风险评估

风险评估要素关系图

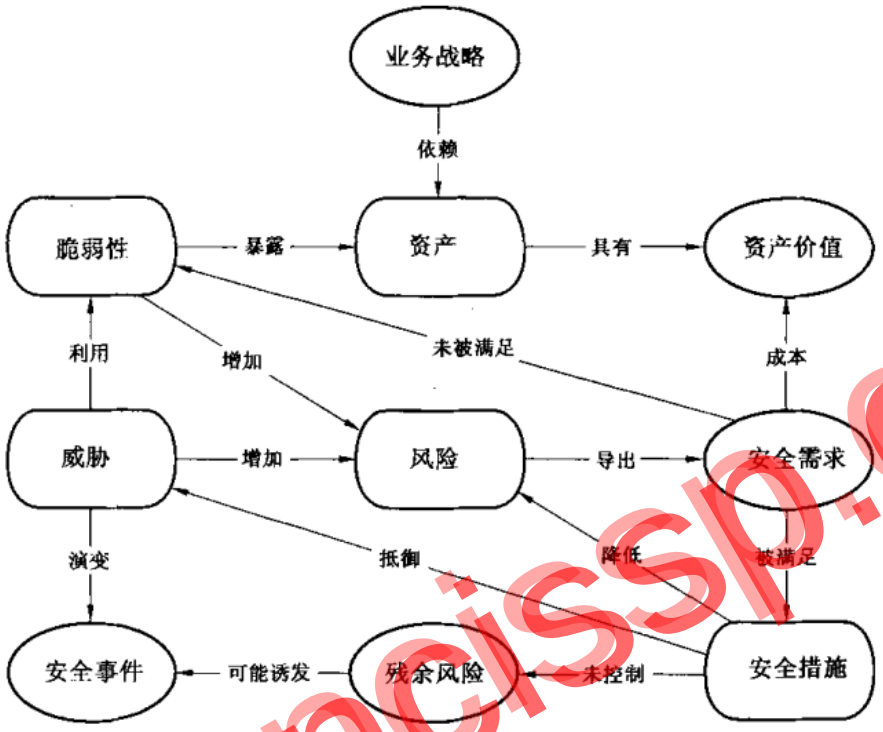

图 1　风险评估要素关系图

风险分析原理图

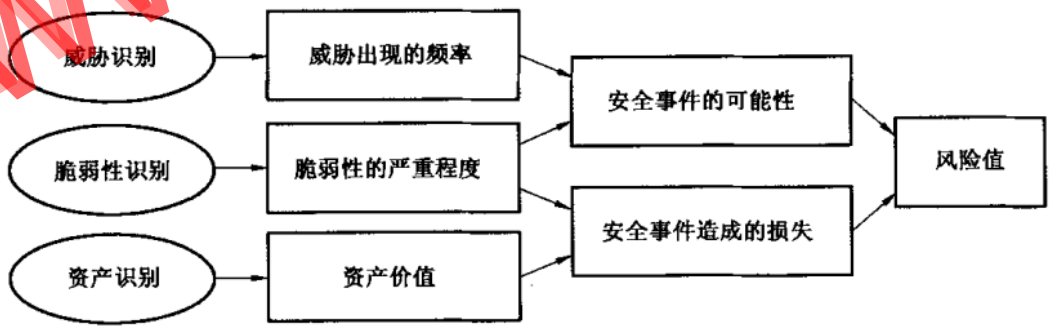

图 2　风险分析原理图

风险评估实施流程图

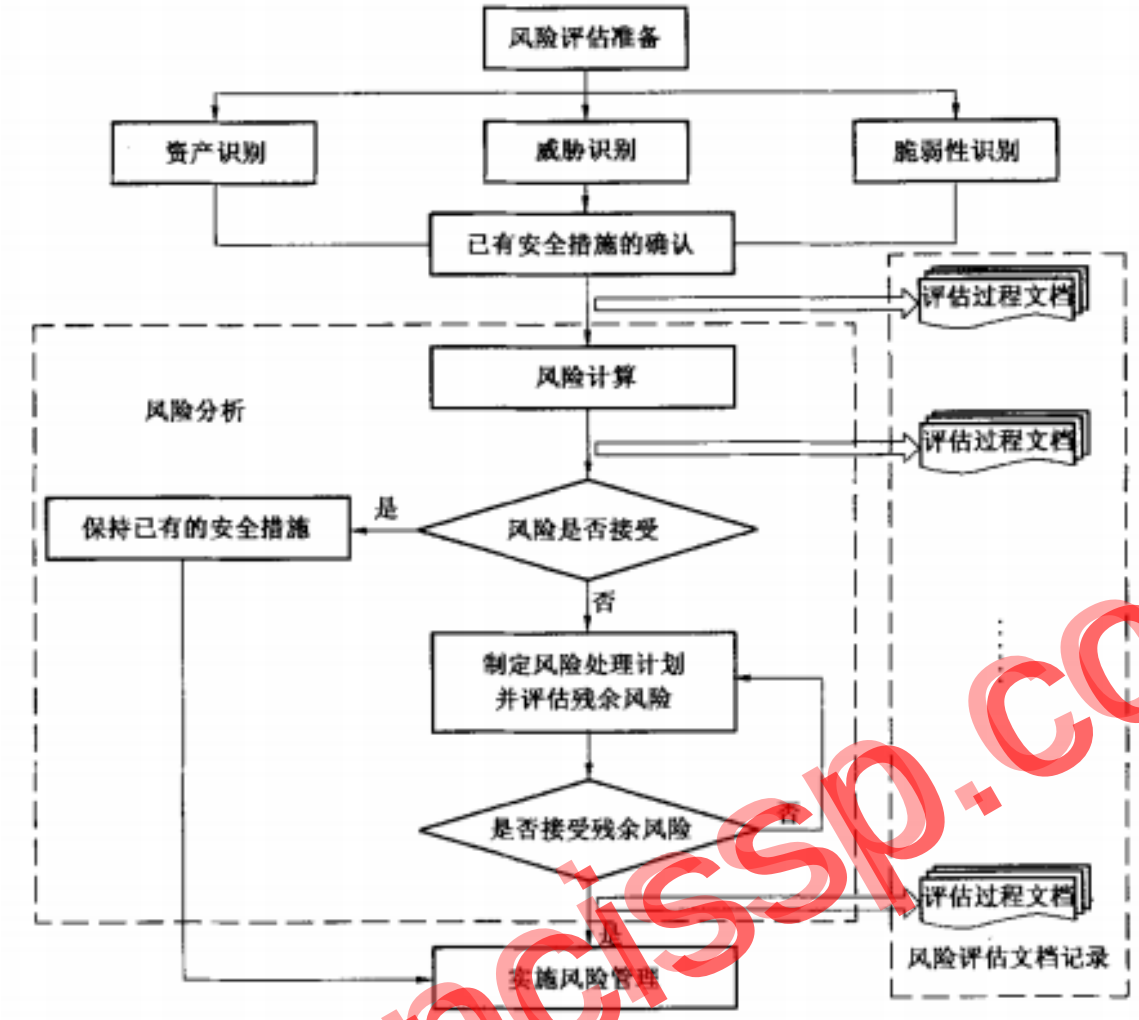

图 3　风险评估实施流程图

等级保护

1、物理安全

2、网络安全

3、主机安全

4、应用安全

5、数据安全及备份恢复

6、安全管理制度

7、安全管理机构

8、人员安全管理

9、系统建设管理

10、系统运维管理

信息系统根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为五级

不同等级的信息系统应具备的基本安全保护能力如下：

第一级安全保护能力：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：（略）。

信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查

要求标注

业务信息安全类要求（标记为 S 类）

系统服务保证类要求（标记为 A 类）

通用安全保护类要求（标记为 G 类）

第一级　用户自主保护级

第二级　系统审计保护级

第三级　安全标记保护级

第四级　结构化保护级

第五级　访问验证保护级

ISO-27001-2005

11 个域、39 个控制目标、133 个控制措施

1、信息安全方针

2、信息安全组织

3、资产管理

4、人力资源安全

5、物理和环境安全

6、通信和操作管理

7、访问控制

8、信息系统获取、开发与维护

9、信息安全事件管理

10、业务连续性管理

11、符合性

ISO-27001-2013

14 个域、35 个控制目标、114 个控制措施

1、信息安全方针

2、信息安全组织

3、人力资源安全

4、资产管理、

5、访问控制

6、密码学

7、物理和环境安全

8、操作安全

9、通信安全

10、系统的获取、开发及维护

11、供应商关系

12、信息安全事件管理

13、业务连续性管理中的信息安全

14、符合性

ISO-20000

5 大过程 13 个管理：

服务交付过程

服务预算和核算管理

服务报告

能力管理

服务持续性与可用性管理

IT 服务预算和核算管理

信息安全管理

控制过程

配置管理

变更管理

发布过程

发布管理

解决过程

事故管理

问题管理

业务过程

业务关系管理

供应商管理

ITIL

1 个服务台，5 个管理

服务台(Service Desk)

- **事件管理(Incident Management)**
- **问题管理(Problem Management)**
- **配置管理(Configuration Management)**
- **变更管理(Change Management)**
- **发布管理(Release Management)**

CMM 是关于如何改进软件开发流程成熟度的一个模型，它提供了一个阶段模型，具体包括以下几个成熟度等级。

- 初始级(Initial)—— 流程是随机发生的。
- 可重复级(Repeatable)—— 流程是经过设计的从而使得稳定的服务质量是可以重复出现的。

- 已定义级(Defined)—— 流程已经实现了文档化、标准化和集成化。
- 可管理级(Managed)—— 组织对服务成果进行评测，并有意识地利用这个评测结果改进服务质量。
- 优化级(Optimizing)—— 组织有意识地优化其流程设计以改进其服务质量，或者开发新的技术或服务。

1 线支持(也称为第 1 层次支持)通常由服务台来提供

2 线支持则通常由管理部门提供

3 线支持则多由软件开发人员和系统结构人员提供

4 线支持由供应商提供。

优先级=紧急度×影响度

COBIT

Cobit 4.1 划分为 4 个域及 34 个控制目标：

1、规划与组织 PO

PO 1　制定 IT 战略规划

PO 2　确定信息体系架构

PO 3　确定技术方向

PO 4　定义 IT 组织与相互关系

PO 5　管理 IT 投资

PO 6　管理目标与方向的协调

PO 7　人力资源管理

PO 8　确保符合外部要求

PO 9　风险评估

PO 10　项目管理

PO 11　质量管理

2、获取与实施 AI

AI 1　确定解决方案

AI 2　获取并维护应用软件

AI 3　获取并维护技术基础设施

AI 4　程序开发与维护

AI 5　系统安装与验收

AI 6　变更管理

3、交付与支持 DS

DS 1 定义并管理服务水平

DS 2 管理第三方服务

DS 3 绩效管理与容量管理

DS 4 确保持续性服务

DS 5 确保系统安全

DS 6 确认与分配成本

DS 7 教育并培训客户

DS 8 为客户提供帮助和建议

DS 9 配置管理

DS 10 问题管理与紧急事件管理

DS 11 数据管理

DS 12 设施管理

DS 13 运营管理

4、监控与评价 ME

ME1　流程监控

ME2　评价内部控制的适当性

ME3　获得独立保证

ME4　提供独立性审计