(ISC)2 CISSP Official Guide 第四版

第一章 安全与风险管理

安全与风险管理的概念
机密性、完整性与可用性
    机密性
    完整性
    可用性
安全治理
    组织的目标 Goals、使命 Mission 与任务 Objectives
    组织流程
    安全角色与职责
    信息安全策略
完整与有效的安全体系
    监管委员会
    控制框架
    应有的关注 due care
    应尽的职责 due diligence
合规性（原法律法规章节）
    治理、风险与合规（GRC）
    法律与法规合规
    隐私需求合规
全球性法律与法规问题 （原法律法规章节）
    计算机犯罪
    版权与知识产权
    进出口
    跨国界数据传输
    隐私
    数据泄露
    相关法律法规
理解专业道德（原法律法规章节）
    道德体系的法规需求
    计算机道德的主题
    一般计算机道德的谬论
    黑客行为与黑客主义
    道德规范的指引与资源
    ISC2 的专业道德规范
    支持组织的道德规范
开发与实施安全策略
业务连续性与灾难恢复需求（原 BCP 与 DRP 章节）
    项目启动与管理

设计并定义项目范围与计划
实施业务影响分析（BIA）
识别与分级
评估灾害的影响
恢复点目标（RPO）
管理人员安全
背景调查
雇佣协议与策略
雇员离职程序
供应商、顾问与合同工控制
隐私
风险管理的概念
组织风险管理概念
风险评估方法论
识别威胁与脆弱性
风险评估与分析
控制措施选择
实施风险控制措施
控制的类型
访问控制的类型
控制评估、监控与测量
实物与非实物资产评价
持续改进
风险管理框架
威胁建模
决定可能的攻击与降低分析
减小威胁的技术与流程
采购策略与实践
硬件、软件与服务
管理第三方供应商
最小的安全与服务级别需求
安全教育、培训与意识
正式的安全意识培训
意识活动与防范-创建组织的安全文化

第二章 资产安全（新增章节）

资产安全概念
数据管理：决定与维护所有者
数据策略
角色与责任
数据所有者
数据保管者

- 数据质量
- 数据文件化与组织化

数据标准

- 数据生命周期控制
- 数据定义与建模
- 数据库维护
- 数据审计
- 数据存储与归档

数据寿命与使用

- 数据安全
- 数据访问、共享与传播
- 数据发布

信息分级与支持资产

资产管理

- 软件版权
- 设备生命周期

保护隐私

确保合适的保存

- 介质、硬件和人员
- 公司“X”数据保留策略

数据安全控制

- 静态的数据
- 传输的数据
- 基线
- 范围与裁剪

标准选择

- 美国的资源
- 全球的资源
- 国家网络安全框架手册
- 提升关键基础实施网络安全的框架

第三章 安全工程

（新增章节、融合了安全架构、物理安全、密码学等）

在工程生命周期中应用安全设计原则

安全模型的基本概念

- 通用系统组件
- 他们如何一起工作
- 企业安全架构
- 通用架构框架
- Zachman 框架
- 获取和分析需求
- 创建和设计安全架构

信息系统安全评价模型
    通用正式安全模型
    产品评价模型
    业界和国际安全实施指南
安全架构的漏洞
    系统
    技术与流程集成
    单点故障
    客户端的漏洞
    服务端的漏洞
数据库安全
    大型可扩展并行数据系统
    分布式系统
    加密系统
软件和系统的漏洞与威胁
    Web 安全
移动系统的漏洞
    远程计算的风险
    移动办公的风险
嵌入式设备和网络物理系统的漏洞
密码学应用
    密码学历史
    新出现的而技术
    核心信息安全原则
    密码系统的附加特性
    密码生命周期
    公钥基础设施（PKI）
    密钥管理流程
    密钥的创建与分发
    数字签名
    数字版权管理
    抗抵赖
    哈希
    单向哈希函数
    加密攻击的方法
站点和设施的设计考虑
    安全调查
站点规划
    路径设计
    通过环境设计来防止犯罪（CPTED）
    窗户
设施安全的设计与实施
设施安全的实施与运营
    通信与服务器机房

区域划分与区域安全限制
数据中心安全

第四章 通信与网络安全

通信与网络安全概念
安全网络架构与设计
OSI 与 TCP/IP
IP 组网
目录服务
多层协议的含义
各类协议
实施
VOIP 网络
无线网络
无线安全问题
加密来保证通信安全
网络组件安全
硬件
传输介质
网络访问控制设备
中断安全
内容分发网络（CDN）
通信通道安全
语音
多媒体
开放协议、应用与服务
远程访问
数据通信
虚拟化网络
网络攻击
网络作为攻击通道
网络作为防护堡垒
网络安全目标与攻击模式
扫描技术
安全事件管理（SEM）
IP 碎片攻击与伪造包
拒绝服务与分布式拒绝服务攻击
欺骗
会话劫持

第五章 身份与访问管理 （原访问控制章节）

身份与访问管理概念
资产的物理与逻辑访问
人员和设备的身份识别与认证
    身份识别、认证与授权
身份管理实施
    密码管理
    账户管理
    用户配置管理
    目录管理
    目录技术
    单/多因素认证
    可审计性
    会话管理
    身份的注册与验证
    证书管理系统
身份即服务（IDaaS）
集成第三方身份服务
授权机制的实施与管理
    基于角色的访问控制
    基于规则的访问控制
    强制访问控制
    自主访问控制
防护或缓解对访问控制攻击
    Windows PowerShell 相关命令
识别与访问规定的生命周期
    规定
    回顾
    撤销

第六章 安全评估与测试 （新增章节）

安全评估与测试概念
评估与测试策略
    软件开发作为系统设计的一部分
    日志审核
    虚假交易
    代码审核与测试
    负向测试/滥用用力测试
    接口测试
收集安全流程数据
内部与第三方审计
    SOC 汇报选项

第七章 安全运营 （融合了原 DRP 相关内容）

安全运营概念

调查

- 犯罪场景
- 策略、角色与责任
- 事件处理与响应
- 恢复阶段
- 证据收集与处理
- 汇报与记录
- 证据收集与处理
- 持续监控
- 数据防泄漏（DLP）

为资源提供配置管理

安全运营的基本概念

- 关键主题
- 控制特权账户
- 使用组和角色管理账户
- 职责分离
- 监控特殊权限
- 工作轮换
- 管理信息生命周期
- 服务级别管理

资源保护

- 实物资产与非实物资产
- 硬件
- 介质管理

事件响应

- 事件管理
- 安全度量与汇报
- 管理安全技术
- 检测
- 响应
- 汇报
- 恢复
- 修补与回顾（经验学习）

针对攻击的防御性措施

- 非授权泄密
- 网络入侵检测系统架构
- 白名单、黑名单、灰名单
- 第三方安全服务、沙箱、恶意代码防范、蜜罐和蜜网

补丁和漏洞管理

- 安全与补丁信息资源

变更与配置管理

- 配置管理
- 恢复站点策略
- 多处理中心
- 系统弹性与容错需求

灾难恢复流程

- 创建计划
- 响应
- 人员
- 通信
- 评估
- 还原
- 提供培训
- 计划的演练、评估与维护

演练计划回顾

- 桌面演练
- 仿真演练
- 并行演练
- 中断演练
- 计划的更新与演练

业务连续性与其他风险领域

- 边界安全的实施与运维

访问控制

- 智能卡类型
- 闭路电视
- 内部安全
- 建筑物内部安全

人员安全

- 隐私
- 出差
- 胁迫

第八章 软件开发生命周期安全

软件开发生命周期安全概念

软件开发安全概要

- 开发生命周期
- 成熟度模型
- 操作与维护
- 变更管理
- DevOps（与产品运维集成）

环境与安全控制

- 软件开发方法
- 数据库与数据仓库环境
- 数据库漏洞与威胁

- 数据库控制
- 知识库管理
- Web 应用环境

软件环境安全

- 应用开发与编码概念
- 软件环境
- 库与工具集
- 源代码安全问题
- 恶意代码
- 恶意代码防范

软件保护机制

- 安全内核、RM 引用监控与 TCB 可信计算基
- 配置管理
- 代码保存安全
- API 安全

评估软件安全的有效性

- 认证与认可
- 变更记录与审计
- 风险分析与缓解

评估软件采购安全