汇哲科技 SPISEC

SPISEC | 国内最可靠的培训服务机构

2014年CISA考试知识点变化总结讲义

汇哲科技原创

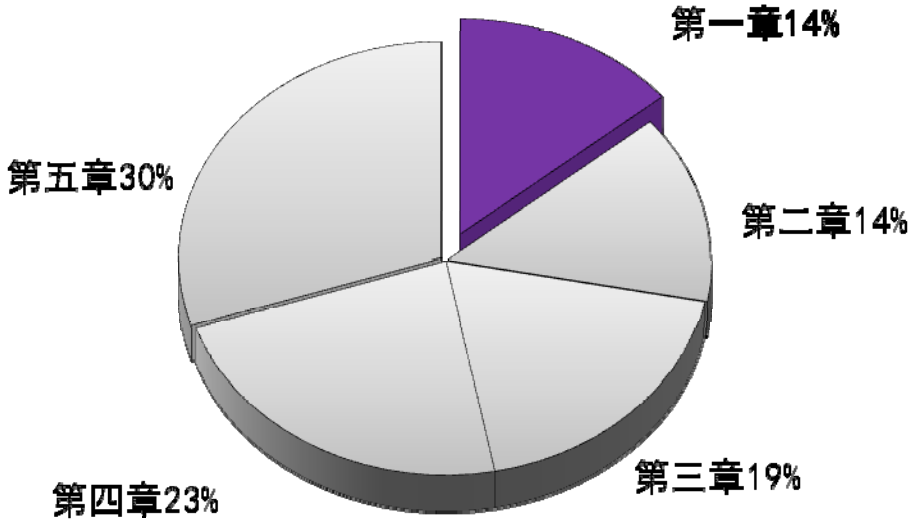
关于我们

- 上海汇哲信息科技有限公司（简称“汇哲”或“SPISEC”），总部设立在上海；其前身为内众多学习群体的持久赞助者；长年致力于信息安全，IT治理，IT审计，IT风险管理，业务连续性，IT服务管理、项目管理；CISA，CISSP，CISP，COBIT，ITIL，CBCP，ISO27001等方面的培训和实践研究，始终以信息安全的共享交流、学习指导、职业规划为已任，并以培养国内信息安全人才、组织中国信息安全专业人员学习交流为发展目标。
- 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30000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、电信、移动、能源、制造、IT等多个行业。SPISEC的成立将更好地带动业内信息安全人员的培养和发展，保障国际信息安全学习联盟的基本运营，实现业内各领域有志之士的共同愿望，汇聚业内各领域的专业顶极人才。

国际信息系统安全认证联盟(ISC)2 —官方授权培训服务提供商！

2014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

➢ 变化内容

- 1.3.2 ISACA信息系统审计和鉴证标准框架
- 1.3.3 ISACA信息系统审计和鉴证准则/指南
- 1.3.4 ISACA信息系统审计和鉴证工具和技术

《2014年ISACA审计标准简体中文版》

下载地址：http://www.cncisa.com/read-htm-tid-22600.html

2014年CISA学习备考群： 119072577

1.3.2 ISACA信息系统审计和鉴证标准框架

IS 审计和鉴证标准	生效日期
1001 审计章程	2013年11月1日
1002 组织独立性	2013年11月1日
1003 专业独立性	2013年11月1日
1004 合理预期	2013年11月1日
1005 应有的职业谨慎	2013年11月1日
1006 业务熟练	2013年11月1日
1007 认定	2013年11月1日
1008 衡量标准	2013年11月1日
1201 项目规划	2013年11月1日
1202 规划中的风险评估	2013年11月1日
1203 执行和监督	2013年11月1日
1204 重要性	2013年11月1日
1205 证据	2013年11月1日
1206 使用其他专家的成果	2013年11月1日
1207 违规和非法行为	2013年11月1日
1401 报告	2013年11月1日
1402 后续活动	2013年11月1日

1.3.3 ISACA信息系统审计和鉴证准则/指南

- ~~G14 Application Systems Review 1 October 2008 Withdrawn 14 January 2013~~
- See Generic Application Audit/Assurance Program
- G15 Audit Planning Revised 1 May 2010
- ~~G16 Effect of Third Parties on an Organisation's IT Controls 1 March 2009 Withdrawn 14 January 2013~~
- See Outsourced IT Environments Audit/Assurance Program

1.3.3 ISACA信息系统审计和鉴证准则/指南

- ~~G18 IT Governance 1 July 2002 Withdrawn 14 January 2013~~
- ~~G19 Irregularities and Illegal Acts 1 July 2002 Withdrawn 1 September 2008~~
- ~~G21 Enterprise Resource Planning (ERP) Systems Review 16 August 2010 Withdrawn 14 January 2013~~
- See Security, Audit and Control Features SAP ERP, 3rd Edition Audit Programs and ICQs
- ~~G22 Business-to-consumer (B2C) E-commerce Review 1 October 2008 Withdrawn 14 January 2013~~
- See E-commerce and PKI Audit/Assurance Program
- ~~G23 System Development Life Cycle (SDLC) Reviews 1 August 2003 Withdrawn 14 January 2013~~
- See Systems Development and Project Management Audit/Assurance Program

1.3.3 ISACA信息系统审计和鉴证准则/指南

- ~~G24 Internet Banking 1 August 2003 Withdrawn 14 January 2013~~
- ~~G25 Review of Virtual Private Networks 1 July 2004 Withdrawn 14 January 2013~~
- See VPN Security Audit/Assurance Program
- ~~G26 Business Process Reengineering (BPR) Project Reviews 1 July 2004 Withdrawn 14 January 2013~~
- ~~G27 Mobile Computing 1 September 2004 Withdrawn 14 January 2013~~
- See Mobile Computing Security Audit/Assurance Program
- ~~G28 Computer Forensics 1 September 2004 Withdrawn 14 January 2013~~
- ~~G29 Post-implementation Review 1 January 2005 Withdrawn 14 January 2013~~
- See Systems Development and Project Management Audit/Assurance Program

1.3.3 ISACA信息系统审计和鉴证准则/指南

- ~~G31 Privacy 1 June 2005 Withdrawn 14 January 2013~~
- Note: Personally Identifiable Information Audit/Assurance Program scheduled to be issued Jan.
- ~~G32 Business Continuity Plan (BCP) Review From IT Perspective 1 September 2005 Withdrawn 14 January 2013~~
- See Business Continuity Management Audit/Assurance Program
- ~~G33 General Considerations on the Use of the Internet 1 March 2006 Withdrawn 14 January 2013~~
- See E-commerce and PKI Audit/Assurance Program
- ~~G36 Biometric Controls 1 February 2007 Withdrawn 14 January 2013~~
- See Biometrics Audit/Assurance Program
- ~~G37 Configuration Management Process 1 November 2007 Withdrawn 14 January 2013~~

1.3.3 ISACA信息系统审计和鉴证准则/指南

- ~~G38 Access Controls 1 February 2008 Withdrawn 14 January 2013~~
- See Identity Management Audit/Assurance Program Note: An updated version is scheduled to be issued in February.
- ~~G39 IT Organisation 1 May 2008 Withdrawn 14 January 2013~~
- ~~G40 Review of Security Management Practices 1 October 2008 Withdrawn 14 January 2013~~
- See Security Incident Management Audit/Assurance Program
- ~~G41 Return on Security Investment (ROSI) 1 May 2010 Withdrawn 14 January 2013~~

1.3.4 ISACA信息系统审计和鉴证工具和技术

- 工具和技术目前被分类为:
- 参考书系列 (书籍)
- 审计鉴证程序
- 白皮书
- 双月刊文章

第二章IT治理与管理

➢ 变化内容

- 2.3 企业IT治理
- 2.3.1 IT治理最佳实践
- 2.3.3 IT平衡记分卡
- 2.6 投资和分配实务
- 2.9.4 财务管理实务
- 2.9.7 绩效优化
- 2.12.2 灾难和其他破坏性事件

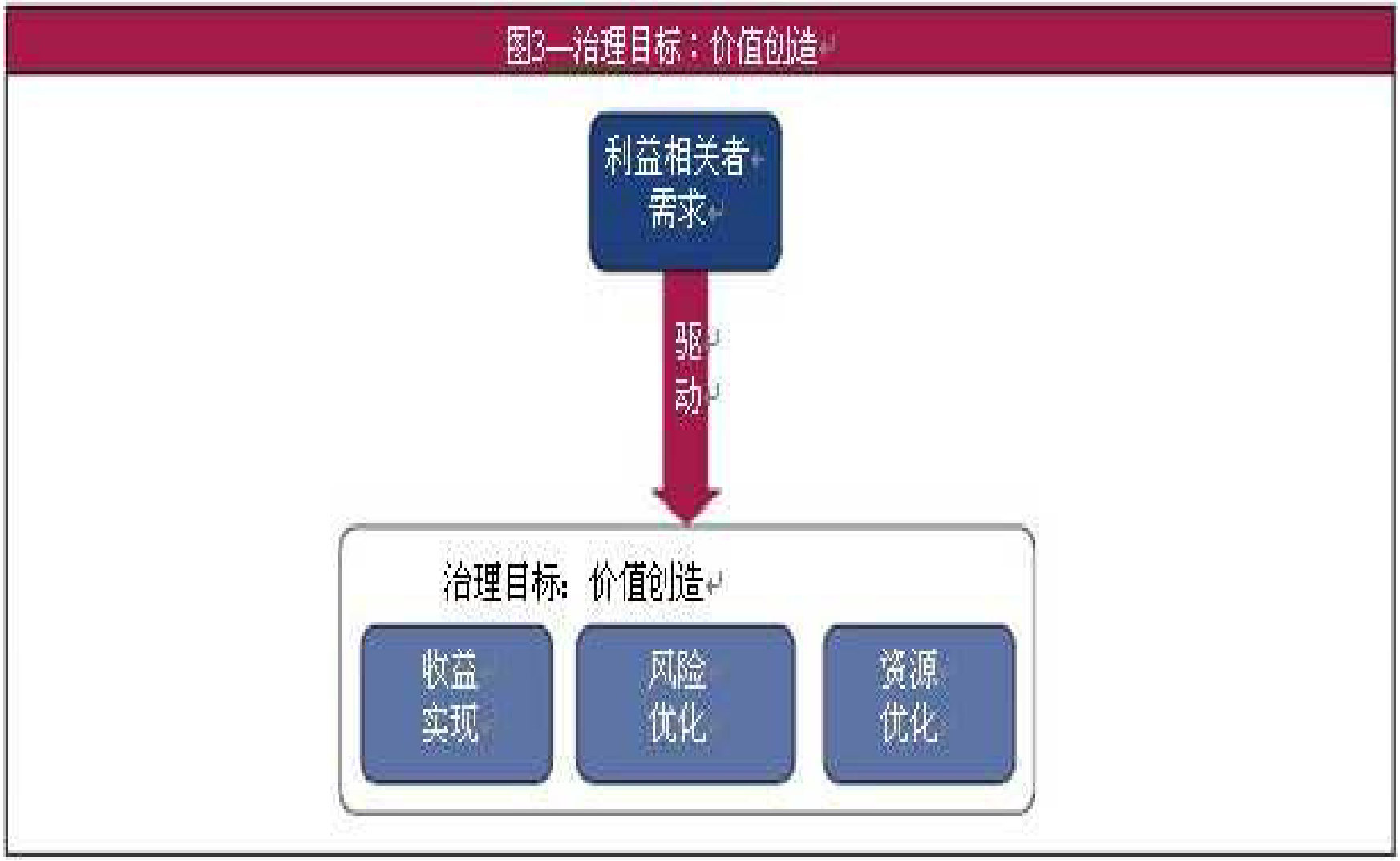
企业IT治理

- 企业IT治理Governance of enterprise IT (GEIT)代替IT Governance

参考文档:

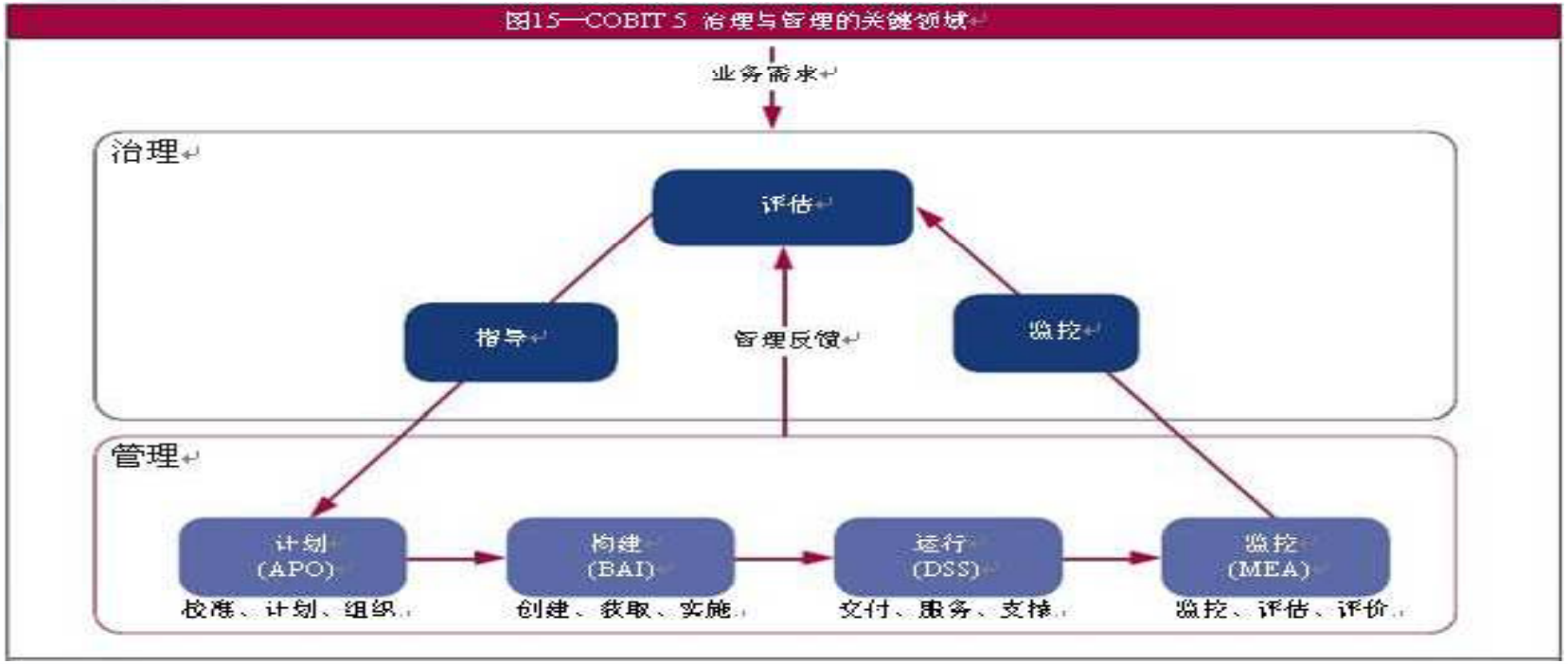
- COBIT5.0过程推动中文版
- COBIT5.0实施指南中文版
- COBIT5.0企业IT治理和管理的业务框架中文版

2.3.1 IT治理最佳实践



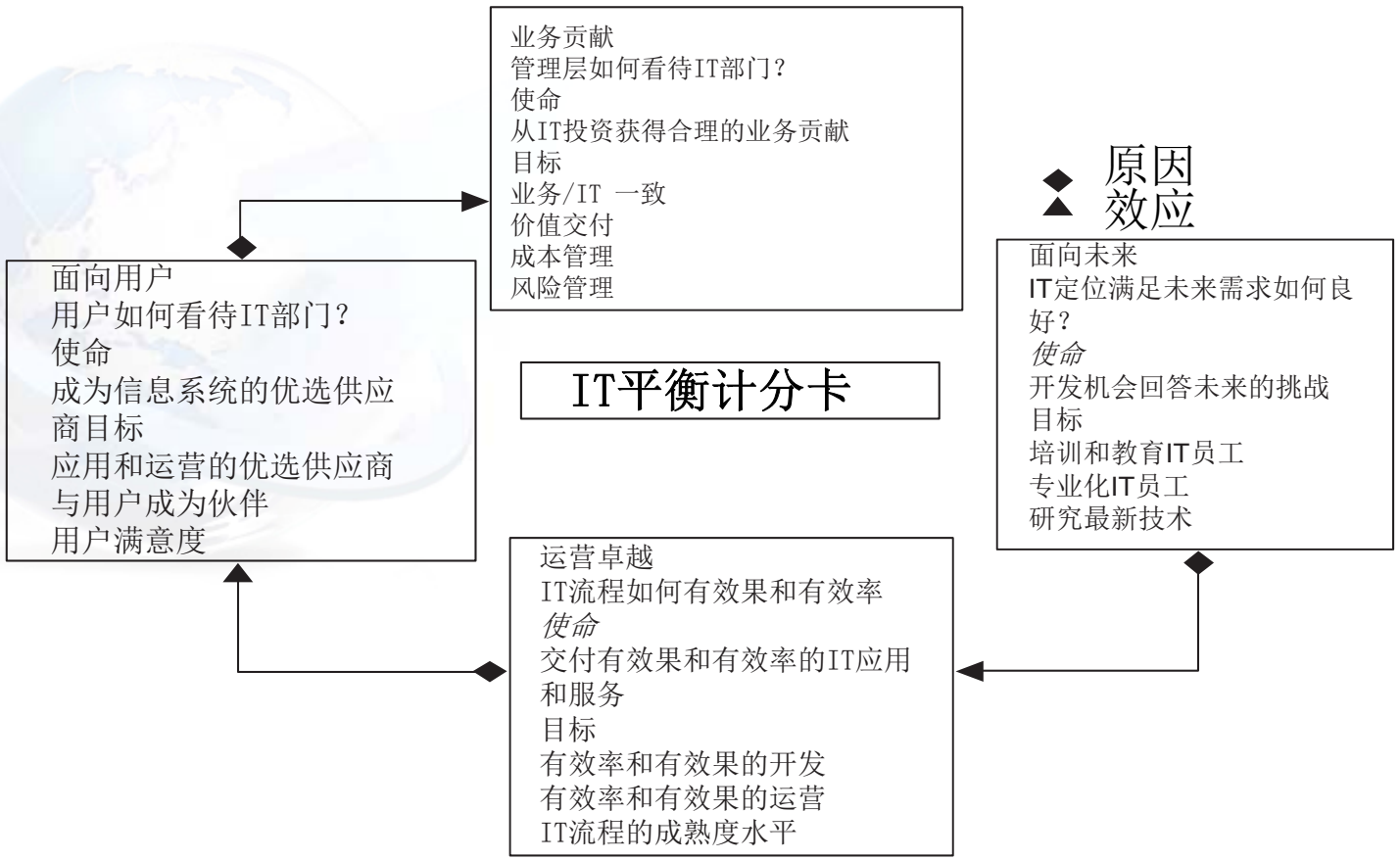
2.3.1 IT治理最佳实践

- 监控、评价和指导（表2.3）流程被端到端集成治理流程，聚焦监控、评价和指导：
  - 符合和绩效
  - 内部控制体系
  - 符合外部要求



2.3.3 IT平衡记分卡

Figure 7-通用IT平衡计分卡



2.6 投资和分配实务

- COBIT 5，EDM02 确保收益交付流程最优化，以可接受的成本投资IT，从业务流程、IT服务和IT资产中贡献业务的价值。流程的关键治理实践包括：
  1. 评价价值最优化
  2. 指导价值最优化
  3. 监控价值最优化

2.9.4 财务管理实务

- 计费提供所有利益相关方 “市场”度量信息处理设施提供的服务的效果和效率。当实施时，计费方针应 由董事会公布，首席财务官，用户管理层和信息系统管理层共同实施。

2.9.7 绩效优化

- 绩效不是一个系统运作多好；绩效是用户和利益相关方感知的服务；绩效优化是改善信息系统生产力到达最可能高水平的流程，不需要不必要、额外的在信息技术基础架构的投资
- 关键成功因素

  在有效的绩效管理方法中，度量不只被用于分配责任还被用于遵守报告要求，被用于创建和推动行动以改善绩效和企业IT治理

  有效的绩效度量依赖被处理的两个关键方面：
  - 绩效目标的清楚定义
  - 建立有效的度量以监控目标的获得

2.9.7 绩效优化

- 绩效度量流程也被要求帮助确保绩效被一致地和可靠地监控
- 有效的治理显著地使全部的绩效最优化，当如下发生时获得：
  - 目标被自顶向下设置，与高层次已批准的业务目标一致
  - 度量被自下向上建立，与使获得所有层次被每个层次管理层监控目标一致

两个关键的治理成功因素（使全面的绩效最优化）

- 利益相关者对目标的批准
- 董事和经理对获得目标的问责的接受

IT是复杂的和技术的话题，因此，通过以对利益相关者有意义的语言明确表达目标、度量和绩效报告以便采取活动以获得透明

2.9.7 绩效优化

- 方法论和工具

  多种改善和最优化方法论补充简单、内部开发的方法
  - 持续改善方法论，例如PDCA循环
  - 补充最佳实践，例如ITIL
  - 框架，例如COBIT
- 工具和技术

  推动度量、良好交流和组织改革的工具和技术包括：
  - Six Sigma
  - IT平衡计分卡
  - 关键绩效指标（KPI）
  - 基准测量
  - 业务流程重组
  - 根本原因分析
  - 生命周期成本-效益分析

2.9.7 绩效优化

- IT绩效度量和报告可能是法令的或合同的要求，对企业恰当的绩效度量实践包括:业务价值的成果度量，竞争优势和定义的绩效度量，显示IT如何表现。激励，例如奖金、报酬和认可应衔接绩效度量，与雇员、客户和利益相关者分享结果和进展是重要的

2.12.2 灾难和其他破坏性事件

意外/不可预知事件

- “不可预测的重大事件;它罕有发生,但一旦出现,就具有很大的影响力.发生后才能说明原因,是不可预测的现象- Black Swan”--Nassim Nicholas Taleb(2004) 黑天鹅现象

- 日本福岛核灾难

第三章信息系统的购置、开发与实施

- 无

第四章信息系统的操作、维护与支持

- 无

第五章信息资产的保护

➢ 变化内容

- 5.3.6授权事项—使用手持设备（Handheld Devices）远程访问

- 删除/变动小节内标题/但内容不变
- 5.6.1审计远程访问— 网络渗透测试（目录删除内部标题）

5.3.6授权事项—使用手持设备（Handheld Devices）远程访问

移动设备可能包括:

- 全功能手机，类似个人计算机功能或“智能手机”
- 笔记本电脑和上网本
- 平板电脑
- 偏携式数字助理(PDAs)
- 偏携式通用串行总线(USB) 设备：存储(例如“拇指驱动器”和 MP3设备) 和连接 (例如 Wi-Fi, 蓝牙® 和 HSDPAlUMTSIEDGE/GPRS调制解调器卡)
- 数码相机
- 无线射频识别技术(RFID)和移动无线射频识别技术(M-RFID)设备—数据存储，识别和资产管理
- 启用红外(IrDA) 设备例如打印机和智能卡

2014年CISA备考资料

➢ 2014年CISA认证考试讲义（标注版）

- 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）

➢ 2014年CISA认证考试中文书（第五版）

- 点评：2014年CISA认证考试中文书根据CISA Review Manual 2014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。

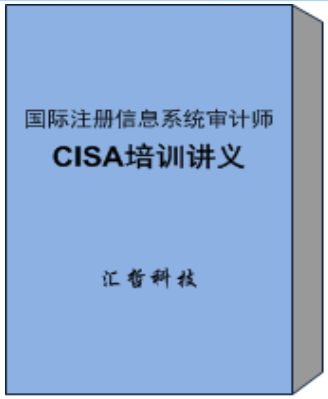
2014年CISA备考资料

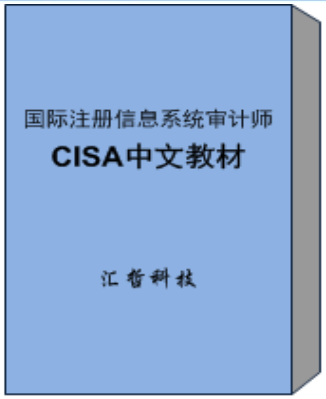
➢ 2014年CISA认证考试中英语对照题目集红宝书第五版

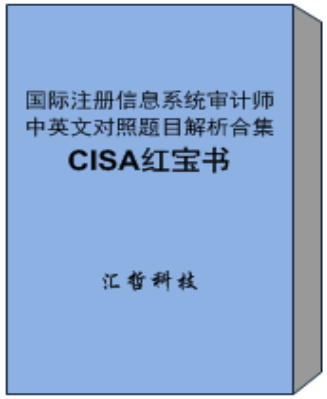
- 点评：2013年CISA认证考试中英语对照题目集红宝书第四版根据CISA Review Questions, Answers & Explanations Manual 2014 Supplement ；CISA Review Questions, Answers & Explanations Manual 2014；CISA Review Questions, Answers & Explanations Manual 2012整理而成；以帮助学员熟悉CISA所涉及所有题目类型，提高考试通过水平为目得！

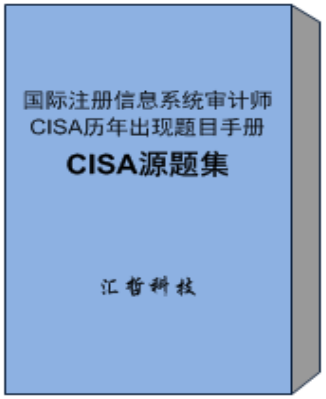
➢ 2014年CISA认证考试历年出现题目手册（2013年12月更新版）

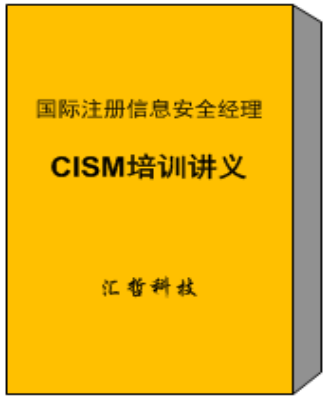
- 点评：CISA认证考试历年出现题目手册是根据历年CISA考试中常出现的题目进行整理和收集而成以帮助和分析题目类型，适用于所有参加考试的学员！

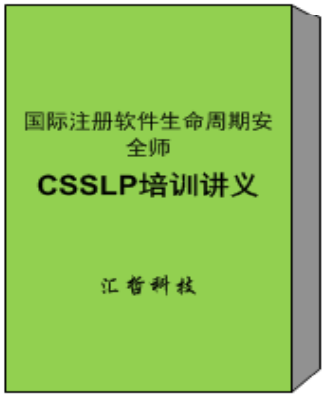


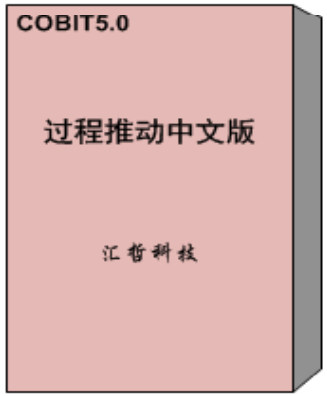


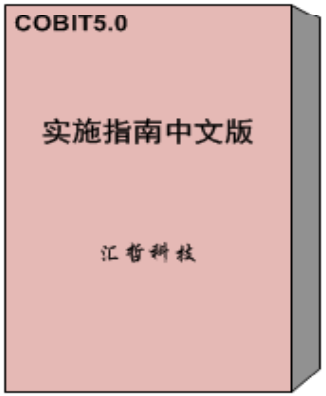


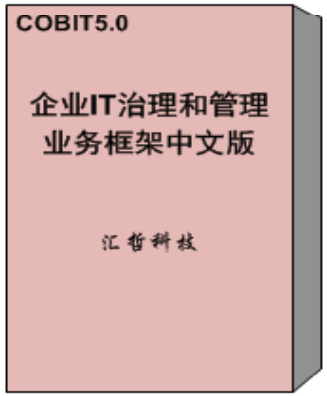


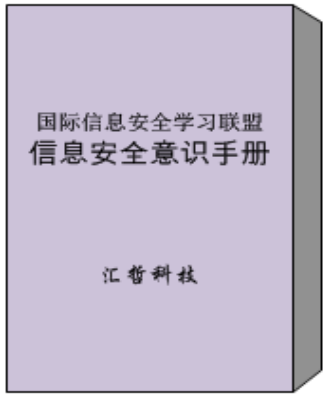








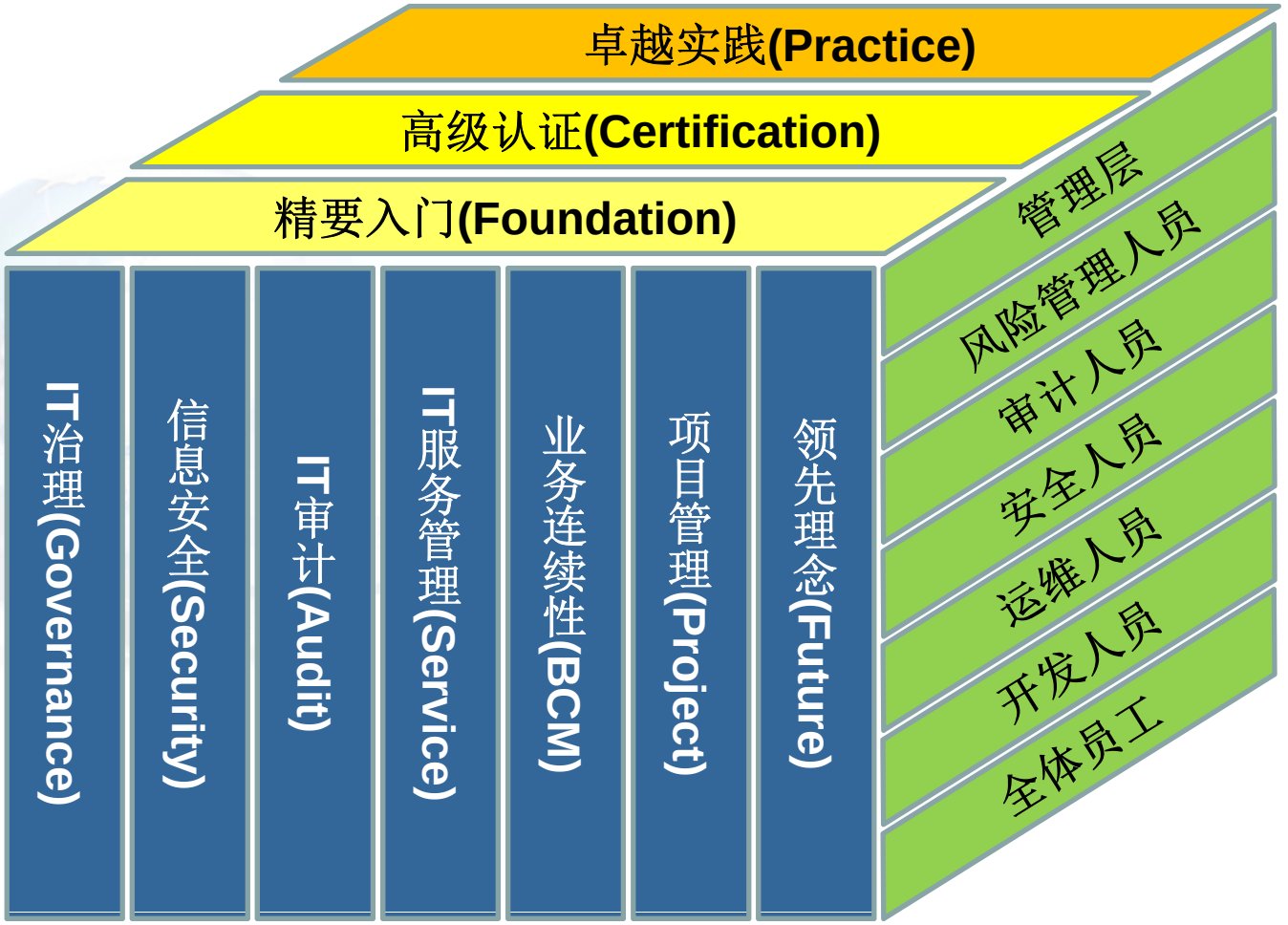




2014年CISA学习计划表

名称	分类	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	十一月	十二月
CISA注册信息系统审计师认证（5天）	高级认证			1-5日 上 海	26-30 上海	23-28 上海	25-29 上海	26-30 上海	27-31 上海	24-28 上海	25-29 上海	26-30 上海	27-31 上海
				26-30 北 京			7-11 北 京		16-20 北 京			15-19 北 京	
					19-23 深 圳			23-27 深 圳			22-26 深 圳		
IT审计实践	卓越实践					23-25 上 海				20-22 上 海		29-1 上 海	
考试时间：6月，9月，12月第二个星期六													

汇哲培训服务三维体系



联系我们

—用心做事|国内最可靠的信息安全培训服务商！

Shanghai Spisec Information & Technology Co., Ltd.

公司电话：+86 (0) 21-33663299

公司邮箱：huizhe@spisec.com

公司网址：http://www.spisec.com

http://www.cncisa.com

公司地址：上海市黄浦区西藏南路760号安基大厦1506

公司邮编：200021