信息安全与安全风险

如何为一个还没有建立的新系统设计制定信息安全保障系统呢？

就是对信息应用系统进行安全风险分析、识别、评估，并为之制定防范措施。

信息安全与安全风险的关系

1、拟定新系统的功能———目标
2、现有系统（业务流程）分析———风险识别
3、对识别出的风险预优估可能的后果———风险评估
4、按照风险的大小和主次、设计相应原对策———控制风险
5、对设计对策进行投入产出评估
6、可行转入 7，不可行返回 1
7、设计
8、实施

安全风险识别

1、安全威胁的分类

从风险性质：静态风险：人们的错误判断和错误行为造成的风险
动态风险：人们欲望的变化，生产方式和生产技术的变化产生的风险

从风险结果：纯粹风险：仅仅会造成损害的风险，称为纯粹风险
投机风险：可能造成利润也可能造成损失的风险

从风险源划分：

① 自然事件风险
② 人为风险
③ 软件风险 ： ⊙兼容风险 ； ⊙维护风险 ⊙ 使用风险
④ 软件过程风险

⊙软件需求阶段风险

首先，要保证软件需求的变化不会持续蔓延，而使系统无法按期完成，另一方面，要保证开发能够为用户所接受。

⊙设计阶段的风险

设计阶段的主要任务：一方面，要完成系统体系结构的定义，使之能够完成需求阶段既定目标；另一方面，检验需求的一致性和需求分析的完整性和正确性。

设计本身的风险：一种是来自于系统分析人员；另一种是来自于设计文档。

⊙实施阶段的风险

本阶段的风险来源：源代码书写的规范性、可读性。

（源代码是文档的一部分，又是计算机系统的实体）

⊙维护阶段的风险

软件维护的两个阶段：第一，试运行阶段维护，目的是发现测试阶段未发现的错误；
第二，软件升级或移值维护

⑤ 项目管理风险

项目管理风险的来源：⊙应用软件产品的不可预见性；
⊙软件的生产过程不存在绝对正确的过程形式；
⊙信息系统应用项目的独特性

项目经理	把握全局，侧重于商务方面，负责同客户的交流
项目负责人	制定开发计划和开发策略，参与系统分析设计，保证项目按时完成。
行业专家	在软件分析阶段，帮助分析人员界定系统实现边界和实现功能
质量监督组	编制质量控制计划，并负责落实；控制必要文档的生成，并监督软件质量，形成软件质量报告；对于质量问题
系统分析员	进行系统的分析和设计工作，书写软件需求分析和系统分析相关的文档。进行测试策略的编制和性能测试的指导。
程序员	进行软件的详细设计及代码的实现，并适当地进行白盒测试；
测试员	对系统进行正确性验证测试及性能测试，书写测试报告和测试统计报告，并提请质量监督组复审查
技术支持	协同系统分析员听取用户需求，对需求分析进行参考性复审；协同测试人员进行测试；书写操作手册和在线帮助；
文档组	对各部门产生的文档进行格式规范、版本编号和控制、存档文件的检索；协助质量监督组进行软件质量监督；

⑥ 应用风险

应用相关的风险：⊙安全性；⊙未授权访问或修改数据；⊙未授权远程访问；⊙不精确的信息；⊙错误或虚假信息的输入；
⊙授权的终端用户滥用 ⊙不完整的处理；⊙重复数据处理；⊙不及时处理；⊙通信系统失败；⊙不充分的测试；
⊙不充分的培训；⊙不充分的支持；⊙不充分的文档

⑦ 用户使用风险

用户使用风险包括：⊙不充分的使用资源；⊙不兼容的系统；⊙冗余系统；⊙无效的应用； ⊙职责不分明；⊙需求分析不全面；
⊙非授权访问数据或程序； ⊙侵犯版权；⊙病毒破坏信息

风险识别与风险评估的方法

1、 风险识别的方法

⊙问询法（头脑风景法、面谈法和德尔菲法）
⊙财务报表法
⊙流程图法（网络或 WBS 法）
⊙现场观察法
⊙历史资料
⊙环境分析法
⊙类比法
⊙专家咨询

2、 风险评估的方法

⊙ 概率分布（专家预测）
⊙ 外推法（使用历史数据）
⊙ 定性评估
⊙ 矩阵图分析
⊙ 风险发展趋势评价方法
⊙ 项目假设前提评价及数据准确度评估