**第五章 信息安全风险评估**

**1．简述信息安全风险评估的概念、目的、原则以及意义。**

**2．信息安全风险评估的核心要素是什么？它们之间有何关系？**

**3．画出信息安全风险评估的流程图并简述其过程。**

**4．风险计算的公式是什么？并解释公式中相关符号的含义。**

**5．简述风险计算的过程。**

**6．进行风险处理的过程中，选择安全控制措施时应该考虑哪些因素？**

**7．风险评估文档的包括哪些？简述并阐述文档内容。**

**8．举例说明几个典型的信息安全风险评估算法。**

**9．信息安全的风险评估工具有哪些？简述并举例说明。**

**10．联系实际谈谈你对风险评估的看法。**

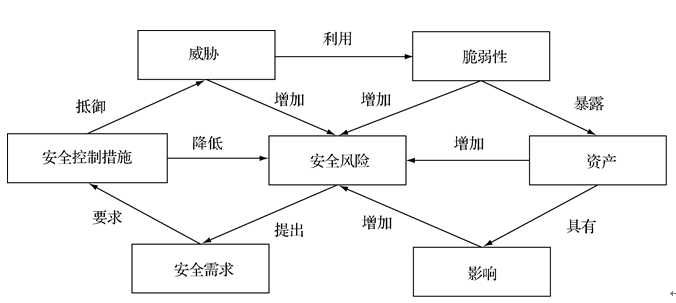
1.（1）概念：信息安全风险评估是参照风险评估标准和管理规范，对信息系统的资产价值、潜在威胁、薄弱环节、已采取的防护措施等进行分析，判断安全事件发生的概率以及可能造成的损失，提出风险管理措施的过程。（2）目的：系统地从计划、设计、制造、运行等过程中考虑安全技术和安全管理问题，找出生产过程中潜在的危险因素，并提出相应的安全措施；对潜在的事故进行定性、定量分析和预测，求出系统安全的最优方案；评价装备或生产的安全性是否符合有关标准和规定，实现安全技术与安全管理的标准化和科学化。（3）原则：

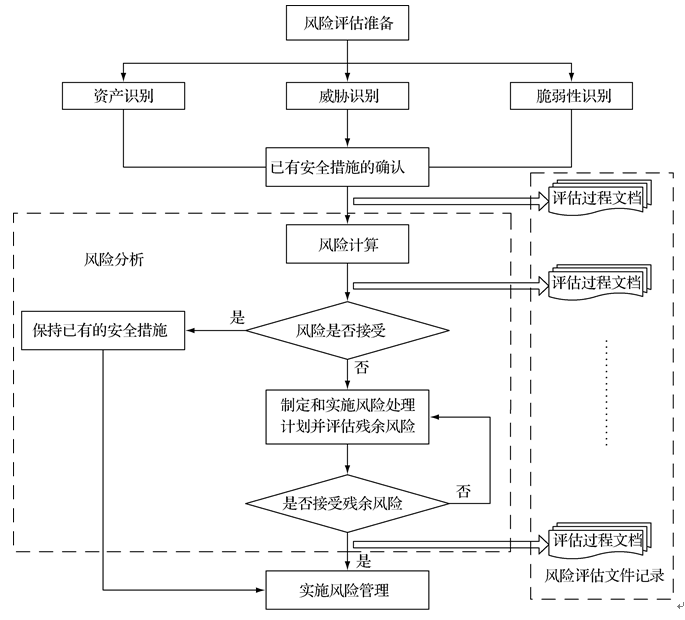
信息安全风险评估相关原则

|  |  |
| --- | --- |
| 相关原则 | 内容 |
| 可控性原则 | 包括人员可控性、工具可控性、项目过程可控性 |
| 可靠性原则 | 风险评估需要参照有关的信息安全标准和规定，做到有据可查 |
| 完整性原则 | 严格按照委托方的评估需求和指定范围进行全面的信息安全风险评估 |
| 最小影响原则 | 风险评估工作不能妨碍组织的正常业务活动，应从系统相关的管理和技术层面，力求将风险评估过程的影响降到最小 |
| 时间与成本有效原则 | 风险评估过程花费的时间和成本应该是有效且合理的 |
| 保密原则 | 受委托的评估方要对评估过程进行保密，应与委托的被评估方签署相关的保密和非侵害性协议，未经许可不得将数据泄露给其他组织或个人 |

（4）意义：一是更准确地认识风险。通过定量方法进行风险评价，可以定量地确定建设工程各种风险因素和风险事件发生的概率大小或概率分布，及其发生后对建设工程目标影响的严重程度或损失严重程度。二是保证目标规划的合理性和计划的可行性。三是合理选择风险对策，形成最佳风险对策组合。

2.（1）信息安全风险评估的基本要素主要包括：资产、威胁、脆弱性、安全风险、影响、安全控制措施以及安全需求。（2）风险要素关系图：



3．

风险评估过程大致分为4个阶段：第一阶段为风险评估的准备；第二阶段是风险识别；第三阶段是风险分析，包括计算风险、风险的影响分析等，并建立相关评估报告；第四阶段进行相应的风险管理过程，并提交风险评估报告。

4. 

风险公式符号含义表

|  |  |  |  |
| --- | --- | --- | --- |
| 符号 | 含义 | 符号 | 含义 |
|  | 安全风险 |  | 资产 |
|  | 威胁 |  | 脆弱性 |
|  | 已有控制所减少的风险 |  | 安全事件所作用的资产价值 |
|  | 脆弱性严重程度 |  | 威胁利用资产的脆弱性导致安全事件的可能性 |
|  | 安全事件发生后造成的影响 |

5. 风险计算过程分以下3个环节进行计算。①计算安全事件发生的可能性：计算安全事件发生的可能性需要考虑两方面的因素：威胁出现频率（）、脆弱性的状况（），即：。②计算安全事件发生后造成的影响：根据资产价值及脆弱性严重程度，计算安全事件一旦发生后造成的影响，即：③计算风险值：根据计算出的安全事件的可能性以及安全事件造成的影响，计算风险值，即：。

6. 选择安全控制措施时，要考虑以下因素。①考虑控制的成本；②考虑控制的可用性；③结合已有的控制措施；④控制措施的功能范围以及强度。

7. 风险评估记录文档

|  |  |
| --- | --- |
| 风险评估文档 | 文档内容 |
| 《风险评估方案》 | 风险评估的目标、范围、人员、评估方法、评估结果的形式和实施进度等 |
| 《风险评估程序》 | 明确评估的目的、职责、过程、相关的文档要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据 |
| 《资产识别清单》 | 根据组织在风险评估程序文档中所确定的资产分类方法进行资产识别，明确资产的责任人／部门 |

|  |  |
| --- | --- |
| 风险评估文档 | 文档内容 |
| 《重要资产清单》 | 根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人、部门等 |
| 《威胁列表》 | 根据威胁识别和赋值的结果，形成威胁列表，包括威胁的名称、种类、来源、动机及出现的频率等 |
| 《脆弱性列表》 | 根据脆弱性识别和赋值的结果，形成脆弱性列表，包括具体脆弱性的名称、描述、类型及严重程度等 |
| 《已有安全控制措施确认表》 | 根据对已采取的安全控制措施确认的结果，形成已有安全控制措施确认表，包括已有安全控制措施名称、类型、功能描述及实施效果等 |
| 《风险评估报告》 | 对整个风险评估过程和结果进行总结，详细说明被评估对象、风险评估方法、资产、威胁、脆弱性的识别结果、风险分析、风险统计和结论等内容 |
| 《风险处理计划》 | 对评估结果中不可接受的风险制定处理计划，选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性 |
| 《风险评估记录》 | 根据风险评估程序，要求风险评估过程中的各种现场记录可复现评估过程，并作为产生歧义后解决问题的依据 |

8.①OCTAVE法：OCTAVE（Operationally Critical Threat，Asset，and Vulnerability Evaluation，可操作的关键威胁、资产和薄弱点评估）是由美国卡耐基·梅隆大学软件工程研究所下属的CERT协调中心开发的用以定义一种系统的、组织范围内的评估信息安全风险的方法。②层次分析法：层次分析法（Analytic Hierarchy Process，AHP）是将与决策总是有关的元素分解成目标、准则、方案等层次，在此基础之上进行定性和定量分析的决策方法。该方法是美国运筹学家、匹茨堡大学教授萨蒂于20世纪70年代初，在为美国国防部研究“根据各个工业部门对国家福利的贡献大小而进行电力分配”课题时，应用网络系统理论和多目标综合评价方法，提出的一种层次权重决策分析方法。

9.风险评估工具可以分成风险评估管理工具、信息基础设施风险评估工具、风险评估辅助工具三类。①例如NIST SP 800-30、BS 7799、ISO/IEC 13335等。②如Nmap、X-scan、Nessus和Fluxay等。③如入侵检测系统（Intrusion Detection System，IDS）等。

10.通过风险评估，可以了解系统目前和未来的风险所在，评估这些风险可能带来的安全威胁与影响程度，为安全策略的确定、信息系统的建立以及安全运行提供依据。同时通过第三方权威或者国际机构评估和认证，也为用户提供了信息技术产品和系统可靠性的信息、增强产品、单位的竞争力。