ISCA 香港分会的免费讲座记录

第一章的主要知识点：
1、IS 审计定义
2、审计章程（职责、权力和 accountability）
3、长短期审计计划
4、法律法规对审计的影响（如何识别与法律法规的符合性）
5、审计规划（planning）
6、审计职业道德准则（独立.....）
7、沟通与报告
8、风险评估
9、控制的定义及分类（预防、检测和纠正）
10、审计程序/步骤
11、风险类型（固有、检测和控制）
12、抽样（属性及变量 VS 符合性测试和实质性测试）
13、计算机辅助审计技术（CAATS）
14、CSA
关键术语：
1、管理控制（administrative control）
2、属性
3、审计风险
4、CAATS
5、控制风险
6、EAM
7、重要程度/实质（material）

第 2 章的主要知识点：
1、公司治理（企业架构）
2、审计在公司治理中的角色
3、IT 战略委员会/IT 战术委员会（组成人员及职责分工）
4、平衡记分卡
5、信息安全治理
6、外包
7、缺乏职责分离所需的补偿性控制
关键术语：
1、abend
2、审计目标（objectives）
3、审计踪迹（留痕）audit trail
4.、标杆管理 benchmark
5、业务风险 business risk
6、补偿性控制
7、证据
8、暴露

第 3 章的主要知识点：
1、项目管理实践
2、系统开发的理论及控制（CPM、PRET 等）
3、项目组成员（包括发起人）及职责
4、SDLC（各个阶段包括的主要活动及目的）
5、在线编程环境
6、各种测试类型（考的比较多）
7、项目实施（实施计划、数据转换）
8、其他开发方法（如快速开发方法、敏捷开发、原型法等）
9、变更管理
10、配置管理
11、第四代编程语言
12、过程改进（ISO9126、CMMI、15504）
13、应用控制（输入控制、过程控制和输出控制）
14、审计应用系统的方法（系统的交易流程、分析应用控制的风险评估模型、观察与测试用户的实施过程、数据完整性测试、在线交易处理中的数据完整性、测试应用系统、持续审计工具、在线审计技术/方法）
关键术语：
1、编辑控制
2、EDI
3、可行性研究
4、PERT
5、恢复测试

第四章：关键知识点
1、SLM，关键是是否符合业务目标
2、插播 ITIL 的 10 个过程
-服务支持 5 个过程：事件管理、问题、变更、发布和配置。前后因果关系
-服务交付 5 个过程：服务水平管理、可用性、容量、服务持续性和财务管理。以服务水平管理为核心监控其他 4 个过程。
3、性能监控工具
4、OSI 模型
5、数据库评审
数据库设计、访问、管理、易用性、规格化和非规格化的目的
6、系统软件的功能
7、能力计划和监控技术
8、变更、配置、发布和补丁管理
9、事件、问题管理
10、软件许可
工具：集中控制、无盘工作站、计量工具、定期扫描。
11、系统可靠性
容错硬件、单点失效和集群。

第五章知识点：（东西太多了，没怎么记录，就把自己记下的给大家）

1、数据分类的目的
2、计算机犯罪和滥用的区别
3、PDA 的加密
4、client-server 架构的安全控制、监控、加密和认证
5、数字签名
数据完整性--签名
认证-------私钥
防抵赖性----签名
包重发-----时间戳
6、SSL 会话层
7、S/HTTP 应用层
8、IPsec 网络层
9、SSH
10、防毒墙
11、审计：网络接入点、参透性测试
12、网络机房选址
13、笔记本电脑的安全
电缆锁、备份数据、加密、对单个文件设置口令等
术语：
1、ACL
2、非对称加密
3、Authentication
4、Biometrics
5、Card Swipes
6、challenge/response token
7、数字证书
8、干管灭火

第六章知识点
1、计划恢复和恢复计划
-高管的责任
-BIA
-恢复策略
-具体的计划
-执行计划
-测试和维护计划
2、BIA
-信息的重要性
-IS 和最终用户的参与
-关键的业务流程、关键信息
-RTO
-系统风险排序
3、异地备份设施的类型
热站、温站和冷站

4、组织和责任分配
5、BCP 计划的组件
-关键启动人或者决策人
-供应商的备份
-通信和网络
6、测试

术语：
Back-up
冷站
连续性
off-line files
offsite storage
recovery testing
resilience