施有效的软件过程改进程序, 在实施SEI服务方面被使用的策略。遵循IDEAL方法进行软件过程改进的企业能够有效地集成SEI的技术、课程、研讨会和服务形成一个综合的方法提高能力。
- CMMI—一个为企业提供有效过程改进的方法, 指导一个项目、一个部门或者整个企业的过程改进。CMMI能够帮助集成传统分立的组织功能, 设置过程改进目标和优先级, 为质量过程提供指导和评估当前过程的参考点。

2.9.2采购实务


- 云治理

在考虑使用云服务时，业务和IT的战略方向在总体是主要焦点。当企业需求转向云提供传统上被内部管理的IT服务时，企业需要做出部分改变以帮助确保可以持续满足绩效目标，技术供应和业务战略一致，风险可管理的。确保IT与业务一致，系统是安全的和风险是可管理的，在任何环境都是挑战，在第三方管理中更加复杂。**典型的治理活动例如目标设定，政策和标准开发，定义角色和责任，管理风险等，在处理云计算技术和云计算服务商时必须得到特别的考虑。**

随着所有组织级改变，期望需要做出部分调整处理业务流程的方式。业务流程例如数据处理，开发和信息恢复是潜在的变化区域。另外，处理细节关于信息被储存，存档和备份的方式将需要重新考虑。

2.9.2采购实务

业务需要考虑云的很多独特情况。一个大的治理问题是业务部门人员，以前被强迫通过IT部门获得服务，现在可以绕过IT部门从云中直接得到服务。**应修改或开发政策以定义流程处理云服务使用的采购，管理和终止。（2013年新增知识点）**



2.9.5 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。流程是由一系列任务组成，如果这些任务被正确地执行，就可以产生预期的结果。
- 信息系统审计师应当关注业务职能和流程是否标准，例如：**ISO9001**，**ISO9001：2008质量管理体系作为突出的标准得到广泛的认识和接受**，**取代早期质量管理的ISO标准（2013年变化知识点）**；ISO20000、**ISO27001**、ISO9126、CMM等正式成文并被遵照执行，如果已制定，是否能产生预期的结果。
- 信息系统审计应关注组织是否已书面制定职能与流程并遵照执行，如果已制定，是否能产生预期的结果。
- 信息系统审计师重点关注为关键业务职能制定的IT相关书面流程。为此，审计师建议实施一个流程改善程序，排定所需活动的次序，制定所需的行动计划，为执行计划投入资源。

2.9.5质量管理

ISO27001前世

- ISO27001/17799的前身是BS7799, BS-7799是由英国标准协会 (British Standards Institution,简称BSI) 制定的信息安全管理体系标准。
- 1993年1月由英国贸易工业部立项, 组织大企业的信息安全经理制定提出了《信息安全管理实践规范》(Code of Practice for Information Security), 9月在英国发布。
- 英国标准协会(BSI)于1995年2月制定世界上第一个信息安全管理体系标准 - BS7799-1:1995信息安全管理实施规范。
- 1998年2月为了适应第三方认证的需求,英国又制定世界上第一个信息安全管理体系认证标准BS7799-2:1998信息安全管理体系规范, 规定信息安全管理体系要求与信息安全管理控制要求, 是一个组织的全面或部分信息安全管理体系评估的基础。 **(2013年新增知识点)**

2.9.5质量管理

ISO27001今生

- 1999年4月,鉴于信息处理技术在网络和通信领域应用的迅速发展,英国对信息安全管理体系标准进行修订 ,形成BS7799-1:1999、 BS7799-2:1999。
- 1999年10月,英国标准协会(BSI)将BS7799提交国际标准化组织,国际标准化组织已于2001年2月正式将该标准转化成国际标准ISO/IEC17799。
- 2002年9月5日 , BS7799-2:2002发布成为正式标准 , BS7799-2: 2002进行重大改版 , 引入国际上通行的管理模式-过程方法和PDCA持续改进模式。
- 2005 年6 月 , ISO/IEC 17799:2000 经过改版 , 形成新的ISO/IEC 17799:2005 , 同时 , BS7799-2:2002 也终于被ISO 组织所采纳 , 于同年10 月推出ISO/IEC 27001:2005。 **(2013年新增知识点)**
- BSI 官方网站(www.bsi-global.com)上对BS7799 的命名 :
 - □ ISO/IEC 17799:2005 Code of practice for Information Security Management
 - □ ISO/IEC 27001:2005 Information Security. Security techniques. Information security management systems. Requirements

2.9.5质量管理

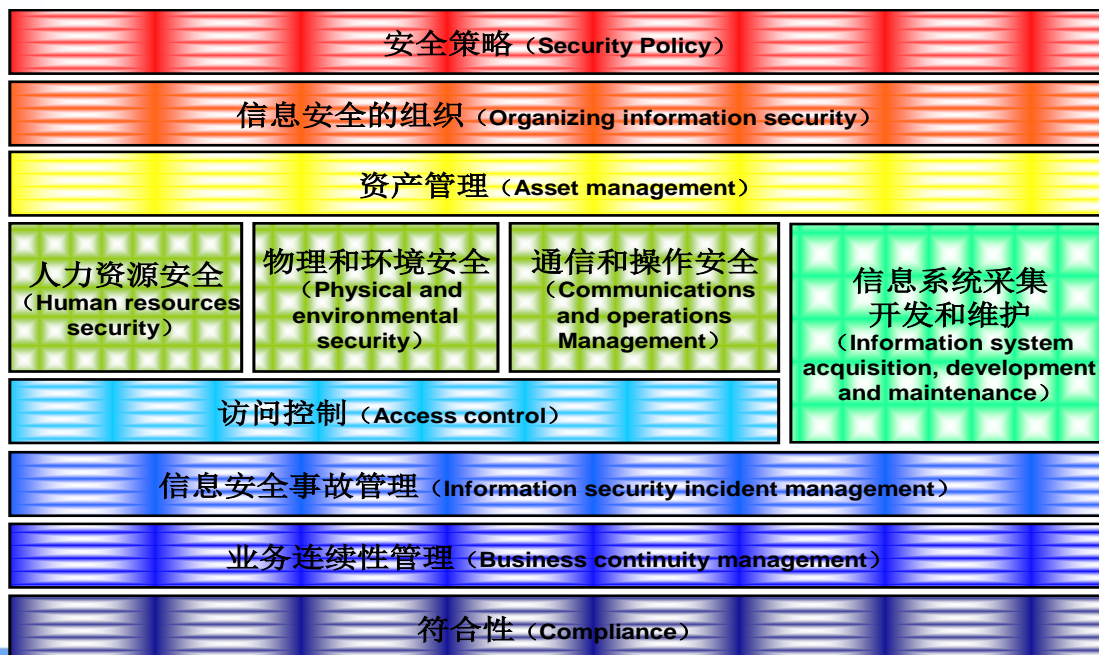
ISO27001发展

- 以ISO/IEC 27001 为核心的信息安全管理标准逐渐发展成为一套完整的标准族，具体包括：
 - **ISO/IEC 27000，基础和术语。**
 - **ISO/IEC 27001，信息安全管理体系要求**，2005 年10 月15 日正式发布（ISO/IEC27001:2005）。
 - **ISO/IEC 27002，信息安全管理体系最佳实践**，2007 年4 月直接由ISO/IEC17799:2005（2005 年6 月15 日正式发布）转换而来。**（2013年新增知识点）**
 - ISO/IEC 27003，ISMS 实施指南。
 - ISO/IEC 27004，信息安全管理体系度量和改进。
 - ISO/IEC 27005，信息安全风险管理指南，以2005年底推出的BS7799-3（基于ISO/IEC 13335-2）为蓝本。

2.9.5质量管理

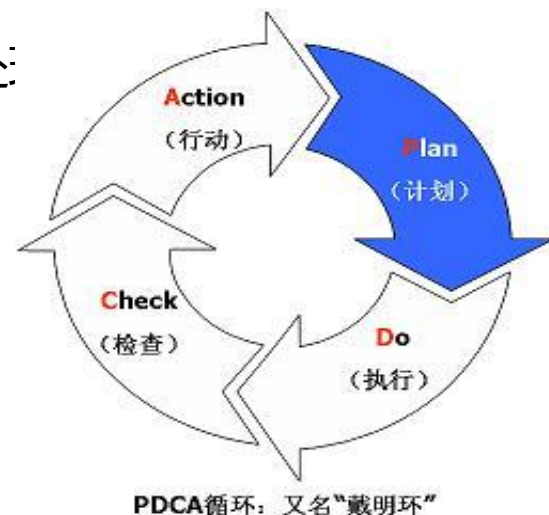
- ISO27002:2005 信息安全管理实施规范，主要是给负责信息安全管理的人员作为参考文档使用，从而在他们的机构内部实施和维护信息安全；
- ISO27001:2005 信息安全管理规范，详细说明建立、实施和维护信息安全管理系统的要求，指出实施组织需要通过风险评估来鉴定最适宜的控制对象，并对自己的需求采取适当的控制。

(2013年新增知识点)



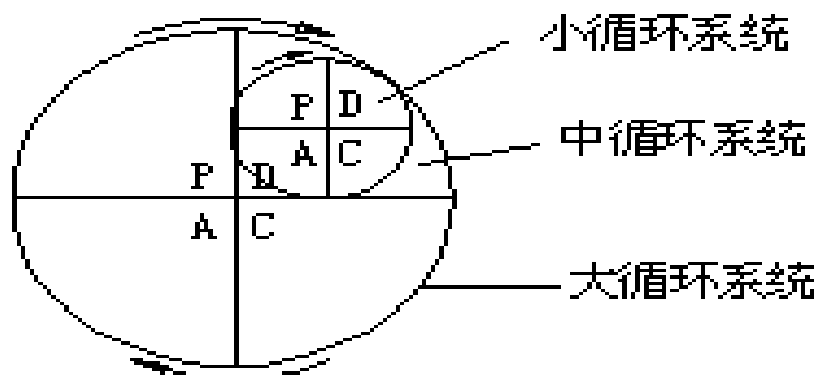
2.9.5质量管理

- PDCA (Plan、Do、Check 和Act) 是管理学惯用的一个过程模型，最早是由休哈特 (WalterShewhart) 于19 世纪30 年代构想的，后来被戴明 (Edwards Deming) 采纳、宣传并运用于持续改善产品质量的过程当中。
 - 1、P (Plan) --计划，确定方针和目标，确定活动计划；
 - 2、D (Do) --执行，实地去做，实现计划中的内容；
 - 3、C (Check) --检查，总结执行计划的结果，注意效果，找出问题；
 - 4、A (Action) --行动，对总结检查的结果进行处理：成功的经验加以肯定并适当推广、标准化；失败的教训加以总结，以免重现，未解决的问题放到下一个PDCA循环。**(2013年新增知识点)**



2.9.5质量管理

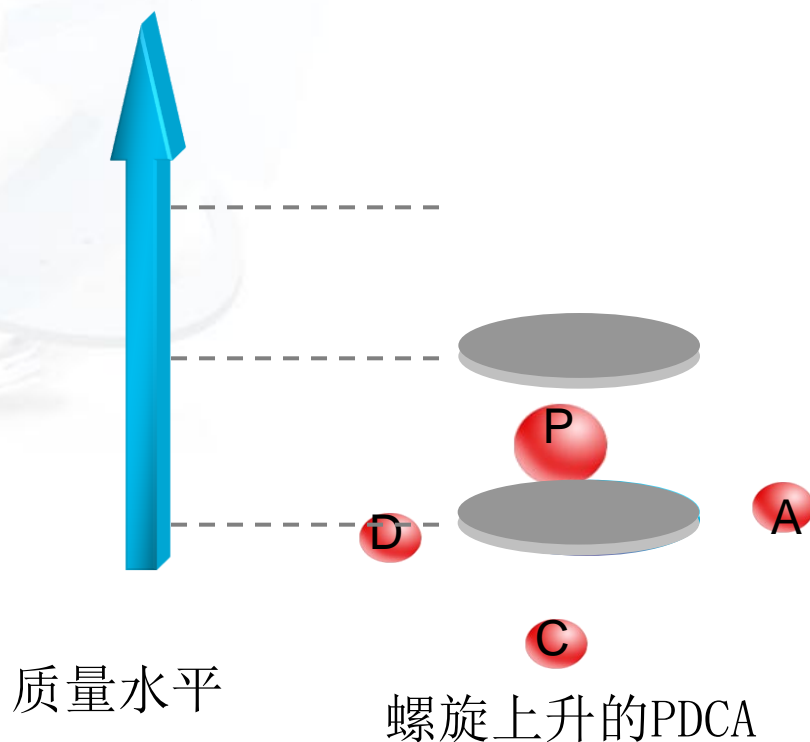
- 大环套小环，小环保大环，推动大循环 **(2013年新增知识点)**
 - PDCA循环作为质量管理的基本方法，不仅适用于整个工程项目，也适用于整个企业和企业内的科室、工段、班组以至个人。各级部门根据企业的方针目标，都有自己的PDCA循环，层层循环，形成大环套小环，小环里面又套更小的环。大环是小环的母体和依据，小环是大环的分解和保证。各级部门的小环都围绕着企业的总目标朝着同一方向转动。通过循环把企业上下或工程项目的各项工作有机地联系起来，彼此协同，互相促进。以上特点。



2.9.5质量管理

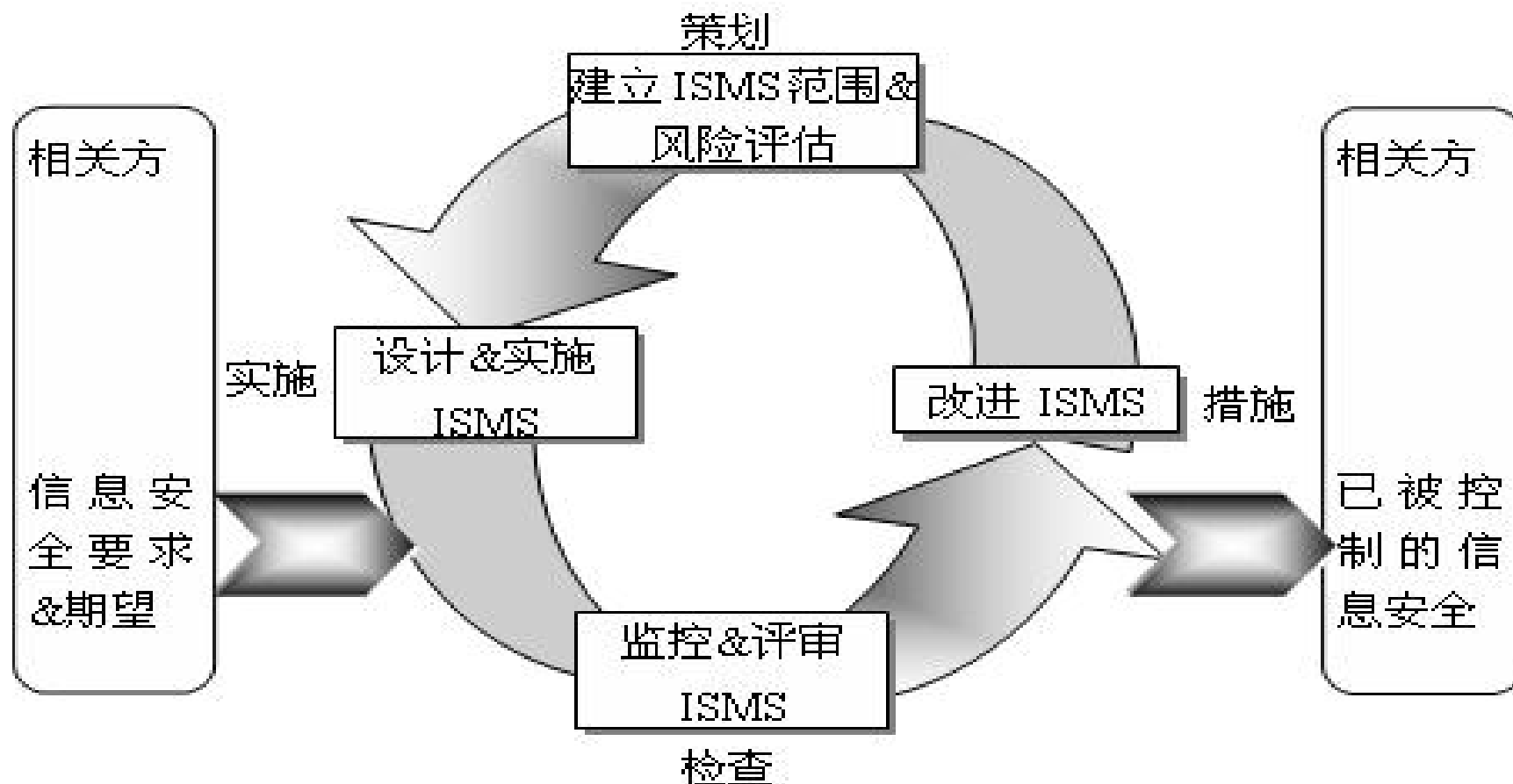
- 不断前进、不断提高 **(2013年新增知识点)**

PDCA循环就像爬楼梯一样，一个循环运转结束，生产的质量就会提高一步，然后再制定下一个循环，再运转、再提高，不断前进，不断提高，是一个螺旋式上升的过程。



2.9.5质量管理

PDCA和ISMS的结合



2.3.1 IT治理最佳实践

IT治理和管理框架

- **COBIT5**：由ISACA制定，通过提供一个框架为IT治理提供支持以确保：IT与各项业务保持一致，IT能够促进业务开展并使效益最大化，IT资源被负责任地使用，IT风险得到妥善管理。COBIT提供的工具可用于评估和衡量组织中37个IT流程的性能。2012年5月发布5.0版本。（注：2013年变化知识点）
- **ISO/IEC 27001 (ISO 27001)系列标准**：属于一组最佳做法，可向各组织提供实施和维护信息安全程序方面的指导。ISO 27001最初作为英国标准7799 (BS7799)在英国 (UK)公布，现已成为该行业的公认标准。（注：第五章“信息安全管理体系 (ISMS)”知识点，2013年新增知识点）
- **ITIL**：由英国商务部(OGC)与IT服务管理论坛联合制定，此框架详细描述了关于如何实现成功的IT运营服务管理的实用信息。2008年发布3.0版本

2.3.2 IT治理/战略委员会

- **IT治理/战略委员会(IT Governing/Strategy Committee)**是业界最佳实践，协助董事会实施其IT治理职责时，提供战略建议，关注IT价值、风险和绩效，IT治理与企业治理融合的机制。 **(2013年变化知识点)**
- IT战略委员会是董事会实施其IT治理目标的重要机制，由董事会成员及非董事会成员（专家）组成，协助董事会治理和监督企业的IT相关事务。
- IT战略委员会应保证在组织中以结构化的方式实施IT治理，董事会可以获得足够的信息实现IT治理的最终目标。
- 对比：组织在执行层设立IT督导委员会（IT Steering Committee)处理整个组织层面的IT事务。应当深入理解IT战略层和指导层的职责。

2.9.7 绩效优化

- 绩效优化的工具COBIT管理指南：满足IT经理进行绩效评价的需求而设计的，为IT的**37个主要流程**定义关键成功要素、关键目标指标、关键绩效指标和成熟度模型。**(2013年变化知识点)**

管理指南的重要内容：

- 关键成功要素 (CSF)
- 关键目标指标 (KGI)
- 关键绩效指标 (KPI)
- 成熟度模型



管理指南要回答的问题：

- 成本与效益——我们究竟应该走多远，成本与利润比例是否合适？
- 绩效评价——对于好的绩效的度量指标是什么？
- IT控制环境——什么是重要点？关键成功要素是什么？
- 意识——不能达到我们的目标的风险是什么？
- 基准测量——他人在做什么？我们应该怎样测量和比较？

2.12.10 计划演练

- **ISACA-COBIT标准为与业务相关的IT控制提供指引 (2013年变化知识点)**
- US National Institute of Standards and Technology (NIST) 美国国家标准与技术研究所
- US Federal Financial Institutions Examination Council (FFIEC)—美国联邦金融机构监管委员会
- US Federal Reserve Board(FRB)—美国联邦储备委员会
- **US Health and Human Services (HHS) —美国卫生和人员服务署制定的HIPPA (美国健康保险流通与责任法案) 标准描述管理医疗信息的要求 (2013年变化知识点)**
- US Federal Energy Regulatory Commission(FERC)--美国联邦能源监管委员会

2.2公司治理

- 必须通过公司治理实践促进组织内部伦理问题的处理、决策的制定以及总体实践。公司治理已被定义为“引导和控制商业公司的系统”。具体来说，**公司治理是指一系列组织的管理人员应该承担的职责和采取的做法，用以指明战略方向，从而确保实现目标、恰当解决风险并合理利用组织资源。**
- 世界经济合作与发展组织（OECD）指出：“公司治理包括组织中管理层、董事会、股东和其他利益相关方之间的一系列关系，它为制定公司目标、确定实现目标和监督绩效的方式提供了框架。良好的公司治理应当能为董事会和管理层提供适当的动力，以促使其追求符合公司及股东利益的目标，并实施有效监督。”
- 关于公共治理，OECD规定：“优质有效的公共治理有助于巩固民主和人权、促进经济繁荣和社会凝聚力、减少贫困、加强环境保护和自然资源的可持续使用以及坚定人们对政府和公共管理部门的信心。” **（2013年删除内容）**

2.2公司治理

- 作为本框架的一部分，还**应建立管理与报告业务风险的机制**。要求组织**应具备一个内部控制系统**，以便在探索用于改善业务的富有创新意义的新方法时能够监控风险。同时，此框架也是**保护利益相关者的平台，因为它定义董事会的责任**。这样，股东、投资者以及其他利益相关者的职责便可分别划定，同时还拥有了一个恰当的架构，以便在清晰的框架内作出他们的投资决定。这样，一方面**需要利用各种可能的机会为利益相关者实现增值**，另一方面又**需要保证组织的运营不超出相关法规要求和社会责任的约束**，因此公司治理便会试图在这两个互相冲突的目标之间找到平衡点。考虑到社会责任在公司治理中的重要性，国际标准化组织（ISO）已开始制定国际标准（ISO 26000），从而为社会责任（SR）提供非强制性的准则。**（2013年删除内容）**

2.3.4信息安全治理

➤有效的信息安全治理

·企业治理是董事会和高级管理层为提供战略方针所实行的一系列职责和实务，以确保实现目标、适当地管理风险及合理使用企业资源。 **(2013年删除内容)**

·业务战略方针通过是通过业务目的和目标来明确，信息安全必须支持业务活动向企业交付的价值。

·信息安全治理是企业治理的一部分，企业治理为安全活动提供战略方针并确保其目标的实现，信息安全治理则确保能适当地管理信息安全风险并合理使用企业信息资源。



第三章信息系统的购置、开发与实施

➤ 增加内容

3.2 业务实现

3.5.2 传统的SDLC各阶段描述-- Phase 4B—配置Configuration

3.6.5 电子邮件

3.6.6 POS系统

3.6.7 电子银行

➤ 变化内容

3.3.6 项目中的团队及个人角色和职责--质量保证人员 (QA)

3.12.4 ISO15504

第三章信息系统的购置、开发与实施

➤ 删除内容

3.4 项目管理实务

3.6.1 电子商务

3.6.7 电子银行

3.6.20 供应链管理

3.8.5 系统软件的获取

3.11.1 业务流程再造和流程变更项目

3.12 应用控制

第三章信息系统的购置、开发与实施

➤ **删除小节和全部内容**

~~2012 3.4.3 项目管理的一般事务 (2013年删除)~~

~~2012 3.6.13 综合客户文件 (2013年删除)~~

~~2012 3.6.14 办公自动化 (2013年删除)~~

~~2012 3.7 其他的软件项目组织形式 (2013年删除)~~

~~2012 3.8.1 面向数据的系统开发 (2013年删除)~~

~~2012 3.9.7 系统软件变更控制流程 (2013年删除)~~

~~2012-3.13.1 输入控制/源头控制~~

~~联机系统或数据库系统中的批输入完整性 (2013年删除)~~

3.2 业务实现

项目的业务实现是综合考虑**成本、质量、速度、可靠性和可信性**等主要因素的折衷结果。战略制定者需进行全面的研究，评估哪些因素“适合”或“略胜一筹”，然后再将这些因素同可用于完成和维护系统的服务的优势、劣势、竞争力进行比较。

大多数大型组织使用结构化项目管理原则以支持其信息系统环境的变更。作为起点，信息系统审计师应理解业务如何定义与开发相关的项目的价值或投资回报率（ROI）。如果公司不能持续地满足其ROI目标，可能表明在其系统开发生命周期（SDLC）和相关的项目管理实践中存在弱点。（2013年新增知识点）

3.5.2 传统的SDLC各阶段描述

➤ Phase 4B—配置 (Configuration) (注：2013年新增知识点)

系统配置，与SDLC关联，包括：定义，跟踪和控制购买的系统中的变更以满足业务的需要。对ERP系统，任务经常涉及配置表的修改和部分开发，主要确保ERP系统与现有IT环境集成。系统配置通过变更管理政策和流程支持，定义：

- 角色和责任
- 基于业务风险对所有变更分类和排优先顺序
- 评估变更的影响
- 业务流程和IT的所有者授权和批准所有变更
- 跟踪和标明变更状态
- **对数据完整性的影响（例如对数据文件的变更处于系统和应用控制而不是由直接用户干预）**

3.6.5 电子邮件

用户向互联网上或封闭网络中的某人发送电子邮件时, 该邮件通常需要穿过一系列网络才能到达接收方。这些网络可能使用不同的电子邮件格式。网关要执行的任务是将电子邮件格式从一个网络转换为另一个网络, 从而使邮件可以通过所有网络。电子邮件由二进制数据组成, 通常采用 ASCII 文本格式。ASCII 是一种允许所有计算机读取文本的标准, 而无论计算机的操作系统或硬件如何。ASCII 码描述用户在其计算机屏幕上看到的字符。

➤ 电子邮件的安全问题

电子邮件涉及到以下安全问题：

- **网络钓鱼 (Phishing) 和鱼叉式网络钓鱼 (spear phishing) 是电子的社交工程攻击, 开始变得复杂, 只能通过安全意识教育培训应对。(注：结合第五章“5.2.10 计算机犯罪及暴露风险”知识点。(2013年新增知识点)**

3.6.6 POS系统

- POS系统标准的进一步信息可以在 www.pcisecuritystandards.org 获得，定义支付卡行业(PCI)数据安全标准（DSS）；在 www.emvco.com 获得，对使用嵌入式微处理芯片智能卡定义标准。 **（2013年新增知识点）**

3.6.7电子银行

- 8. 电子银行交易、记录、信息的数据完整性
- 9. 为电子银行交易建立清晰的审计轨迹
- 10. 确保重要银行信息的机密性
 - 法律与信誉风险管理：
- 11. 电子银行服务的相应泄漏问题
- 12. 客户信息的隐私权
- 13. 制定容量、业务连续性与偶发事件相关计划，以确保电子银行系统与服务的可用性
- 14. 事故应对计划
- 15. 遵守银行业监管规定（例如巴塞尔Basel Accords III）
(2013年新增知识点)

3.3.6 项目中的团队及个人角色和职责

- 质量保证人员 (QA) : 在各阶段期间以及各阶段结束时审查结果和交付成果的人员, 还负责确认操作是否符合要求。他们的目标是通过衡量项目人员对组织软件开发生命周期 (SDLC) 的遵守情况, 来确保项目质量; 提出有关偏差的建议; 发生偏差时, 针对流程的改善或控制点的增加提出建议。审查点位置的设定取决于使用的SDLC方法、系统的结构和大小以及潜在偏差的影响。此外, 还应重视审查基于流程的相应活动, 这些活动可能与生命周期中特定阶段的项目管理有关, 也可能与此阶段中特定软件工程设计流程的使用有关。这样的重视对于如期完成项目且不超出预算至关重要, 而对于达到指定的软件过程成熟度也至关重要 (请参阅本章3.11.4, ISO/IEC 15504, 2013年更新知识点)。
- QA功能的具体目标包括:
 - 确保在修订、评估和传播, 应用标准、管理准则和流程过程中所有相关方积极配合参与

3.12.4 ISO15504 (2013年变化内容)

ISO/IEC 15504是标准族（一系列文档）为流程改善，基准标杆和评估提供指导。它包括详细的指导，可以被杠杆化创建企业最佳实践。在每个流程中包括一般事务，形式化指导和流程能力的绩效评估指标（注:例如KPI和KGI）。

能力维度提供对流程的度量以满足组织目前或计划的流程的业务目标。流程能力以流程属性表达，如**exhibit 3.28**显示。流程的能力水平基于按照ISO/IEC 15504-2:2003定义的特定流程属性确定。

评价尺度涉及如下6个能力水平：

- 级别0未完成—流程没有实施或失败以致无法获得流程目标。在本级别，没有流程目标系统化的获得的证据。
- 级别1已执行—实施的流程获得其流程目标。

3.12.4 ISO15504 (2013年变化内容)

- 级别2受管理—前述已执行级别流程目前被实施，以受管理方式（计划，监控和调整）并且其产出产品被恰当地建立，控制和维护。
- 级别3已建立—前述受管理级别流程目前使用定义的流程实施，有能力获得其流程产出。
- 级别4可预测—前述已建立级别流程目前在定义的界限中获得其流程产出。
- 级别5优化—前述可预测级别流程持续改善以满足与目前和未来计划的相关业务目标。

3.4 项目管理实务

- 项目的许多元素需要始终考虑。
- 项目管理应关注三个关键交织元素：**交付成果、持续时间和预算**。其关系非常复杂，但示例以一种简明扼要的方式对该关系进行了说明。**项目持续时间和预算必须与交付成果的性质和特征相称。一般来说，对交付成果的要求越高，持续时间就越长，预算也越高。**
- **在时间和资源管理时也要考虑的一个重要交付成果因素是交付成果的质量。交付成果质量的参数可由项目督导委员会或项目发起人明确指定，也可由项目经理从用户管理推导给出。在这两种情况下，项目经理必须清楚并记录项目督导委员会、发起人和用户对交付成果的质量期望。（2013年删除内容）**

3.6.1 电子商务

➤ 电子商务模型

- 消费者对政府 (Customer-to-Government , C-to-G)关系:尚未兴起。然而,随着企业对消费者以及企业对政府两类关系的发展,政府可能会将电子交互方式扩展到福利金支付和自报税申报等领域。 (2013年删除内容)
- 交易对交易 (Exchange-to-Exchange , X-to-X)关系:这是多个B-to-B关系/市场间的连接。X-to-X是超越B-to-B或B-to-SB的下一个合理步骤。组织能够以有竞争力的价格购买到用品/产品。 (2013年删除内容)

3.6.7 电子银行

银行组织已为消费者和企业提供了多年的远程电子服务。电子资金转移(EFT)系统(包括小额支付和企业现金管理系统)、公用自动提款机和零售帐户管理系统已遍布全球。

在现有银行组织与新的市场参与者之间不断出现的技术创新和竞争为批发零售银行客户提供了范围更为广泛的电子银行产品和服务。但是,随着全球越来越多的用户将互联网作为银行产品和服务的供应渠道,新的商机应运而生,同时也带来了新的风险。

与银行活动相关的主要风险有策略、信誉、运营(包括安全性,有时称为交易风险和法律风险)、信用、价格、外汇、利率以及流动资金等风险。**电子银行(e-banking)活动不会引起传统银行业务范围内尚未识别的风险,但电子银行会增加和改变其中一些传统风险。核心业务与IT环境紧密相关,因而会影响电子银行的总体风险预测。** **(2013年删除内容)**

1

3.6.7 电子银行

特别是从IS审计师的角度来讲时，主要问题就是**策略、运营和信誉风险，因为其直接关系到对可靠数据流和运营风险的威胁，并且毫无疑问会因电子银行的快速引入和潜在的技术复杂性而得到增强。**

银行应具有风险管理程序，以便能够识别、衡量和监控所面临的技术风险。新技术的风险管理包含三个基本元素：

- **风险管理是董事会和高级管理层的职责。**他们负责制定银行的业务策略以及建立有效的风险管理方法。他们需要具备管理银行使用电子银行业务以及所有相关风险的知识 and 技能。对于银行是否提供电子银行服务以及如何提供该类服务，董事会应做出明确、精明且记录在案的战略性决策。初步决策应包括与处理风险（包括出现在跨边界领域内的风险）相关的具体问责性、政策和控制。董事会应审查、批准和监控对银行的风险概况产生重大影响的电子银行技术相关项目，并确保识别、规划和实施适当的控制。**(2013年删除内容)**

3.6.7 电子银行

- **实施技术是IT高级管理层成员的职责。**他们应具备有效评估电子银行技术和产品所需的技能，并确保这些技术和产品得到合理实施和记录。 (2013年删除内容)
 - **衡量和监控风险是运营管理人员的职责。**他们应具备有效识别、衡量和监控电子银行相关风险所需的技能。董事会应定期收到与所用技术、可能存在的风险以及如何管理这些风险相关的报告。 (2013年删除内容)
- 电子银行所面临的风险管理挑战

电子银行面临着众多的风险管理挑战：

- 在电子银行方面，技术和服务创新的变化速度是史无前例的。目前，银行正面临着在极短的时间内推出新型业务应用程序的竞争压力。这种竞争增加了确保在实施新型电子银行应用程序之前执行充分的策略评估、风险分析和安全审查的管理挑战。

3.6.20 供应链管理

- 不动物品的库存水平明显降低，并且形成了供需之间的自动流动。同时也避免了人工操作（如传真、数据输入、延期和订单不准确）所带来的固有成本和误差。

注：JIT需考虑BCM，日本大地震影响全球半导体相关企业供应链，泰国水灾影响全球硬盘价格，欧洲冰岛火山爆发影响欧亚航空物流。

- 广泛应用于SCM中的EDI并不是一项新技术，但是直到近几年才有很多人负担起与其相关的成本。如今，基于Web且价格便宜的SCM解决方案已经问世，为每个人开启了通向这一领域的大门。但是，商业模式却需要进行重大变革。（
2013年删除内容）

3.8.5 系统软件的获取

- 如果没有进行更新和升级,业务运营可能会遭遇严重阻碍或中断。软件供应商通常会将最新的系统升级或修复程序(旨在减少与安全相关的漏洞)以及其他独立实体或公司(如SANS协会、卡内基梅隆大学软件工程学院(SEI)的CERT或McAfee威胁中心)的最新消息通知给客户。另外,历史软件可能与引入新功能时伴随着的新技术要求不兼容。**(2013年删除内容)**

3.11.1 业务流程再造和流程变更项目

- “业务实际上是指基本业务流程，成功的业务意味着基本业务流程很有效。构成业务的所有其他内容都在丧失其唯一性，而变成了一种商品。毫无疑问，有效地组织过程正在演变成为一项世界性的董事会议程。”（Nagaraj,N.S.;*Business Process Management ——An Emerging Trend*, Infosys/SETLabs, India, 2001) (2013年删除内容)
- 业务流程可以看成是一种社会技术系统，也就是说，“一组以生成客户导向型输出的特定输入和增值任务为特征的相互关联的工作活动。业务流程由跨越多个部门或职能的横向工作流程组成。”（Seth, Vikram; William King; *Organizational Transformation through Business Process Reengineering*, Prentice Hall, USA, 1998) (2013年删除内容)

3.12 应用控制

应用控制涉及与每个基于计算机的应用程序系统相关的事务和数据；因此，应用控制特定于各个应用。应用控制（可以是手动的或编程的）的目标是确保记录完整和准确以及在其中所做的输入有效。 **(2013年删除内容)**

应用控制是对输入功能、处理功能和输出功能的控制。

应用控制包括用于确保以下方面的方法：

- 仅在计算机系统中输入和更新完整、准确和有效的数据
- 处理操作完成正确任务
- 处理结果满足预期要求
- 维护数据

应用控制可以包含对不正确、丢失或异常数据进行编辑测试、求和、对账以及识别和报告。自动控制应该伴随着手动程序一起使用，以确保正确探查异常情况。

3.4.3 项目管理的一般事务 (~~2013年删除~~)

- 项目管理软件的应用
 - 一般性项目管理采用自动化技术，**处理建议和成本估算以及根据推荐的任务事项来监控、预测和报告完成情况**。其中的许多技术作为决策支持系统(DSS)提供，用于规划和控制项目资源。这些自动化技术可以执行许多功能，从人事要求到预算系统。这些**自动化系统通常融合PERT和CPM技术**。
- 文档
 - 自动化文档工具可**处理系统和程序文档的制作、验证和维护**。这些工具通常**允许用户输入程序和系统参数，不必使用专门的文字处理功能**。该软件包将**根据用户的输入生成程序注释和流程图**。
- 办公自动化
 - 可减少员工参与为满足政策要求和在员工会议上执行通信和记录功能所需的任务。最有效的办公自动化功能是电子邮件、语音信息系统、时间自动化工具（如电子日历和日期提醒）、自动库管理系统、文件归档与检索系统等。

3.6.13 综合客户文件 (~~2013年删除~~)

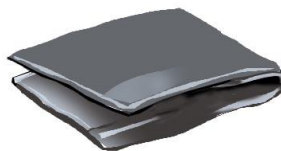
➤ 定义

- 综合客户文件提供客户与组织之间的所有业务关系情况。有助于组织进行客户分析和市场营销。
- 集成的银行客户文件，包括客户的贷款数据、支票账户、存款账户以及所有的存款证明等信息。

3.6.14 办公自动化 (~~2013年删除~~)

➤ 定义

- 很多组织的办公室都使用了大量的电子设备和技术来帮助进行业务处理。字处理、自动化的电子表格和电子邮件每天都在很多办公室里使用，局域网将本地办公室的计算机连接在一起，以便于这些技术的使用。
- 办公自动化设备和网络可能会包含一定的敏感数据，但是常常缺乏必要的访问控制和安全措施。



3.6.16 协同处理系统 (~~2013年删除~~)

➤ 定义

- 协作处理系统被分为几个部分，不同的部分可以在不同的独立计算机设备上运行。
- 系统首先将要处理的问题分成适合在不同环境下处理的一个个单元，并在这些单元之间沟通处理结果，最终对总的问题产生一个整体的解决方案。
- 这种系统必须被设计成最小组成部分并保持各组成部分之间通讯的完整性，以对每一个问题单元分配最适当的处理设备。

3.7 其他的软件项目组织形式 (~~2013年删除~~)

根据不同需要（如交付时间、系统规模、要求的清晰程度和所用技术的成熟度）组织软件项目有不同的方法。 IS审计师必须了解，传统方法中概括的基本步骤在某种程度中存在于几乎所有软件开发项目中。但是，步骤的顺序、重复的次数、步骤持续时间和所采用的方式对于不同的项目却大相径庭。另外一个不争的事实是，由于系统的复杂性已增加，对于如何最有效地组织软件项目的想法也随着时间的推移而不断进步。

鉴于这些因素，IS审计师可能遇到的其他方法包括：

- **递增式或渐进式开发(Incremental or progressive development)：**
分阶段或分不同版本构建系统，而不是一次开发完后整体交付。 通常分别交付各个版本也属于较重的任务，因此操作时也要划分为独立的子项目。通常的做法是在第一个版本中交付基本的系统架构。后续的版本将在功能、用户范围或使用定位方面对系统进行扩充。

3.7 其他的软件项目组织形式 (~~2013年删除~~)

- **迭代开发(Iterative development)**：这种方法涉及到通过迭代的方式构建系统，而每次迭代后产生的反馈还可有助于对项目计划和软件开发产品进行任何必要的调整。**迭代开发现在普通被认为是最佳的做法。迭代开发被认为是处理当代软件开发项目中复杂性和相关风险问题的最适合方法。**
- 复杂性的来源包括：
 - **现在所开发系统的深度和广度**。例如电子商务、客户关系管理 (CRM)、供应链集成、在线交易处理和在线分析处理
 - **业务变更率**。增加了需求的不稳定性
 - **需要作出各种各样架构方面的决策**。例如，系统应具有图形用户界面 (GUI)还是浏览器界面；使用哪个防火墙；使用哪个Web服务器；是使用应用程序服务器还是其他的集成/控制中间件；使用哪个DBMS;采用哪个通信和数据定义协议；是将系统组织成子系统和模块、类和对象，还是采用组件架构；业务逻辑存在的位置？
 - **常常需要将新系统与旧版系统进行整合**

3.7 其他的软件项目组织形式 (~~2013年删除~~)

- 在迭代式生命周期这个总类别下, 还存在多种变形。包括:
 - **进化式开发(Evolutionary development)**: 通过原型法可构建一个用于引出/验证需求并探究设计问题的工作模型。从安全的角度讲, 原型最终将得到加固, 因此可以直接应用到生产当中, 或者也可以根据从原型中获得的知识为系统重新编码。
 - **螺旋式开发 (Spiral development)**: 开发解决方案时使用一系列原型, 并且都达到详细设计、构建和测试的程度。解决方案从功能有限的最初原型开始得到螺旋式改进, 从而变得越来越全面、越来越精细。**正式的风险分析应在生成各原型之前进行, 并且各个原型 (取决于所完成的迭代) 构成了生成软件开发产品的基础 (包括需求的详细说明、系统设计和测试计划)。**

3.7 其他的软件项目组织形式 (~~2013年删除~~)

- **敏捷开发(Agile development)**：项目被划分为持续时间相对较短且固定的迭代。从最开始的迭代开始，重点就是生成实际的操作功能，但软件版本可能并不与完成的改进保持一致。在早期的步骤中，可采用曳光弹法，即一项功能以与预定的开发方法和架构保持一致的方式开发。此功能将从用户界面开始延伸，通过中间过渡层，最后到达存储的数据，然后循环往复。对预期的架构充满信心后，后期迭代的重点就会转移到尽量提高所交付功能的投资回报率上。

3.8.1 面向数据的系统开发 (~~2013年删除~~)

- DOSD (DATA-ORIENTED SYSTEM DEVELOPMENT) 是一种通过关注数据及其结构来表示软件需求的方法。股票交易所以及一些服务提供商 (如航空公司、电话公司等) 生成的是与时间相关的数据。这些数据将离线提供给一些服务订购者。例如, 股票交易所到股票经纪人再到次级经纪人; 航空公司到各自的旅行社等。这些数据以预知或预先规定的格式呈现, 即能够以CD-ROM形式提供, 也可通过文件传输协议(FTP)以逗号分隔值 (CSV)、ASCII或其他 规定的格式提供下载。用户组织可以开发属于自己的应用程序 (平台变体和开发工具变体), 并可以直接将这些数据用于自己的应用程序中, 以便发行票据或促成与客户之间的股票买卖。**该面向数据的系统开发方法的主要优势是可以消除数据转换误差, 如字符易位、抄写错误、移植错误或转换、抄写和易位。** DOSD通常将与用于应对处理方面问题的另一种开发技术相结合, 便制定出一个适合的业务解决方案。

3.8.1 面向数据的系统开发 (~~2013年删除~~)

- DOSD是一种通过关注数据及其结构来表示软件需求的方法
- 面向数据的开发方法是通过数据和数据结构来表达软件需求的一种开发方法；
- 不像基于传统的SDLC的结构化分析方法，面向数据的开发方法把数据与处理数据的过程加以分离，只考虑数据，不考虑处理数据的过程；
- 这种方法必须与其他开发方法结合起来使用，才能有效地开发出适合的业务解决方案。

3.9.7 系统软件变更控制流程 (~~2013年删除~~)

- 所有测试结果均应在用于生产前由具有技术方面资质的主题存档记录、审查和批准。
- 变更控制流程旨在确保变更经过授权并且处理过程不会因此中断。这就要求IS管理人员和工作人员了解并参与到系统软件变更流程中。变更控制流程应确保影响生产系统的变更进行过合理评估（尤其是安装时所产生的故障的影响），并且保证具有合适的恢复/取消（回滚）流程，从而最大限度地减少安装期间所产生任何故障的影响。例如，要实现变更控制，可以安装配置管理系统，以便在应用针对高风险安全问题的安全补丁时保留之前的OS版本或之前的状态（请参阅第五章“信息资产保护”）。许多情况下，IS管理人员必须应用补丁才能实施供应商提供的解决方案，从而解决影响基于网络和基于主机的系统的安全问题。因此变更控制流程还应确保可能受到变更影响的管理队伍中所有相关成员都收到相应通知，以便在变更前针对变更对各自领域的影响进行评估。

3.11.3 软件能力成熟度模型 (~~2013年删除~~)

➤ 什么是CMM ?

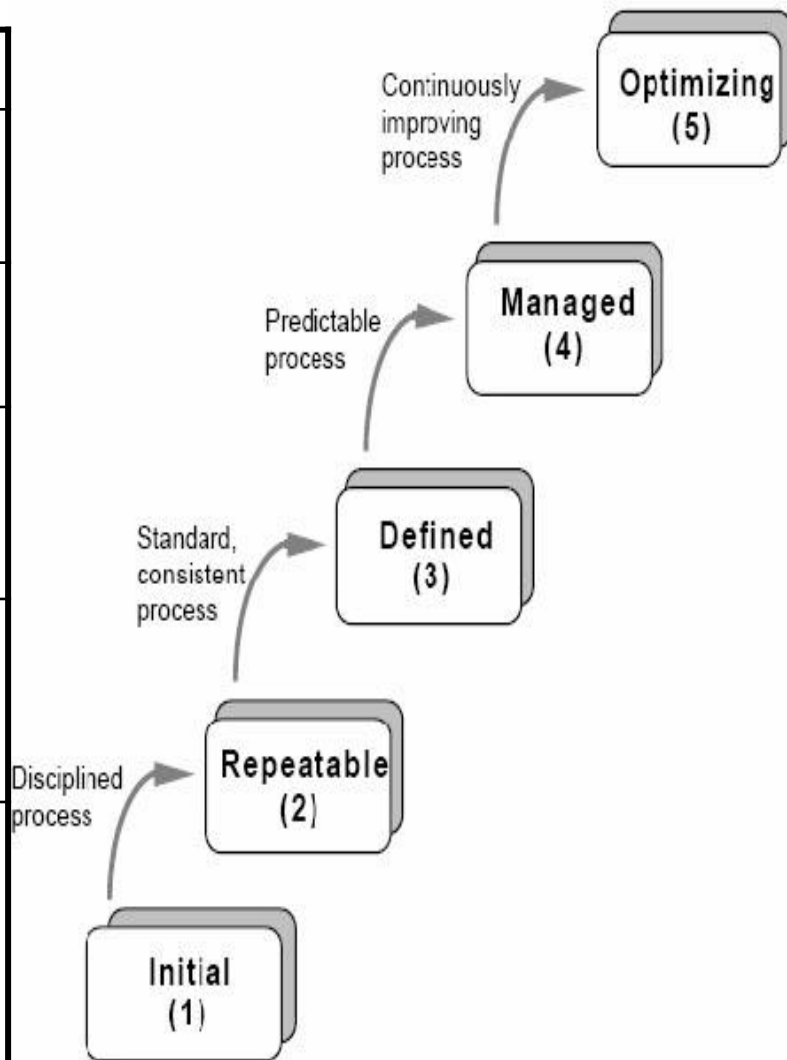
- 1990年由美国卡耐基-梅隆大学软件工程师研究所在政府和行业的资助下提出的软件能力成熟度模型 (CMM)。
- 用于帮助软件组织提高软件开发生命周期的质量，擅长通过提供必须的基本设施防止软件开发超期和超预算的问题。
- CMM是基于5个级别的过程管理准则，有助于帮助软件组织在评估现有的过程成熟度基础上，考虑几个对软件过程质量改善最为关键的问题以选择适合于自身的过程改进策略，使得组织可以通过有限的活动以稳固地提升软件过程的能力。

3.11.3 软件能力成熟度模型 (~~2013年删除~~)

- CMM
- 核心：把软件开发过程视为一个过程，并根据这一原则对软件开发和维护进行过程监控和研究，以使其更加科学化、标准化，使企业能够更好地实现商业目标。
- 目的：评估软件供应商的能力→帮助软件企业管理和改进软件过程质量
- 好处：
 - 指导软件组织提高软件开发管理能力
 - 降低软件承包商和采购者的风险
 - 评估软件承包商的软件开发管理能力
 - 帮助软件组织识别有效过程和关键实践
 - 增加软件组织的国际竞争能力

3.11.3 软件能力成熟度模型 (~~2013年删除~~)

等级	特点
优化级	软件过程的量化反馈和新思想、技术促进过程改进
已管理级	对软件过程和产品质量有定量的理解和控制
已定义级	将软件管理和过程文档化、标准化,形成所有项目都使用的组织标准软件过程
可重复级	建立基本项目管理,能够利用以前类似项目的成功
初始级	软件过程混乱无序,几乎没有过程定义,成功依靠个人才能和经验,管理是反应式



3.11.3 软件能力成熟度模型 (~~2013年删除~~)

➤ CMM 的5个级别：

- 初始级、可重复级、已定义级、已管理级、优化级。

➤ 各级别要点：

- 第二级的关键之处是建立基本的项目管理控制，需求管理、软件项目计划、软件项目的跟踪和监督、软件外包管理、软件质量保证和软件状态管理。
- 第三级的关键之处是既关注项目问题，也关注组织问题。组织建立使高效率软件工程制度化的基本架构和跨项目的管理集成化的软件管理、软件产品化机制、项目组的内部协调和对出现错误的复查。
- 第四级的关键之处是对软件开发过程和软件产品都有一个定量的理解，强调定量的过程管理和软件质量管理。
- 第五级的关键点强调不论组织还是项目必须追求持续的、可度量的过程改进，包括缺陷预防、技术更新管理和流程改造管理。

3.13.1 输入控制/源头控制

~~联机系统或数据库系统中的批输入完整性 (2013年删除)~~

删除内容

- 通过限制时段、终端及人员输入等方式来建立批控制。
- 监督人应首先检查联机批输入，然后提交给系统进行处理。

第四章信息系统的操作、维护与支持

➤ 增加内容

4.2.2 IT服务管理

4.2.5 支持与服务台

4.4.8 软件许可

➤ 删除内容

4.5.6 OSI模型在网络体系结构中的应用

客户机-服务器技术--解决方案、解决方案

第四章信息系统的操作、维护与支持

➤ 删除/变动小节内标题/但内容不变

4.2.3 架构运行（目录删除内部标题）

4.3.1 计算机硬件组成和架构—内存卡闪存盘，RFID（目录删除内部标题）

4.5.6 OSI在网络架构的应用—局域网，广域网，无线网，公共“全球”互联网架构，网络管理和控制（目录删除内部标题）

4.7.6 备份和恢复—备份安排（目录删除内部标题）

4.2.2 IT服务管理

- 当IS部门的职能被外包给第三方时, IS审计师应确保为涵盖所有必要领域且提供完全审计权限的独立审计报告制定相关条款。
- 管理层使用多种技术, 包括问卷 (questionnaires), 现场检查 (onsite visits), 独立第三方鉴证报告 (independent third-party assurance report), 例如 : SSAE16 SOC1 report , AT-101 SOC 2 and SOC 3 reports (formerly SAS 70) 审计 (**2013年新增知识点**)。
注 : 第一章 “专项审计” 知识点 , 第二章 “外包管理” 、 “对外包服务商审计”

4.2.5 支持与服务台

- 当启动服务台工单/呼叫 (ticket/call) 时触发支持，基于故障的复杂性升级，要求专业人员解决该问题。 **(2013年新增知识点)**
- 服务台的宗旨是为用户提供服务。服务台人员必须确保发生的所有硬件和软件事件都被全面记录并根据管理人员建立的优先级进行升级。在不同的组织内，服务台的职能会有所差异。但是，服务台的基本职能是执行如下任务：
 - 记录产生于用户的事件和启动问题解决方案。
 - 确定项目的优先级，然后将其提交到相应到IT人员，并且可根据需要将其上报到IT管理人员。
 - 跟踪未解决的事件。
 - 关闭未解决的事件，通知相应职能部门关闭产生自用户的事件。

4.4.8 软件许可

- 定期从LAN中或直接地扫描用户PC,以确保PC上没有加载未经授权的软件副本,通过比较实际安装软件和授权批准的软件“白名单” **(2013年新增知识点)**



4.5.6 OSI模型在网络体系结构中的应用

(2013年删除内容)

客户机-服务器技术--业务挑战

- 要有效管理和支持这些环境，IT人员需要解决**客户端/服务器环境的快速发展和复杂性带来的挑战**。
- 关键任务应用程序的日益复杂使越来越多的公司开始尝试客户端/服务器平台。
- 公司正在经历更多将应用程序的更改整合到现有网络系统中的问题。
- 对客户端/服务器技术人员的需求导致频繁的人员流动，增加了雇佣和培训的成本，对公司的预算造成了较大的影响。
- 办事处很多且合并/收购策略非常积极的公司却没有中央客户端/服务器系统。此外，多个办事处需要多种操作系统的支持，这为正确管理和支持系统增添了难度。

4.5.6 OSI模型在网络体系结构中的应用

(2013年删除内容)

客户机-服务器技术--解决方案

要应对业务挑战，管理人员必须解决COBIT的交付与支持 (DS)领域的问题。该域与所需服务的实际交付相关，其中包括**服务交付、安全性与连续性管理、用户服务支持以及数据和操作设备管理**。它通常解决以下管理问题：

- 所要交付的IT服务是否符合业务优先级？
- 是否已经优化IT成本？
- 全体员工是否能够高效安全地使用IT系统？
- 在信息安全方面是否具有足够的机密性、完整性和可用性？

第五章信息资产的保护

➤ 增加内容

5.2.1 信息安全管理组成—信息安全管理体系

5.3.6 授权问题—使用手持设备

5.4.4 互联网威胁和安全—入侵检测系统

➤ 删除/变动小节内标题/但内容不变

5.3.5 身份识别和认证—登录ID和口令，生物认证系统（目录删除内部标题）

5.3.6 授权问题—远程访问安全，审计系统访问日志（目录删除内部标题）

5.4.4 互联网威胁和安全—防火墙类型，入侵检测系统（目录删除内部标题）

5.5.4 调查技术—计算机犯罪司法调查（目录删除内部标题）

2013年CISA复习备考索引

- 2013年6月,9月,12月CISA考试报名,考试,认证,CPE维持和备考要点：
<http://www.cncisa.com/read-hm-tid-20504.html>
- 2013年CISA新版在线考试报名流程详解
<http://www.cncisa.com/read-hm-tid-8166.html>
- 2012年12月8日CISA考试通过心得
<http://www.cncisa.com/read-hm-tid-20917.html>
- 2013版CISA国际注册信息系统审计师认证手册
<http://www.cncisa.com/read-hm-tid-9753.html>
- 2013年新CISA证书申请流程指导，附申请文件模板
<http://www.cncisa.com/read-hm-tid-17186.html>
- CISA认证申请与CPE维持
<http://www.cncisa.com/thread-hm-fid-45.html>
- **CISA Review Manual 2013英文版本建议加深学习资源SUGGESTED RESOURCES FOR FURTHER STUDY（汇哲索取）**

2013年CISA复习备考资料

- **100%全面梳理CISA认证考试讲义**

点评：CISA目前国内讲义均为多年前原始版本更新，其中不少知识点涉及面不全，重点考点较少、非考点出现较多，经过20年CISA专业经验讲师历时2个月全面梳理100%全新考试讲义（突出考点、强化复习、对于无时间看书的学员适用于看讲义，确保通过考试）

- **全面梳理2013年CISA认证考试中文书**

点评：2013年CISA认证考试中文书根据CISA Review Manual 2013英文版本全面整理，优化历年存在的问题，全面帮助学员理解CISA考试内容和所有知识点，为学员学习CISA打下基础。

以上版本发布时间为2013年3月20日将全面发布给汇哲培训学员！

2013年CISA复习备考资料

- **2013年CISA认证考试中英语对照题目集红宝书第四版**

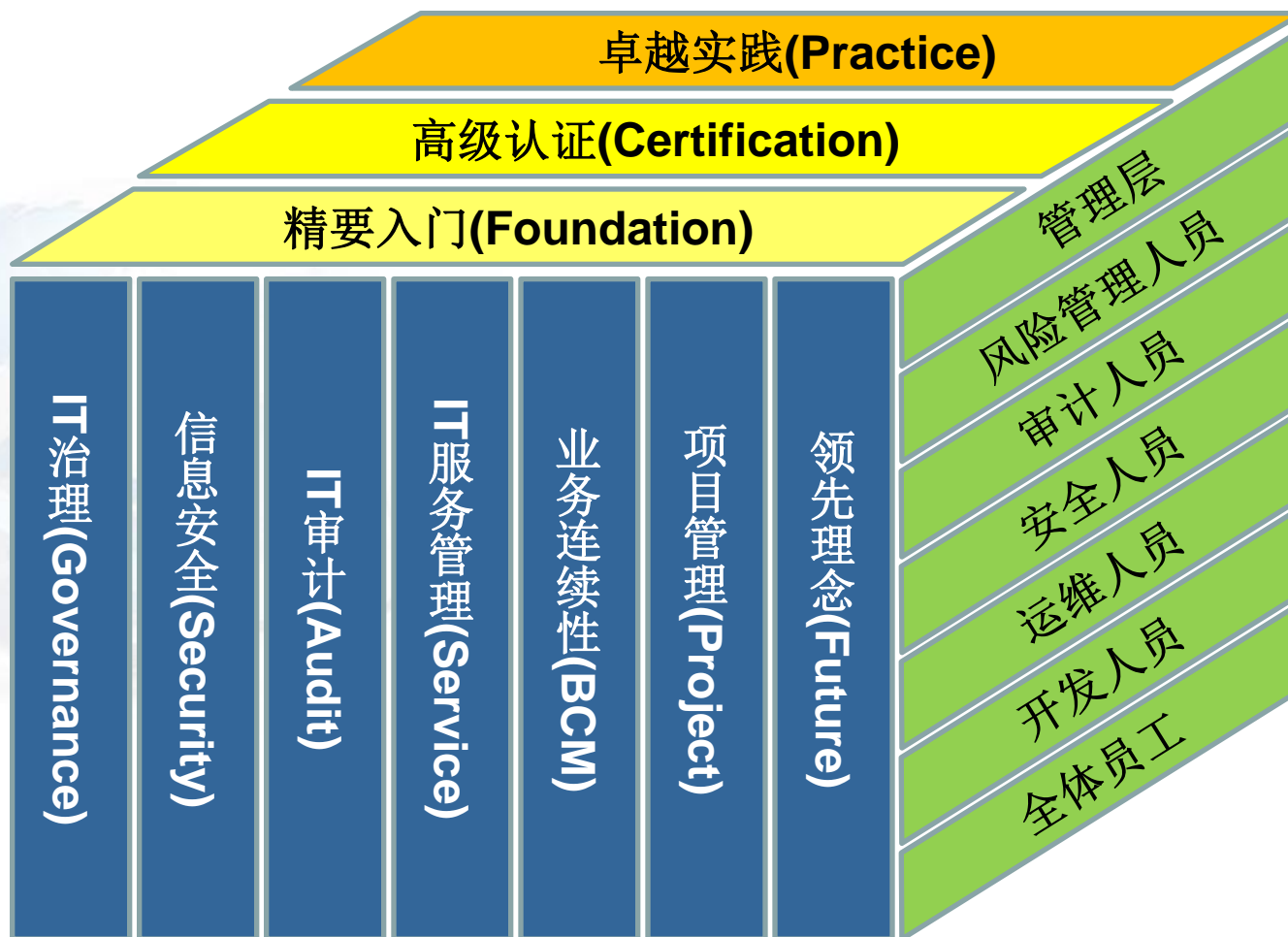
点评：2013年CISA认证考试中英语对照题目集红宝书第四版根据CISA Review Questions, Answers & Explanations Manual 2013 ; CISA Review Questions, Answers & Explanations Manual 2013 Supplement ; CISA Review Questions, Answers & Explanations Manual 2012整理而成；以帮助学员熟悉CISA所涉及所有题目类型，提高考试通过水平为目得！

- **全面梳理CISA认证考试历年出现题目手册**

点评：CISA认证考试历年出现题目手册是根据历年CISA考试中常出现的题目进行整理和收集而成以帮助和分析题目类型，适用于所有参加考试的学员！

以上版本发布时间为2013年3月20日将全面发布给汇哲培训学员！

汇哲培训服务三维体系



联系我们

网址：www.spisec.com

赞助：www.cncisa.org www.cncisa.com

商城：<http://spisec.taobao.com/>

地址：上海黄浦区陆家浜路1332号南开大厦1508

邮编：200011

电话：021-33663299

邮箱：huizhe@spisec.com

在线咨询：Q 2443445995 ; Q 1109871256