第3章 信息安全风险评估的主要内容

3.1 信息安全风险评估工作概述

3.1.1 风险评估依据

风险评估依据国家政策法规、技术规范与管理要求、行业标准或国际标准进行，其依据主要包括：

1. 政策法规

国家信息化领导小组关于加强信息安全保障工作的意见(中办发[2003]27号)。

2. 国际标准

(1) ISO/IEC 27001：2005 信息安全管理体系　要求。
(2) ISO/IEC 27002：2005 信息安全管理实用规则。
(3) ISO/IEC TR 13335 信息技术安全管理指南。
(4) SSE-CMM 系统安全工程能力成熟模型。

3. 国家标准

(1) GB/T 20984—2007 信息安全技术　信息安全风险评估规范。
(2) GB 17859—1999 计算机信息系统安全保护等级划分准则。
(3) GB/T 18336.1～18336.3—2001 信息技术　安全技术　信息技术安全性评估准则。

4. 行业通用标准

(1) CVE 公共漏洞数据库。
(2) 信息安全应急响应机构公布的漏洞。
(3) 国家信息安全主管部门公布的漏洞。

3.1.2 风险评估原则

通过风险评估有助于认清信息环境的安全状况，明确责任达成共识；有助于采取并完

善更加经济有效的安全保障措施；有助于保持信息安全策略的一致性和连续性，从而服务于国家信息化发展，促进信息安全保障体系的建设，提高信息系统的安全保障能力。

风险评估原则包括：可控性原则（人员可控性、工具可控性、项目过程可控性）；完整性原则；最小影响原则；保密原则。具体如下：

1. 可控性原则

1）人员可控性

所有参与信息安全风险评估的人员均应进行严格的资格审查和备案，明确其职责分工，并对人员工作岗位的变更执行严格的审批手续，确保人员可控。评估人员的安排需在评估工作说明中明确定义，并要得到双方的同意、确认。如果根据项目的具体情况，需要进行人员调整时，必须经过正规的项目变更程序，得到双方的正式认可和签署。

2）工具可控性

所使用的风险评估工具均应通过多方综合性能对比、精心挑选，并取得有关专家论证和相关部门的认证。评估工作中所使用的技术工具均事先通告评估对象，向评估对象介绍主要工具的使用方法并进行实验后方可使用。

3）项目过程可控性

评估项目管理将依据项目管理方法学，重视项目管理的沟通管理，达到项目过程的可控性。

2. 完整性原则

严格按照委托单位的评估要求和指定的范围进行全面的评估服务。

3. 最小影响原则

从项目管理层面和工具技术层面，力求将风险评估对信息系统的正常运行的可能影响降低到最低限度。

4. 保密原则

与评估对象签署保密协议和非侵害性协议。

3.1.3　风险评估组织管理

由于信息安全风险评估工作必然涉及系统当中的关键部分和核心信息，敏感性极强，如果处理不当，反而可能引入新的风险。因此，必须高度重视信息安全风险评估的组织管理工作。网络与信息系统的拥有、运营、使用单位和主管部门要按照“谁主管谁负责，谁运营谁负责”的原则，负起严格管理的责任。一方面，对评估者的技术水平要提出高要求；另一方面，参与信息安全风险评估工作的单位及有关人员必须遵守国家信息安全的有关法律法规，承担相应的责任和义务。风险评估工作的发起方必须采取相应保密措施，并与参与评估的有关单位或人员签订具有法律约束力的保密协议。对关系国计民生和社会稳定的基础信息网络和重要信息系统，信息安全风险评估工作必须遵循国家的有关规定。

信息系统风险评估的参与角色一般有主管机关、信息系统拥有者、信息系统承建者、信

息系统安全评估机构、信息系统的关联者(即因信息系统互联、信息交换和共享、系统采购等行为与该系统发生关联的机构)。他们在信息系统安全风险评估中的责任如表 3-1 所示。

表 3-1 风险评估中的角色和责任

角 色	责 任
主管机关	提出、制定并批准本部门的信息安全风险管理策略； 领导和组织本部门内的信息系统安全评估工作； 基于本部门内信息系统的特征以及风险评估的结果，判断信息系统残余风险是否可接受，并确定是否批准信息系统投入运行； 检查信息系统运行中产生的安全状态报告； 定期或不定期地开展新的信息安全风险评估工作
信息系统拥有者	制定安全计划，报主管机关审批； 组织实施信息系统自评估工作； 配合强制性检查评价或委托评估工作，并提供必要的文档等资源； 向主管机关提出新一轮风险评估的建议； 改善信息安全防护措施，控制信息安全风险
信息系统承建者	根据对信息系统建设方案的风险评估结果，修正安全方案，使安全方案成本合理、积极有效，在方案中有效地控制风险； 规范建设，减少在建设阶段引入的新风险； 确保安全组件产品得到了相关机构的认证
信息系统安全评估机构	提供独立的信息系统安全风险评价； 对信息系统中的安全防护措施进行评估，以判断： (1) 这些安全防护措施在特定运行环境中的有效性。 (2) 实现了这些措施后系统中存在的残余风险。 提出调整建议，以减少信息系统中的脆弱性，有效对抗安全威胁，控制风险； 保护风险评估中获得的敏感信息，防止被未授权的、无关人员和单位获得
信息系统的关联机构	遵守安全策略、法规、合同等涉及信息系统交互行为的安全要求，减少信息安全风险； 协助风险评估机构确定评估边界； 在风险评估中提供必要的资源和资料

3.2 风险评估基础模型

3.2.1 风险要素关系模型

要实施风险评估就必须对其要素有一个准确的理解，图 3-1 显示了风险评估的各要素及其关系。其中方框部分的内容为风险评估的基本要素，椭圆部分的内容是与这些要素相关的属性，也是风险评估要素的一部分。

图 3-1 中这些要素之间存在着以下关系：业务战略依赖于资产来完成；资产拥有价值，组织的业务战略越重要，对资产的依赖程度越高，资产的价值就越大；资产的价值越大，则

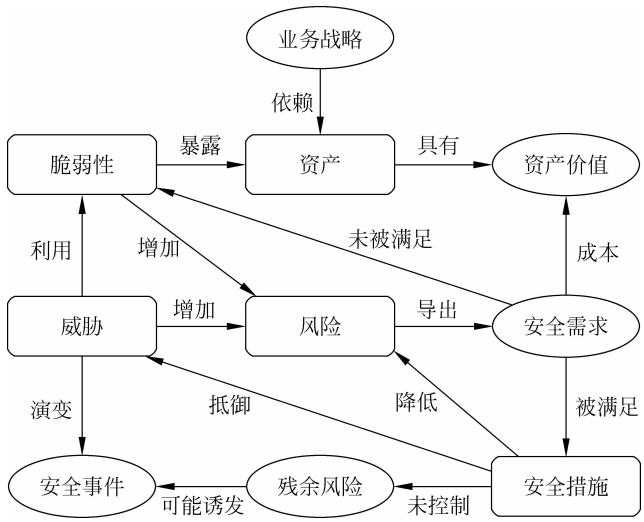

图 3-1　风险评估要素关系图

风险越大；风险是由威胁发起的，威胁越大则风险越大，并可能演变成安全事件；威胁需要利用脆弱性，脆弱性越大则风险越大；脆弱性使资产暴露，是未被满足的安全需求，威胁通过利用脆弱点危害资产，从而形成风险；资产的重要性和对风险的意识将会导出安全需求；安全需求要通过安全措施来得以满足，且是有成本的；安全措施可以抗击威胁，降低风险，减弱安全事件的影响；风险不可能、也没有必要降为零，在实施了安全措施后还会有残留的风险；部分残余风险来自于安全措施可能不当或无效，在以后需要继续控制这部分风险，另一部分残余风险则是在综合考虑了安全的成本与资产价值后，有意未去控制的风险，这部分风险是可以被接受的；残余风险应受到密切监视，因为它可能会在将来诱发新的安全事件。

下面主要参考 ISO/IEC TR 18044、ISO/IEC Guide 73：2002 等国际标准给出相关要素的定义。

资产是任何对组织有价值的事物。

信息安全事件(Event)是指识别出的发生的系统、服务或网络事件，表明可能违反信息安全策略或防护措施失效；或以前未知的与安全相关的情况。

信息安全事故(Incident)是指一个或一系列非期望的或非预期的信息安全事件，这些信息安全事件可能对业务运营造成严重影响或威胁信息安全。

残余风险：实施风险处置后仍旧残留的风险。

接受风险：接受风险的决策。

风险分析：系统地使用信息以识别来源和估计风险。

风险评估：风险分析和风险评价的全过程。

风险评价：将估计的风险与既定的风险准则进行比较以确定重要风险的过程。

风险管理：指导和控制一个组织风险的协调的活动。

风险处置：选择和实施措施以改变风险的过程。

控制目标和控制措施是基于风险评估和风险处理过程的结果和结论、法律法规要求、合

同业务和组织对信息安全的业务要求而确定的。

3.2.2 风险分析原理

风险分析原理如图 3-2 所示。

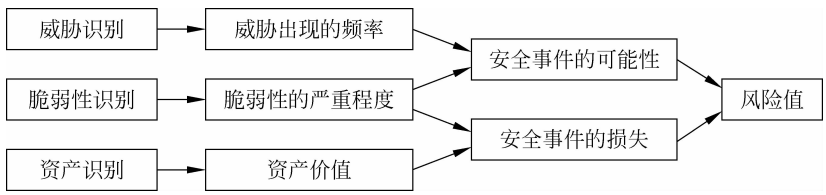

图 3-2 风险分析原理图

风险分析中要涉及资产、威胁、脆弱性等基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。风险分析的主要内容为：

(1) 对资产进行识别，并对资产的价值进行赋值。

(2) 对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值。

(3) 对资产的脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值。

(4) 根据威胁及威胁利用弱点的难易程度判断安全事件发生的可能性。

(5) 根据脆弱性的严重程度及安全事件所作用资产的价值计算安全事件的损失。

(6) 根据安全事件发生的可能性以及安全事件的损失，计算安全事件一旦发生对组织的影响，即风险值。

3.2.3 风险评估方法

评估方法的选择直接影响到信息系统安全风险评估过程中的每个环节，甚至可能影响最终的评估结果，因此需要根据系统的具体情况，选择合适的风险评估方法。风险评估的方法有很多种，概括起来可分为三大类：定性的风险评估方法、定量的风险评估方法、定性与定量相结合的评估方法。

1. 定性评估方法

定性评估方法是目前采用最为广泛的一种方法，它需要凭借评估分析者的经验、知识和直觉，结合标准和惯例，为风险评估要素的大小或高低程度定性分级，带有很强的主观性。定性分析的操作方法可以多种多样，包括小组讨论、检查列表、问卷、人员访谈、调查等。定性分析操作起来相对容易，但可能因为评估分析者在经验和直觉上的偏差而使分析结果失准。

常用的定性评估方法有：安全检查表法、专家评价法、事故树分析法、事件树分析法、潜在问题分析法、因果分析法、作业安全分析法等。

2. 定量评估方法

定量的评估方法对构成风险的各个要素和潜在损失的水平赋以数值或货币的金额，当

度量风险的所有要素(资产价值、威胁可能性、弱点利用程度、安全措施的效率和成本等)都被赋值以后,风险评估的整个过程和结果就可以进行量化。通过定量分析可以对安全风险进行准确的分级,能够获得很好的风险评估结果。但是,对安全风险进行准确分级的前提保证是可供参考的数据指标正确,而这个前提对于信息系统日益复杂多变的今天,是很难得到保证的。由于数据统计缺乏长期性,计算过程又极易出错,定量分析的细化非常困难,所以目前的风险评估分析很少完全只用定量的分析方法进行分析。

常用的定量评估方法有:层次分析法、模糊综合评判法、神经网络、灰色系统预测模型等。

3. 定量分析和定性分析方法的比较

定量的风险评估方法、定性的风险评估方法、定性与定量相结合的评估方法的比较如表 3-2 所示。

表 3-2　定性、定量的风险评估方法比较

名称	定性评估方法	定量评估方法	定量与定性结合方法
定义	主要依据研究者的知识、经验、历史教训、政策走向及特殊案例等非量化资料对系统风险状况做出判断的过程	运用数量指标来对风险进行评估	定量分析是基础和前提;定性分析是灵魂,是形成概念、观点,做出判断,得出结论所必须依靠的
优点	可以挖掘出一些蕴藏很深的思想,使评估的结论更全面、更深刻;便于企业管理、业务和技术人员更好地参与分析工作,大大提高分析结果的适用性和可接受性	能够通过投资收益计算的客观结果来说服企业管理人员来推动风险管理;随着组织建立数据的历史记录并获得经验,其精确度将随着时间的推移而提高	在复杂的信息系统风险评估过程中,将这两种方法融合起来,取其优点
缺点	主观性很强,对评估者本身的要求很高;缺乏客观数据支持	计算过程复杂、耗时,需要专业工具支持和一定的专业知识基础;计算结果量化以后用财务术语描述有可能被误解和曲解	难度大,复杂度高

3.2.4　风险评估实施流程概述

要对一个复杂的信息系统进行正确的评估,并使得这个过程更有效率、更具可操作性,一个科学、合理的评估流程必不可少。图 3-3 给出了一个比较通用的评估实施流程。

风险评估准备:组织评估信息系统的安全性是一种战略性的考虑。评估前充分的准备能保证整个风险评估过程的有效性。

风险因素识别:包括资产识别、威胁识别和脆弱性识别、现有安全控制措施确认。通过前期准备阶段收集到的信息,将划入范围和边界的资产进行确认评估,并根据资产目前所处的环境条件和以前的报告记录情况来识别每项资产可能面临的威胁,对每一项需要保护的信息资产,找到可能被威胁利用的脆弱点并对其进行评估。现有的安全控制措施也是威胁事件发生的决定因素之一,因此也需要确认。

风险分析管理:依据前面对资产、威胁、脆弱性以及现有安全风险控制措施的识别结

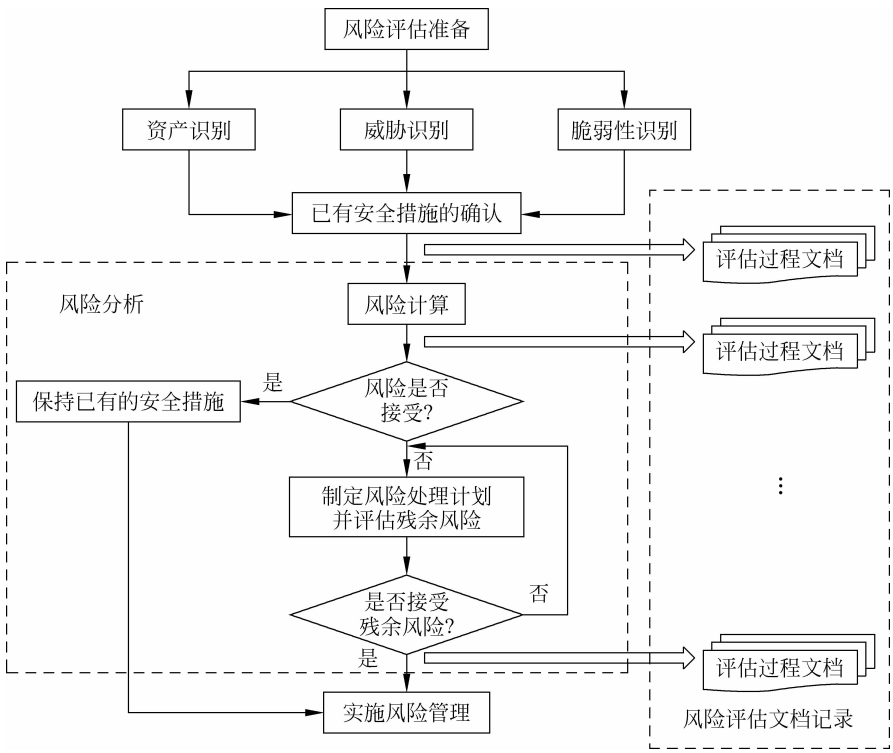

图 3-3 风险评估流程实施图

果,通过给定的风险计算模型进行风险计算,确定出各种风险所处的安全等级,并针对高风险区域给出风险控制方案。没有绝对的安全,风险评估的最终目的是使信息系统的安全风险降低到用户和决策者能够接受的程度。

风险评估文档记录:在项目进展过程中,风险评估的方法和结果都可能发生变化,所以详尽而完整的文档和材料非常重要。

信息系统的风险评估管理是一个不断降低风险的过程,可能需要进行多次评估。每次可根据条件和目的的不同,对这些步骤进行适当的调整。

3.3 风险评估相关标准

3.3.1 国外信息安全风险评估相关标准

1. OCTAVE

1) OCTAVE 简介

OCTAVE(Operationally Critical Threat, Asset and Vulnerability Evaluation,可操作的关键威胁、资产和弱点评估)是由美国卡耐基·梅隆大学软件工程研究所下属的 CERT 协调中心开发的一种信息安全风险评估的方法。这是一种信息安全风险评估规范,是从组织的角度开发的一种信息安全保护方法。

OCTAVE 信息安全风险评估方法，由一系列循序渐进的讨论会组成，每个讨论会都需要其参与者之间的交流和沟通。其核心是自主原则，即由组织内部的人员管理和指导该组织的信息安全风险评估。信息安全是组织内每个成员的职责，而不只是 IT 部门的职责。组织内部的人员需要负责信息安全评估活动，并对改进信息安全的工作做出决策。

OCTAVE 使组织能够理清复杂的组织问题和技术问题，了解安全问题，改善组织的安全状况并解决信息安全风险，而无须过分依赖外部专家和厂商。OCTAVE 包括两种具体方法：面向大型组织的 OCTAVE Method 和面向小型组织的 OCTAVE-S。

2) OCTAVE Method

OCTAVE Method 是为有 300 名以上员工的大型组织而设计的，但可以以此为基线或起点，对该方法进行开发剪裁，使它适合于不同规模的组织、业务环境或工业部门。

OCTAVE Method 包括三个阶段 8 个过程。

第 1 阶段：建立基于资产的威胁配置文件

这是从组织的角度进行评估，这一阶段的目标是建立组织对信息安全问题的概括认识。要实现这一目标，首先需要采集组织内员工对安全问题的个人观点，然后对这些个人观点进行综合整理，为评估过程中的所有后续分析活动提供依据。通过对组织专业领域知识的调研，可以清楚地表明员工对信息资产、资产面临的威胁、资产的安全需求、组织现行保护信息资产的措施等有关问题的理解。本阶段主要由 4 个过程组成。

(1) 过程 1：收集高层管理部门的观点，参与者为组织的高层管理人员。

(2) 过程 2：收集业务区域管理部门的观点，参与者为组织业务区域经理。

(3) 过程 3：收集员工的观点，参与者是组织的一般员工，信息技术部门的员工通常与一般的员工分开，参与一个独立的讨论会。

(4) 过程 4：建立威胁配置文件，包括整理过程 1～3 中所收集的信息、选择关键资产、提炼关键资产的安全需求、标志对关键资产构成影响的威胁等工作。

通用的配置文件是基于关键资产的威胁树。

第 2 阶段：识别基础设施的薄弱点

这一阶段也称为 OCTAVE Method 的“技术观点”。因为在这一阶段，分析人员的注意力转移到组织的计算基础设施上。在这一阶段中，对当前信息基础设施的评价包括数据收集和分析活动。通过检查信息技术基础结构的核心运行组件，可以发现导致非授权行为的漏洞或技术脆弱性。本阶段主要由两个过程组成。

(1) 过程 5：识别关键单元，包括识别结构单元的种类、要分析的基础设施的结构单元等。

(2) 过程 6：评估选定的单元，包括对选定的基础设施的结构单元进行薄弱点检查、对技术薄弱点进行评审并总结。

第 3 阶段：开发安全策略和计划

第 3 阶段旨在理解迄今为止在评估过程中收集到的信息，即分析风险。在这一阶段中，需要开发出解决组织内部存在的风险和问题的安全策略和计划。通过分析阶段 1 和阶段 2 中对组织和信息基础结构评估中得到的信息，可以识别出组织面临的风险，同时基于这些风险可能给组织带来的不良影响对其进行评估。此外，还要按照风险的优先级顺序制定出组织保护策略和风险缓解计划。本阶段主要由两个过程组成。

(1) 过程 7：执行风险分析，包括识别关键资产的威胁、制定风险评估标准、评估关键资产的威胁所产生的影响等。

(2) 过程 8：开发保护策略，评估小组开发整个组织的保护策略，该策略注重提高组织的安全实践，以及关键资产的重要风险的削减计划。

OCTAVE 的关键结果包括组织改进其安全状态的保护策略和减少组织关键资产风险的缓和计划。然而，评估结果仅为组织改进安全状态指明了方向，但不一定有重大改进。为了有效地管理信息安全风险，必须根据风险评估的结果开发详细的行动计划，并对这些计划的实施进行管理。

3) OCTAVE-S

OCTAVE-S 即 OCTAVE 简化版，是为规模较小的组织而开发的，这里将 20～80 名员工的组织视为小规模的组织。通过这种方法，3～5 人的评估小组就可以完成整个评估活动。与 OCTAVE Method 一样，OCTAVE-S 评估方法同样包括三个阶段，但其中的过程有些不同。

第 1 阶段：建立资产的威胁描述文件

本阶段主要由两个过程组成。

(1) 过程 S1：收集组织信息。分析小组应识别与组织重要信息相关的资产，确定一组评估标准，并定义组织当前的安全实践状况。

(2) 过程 S2：建立威胁描述。分析小组应选择 3～5 个关键信息资产，并为每个关键信息资产定义相应的安全要求和威胁描述文件。

第 2 阶段：识别基础设施的薄弱点

本阶段主要由一个过程组成。

过程 S3：检查与关键信息资产相关的计算基础设施。分析小组对关键资产支持系统中的访问路径进行分析，并确定这些技术措施对关键资产的保护程度。

第 3 阶段：开发安全策略和计划

本阶段主要由两个过程组成。

(1) 过程 S4：确定和分析风险。分析小组就风险所产生的影响、发生的可能性进行评估。

(2) 过程 S5：开发保护策略和风险降低计划。评估小组根据实际情况，开发一个整个组织范围的保护策略和风险削减计划。

2. SSE-CMM

1) SSE-CMM 概述

SSE-CMM 是 System Security Engineering Capability Maturity Model(系统安全工程能力成熟度模型)的缩写，它源于 CMM(能力成熟度模型)的思想和方法，是 CMM 在系统安全工程领域的应用，SSE-CMM 是偏向于对组织的系统安全工程能力的评估标准。

SSE-CMM 模型将信息系统安全工程分为三个相互联系的部分：风险评估、工程实施和可信度评估。针对这三个部分 SSE-CMM 定义了 11 项关键过程，并为每个过程定义了一组完成该过程必不可少的、确定的基本实践。同时模型还定义了 5 个能力成熟度等级，每个等级的判定反映为一组共同特性，而每个共同特性进而通过一组确定的通用实践来描述，通

用实践是对所有过程通用的工程实践。只有某一级别的所有共同特性都得到满足时，该过程的实施能力才达到对应的能力级别。

从整体上看，SSE-CMM 模型定义了一个“二维”架构，横轴上是 11 个系统安全工程的过程域，纵轴上是 5 个能力成熟度等级，如果给每个过程域赋予一个能力成熟度等级的评定，所得到的“二维”图形便形象地反映了安全工程的质量以及工程在安全上的可信度，也间接地反映了工程队伍实施安全系统工程的能力成熟性。

2）安全工程过程

（1）风险过程

风险是潜在的威胁、利用有用资源的脆弱性造成资源的破坏和损失。风险事件有三个组成部分：威胁、系统脆弱性、事件造成的影响。

安全机制在系统中存在的根本目的是将风险控制在可接受的程度内，SSE-CMM 模型定义了 4 种风险过程：评估威胁过程（PA04）、评估脆弱性过程（PA05）、评估风险事件影响过程（PA02），以及在前三种过程基础上的评估安全风险过程（PA03）。

（2）工程过程

安全工程是一个包括概念、设计、实现、测试、部署、运行、维护、废弃的完整过程。针对工程实施管理，SSE-CMM 模型定义了安全需求说明过程（PA10）、安全方案制定过程（PA09）、安全控制实施过程（PA01）、安全状态监测过程（PA08）。安全工程不是一个独立的实体，而是整个信息系统工程的一个组成部分，模型强调系统安全工程与其他工程的合作和协调，并定义了专门的协调安全过程（PA07）。

（3）保证过程

保证是指安全需求得到满足的信任程度。用可信度描述对建立的安全系统正确执行其安全功能的信心究竟有多大信任程度。传统方法是面向最终系统的方法，通过对系统所有文档和产品的严格分析和测试来建立可信度指标。但这种测试结果缺少继承性，当前工程的安全可信度与同一实施队伍依照类似工程过程在此之前所完成的工程的安全可信度并无直接关系，对每个工程的评测都要从头做起，于是导致了测试过程的复杂和冗长。SSE-CMM 模型在信任度问题上强调对安全工程结果可重复性的信任程度，它通过对现有系统安全体系真实性和有效性的测试（PA11）来构造系统安全可信度论据（PA06）。

3）能力成熟度等级

SSE-CMM 模型定义了 5 个能力级别。

1 级：非正式执行的过程。仅仅要求一个过程域的所有基本实践都被执行，而对执行的结果并无明确要求。

2 级：计划并跟踪的过程。这一级强调过程执行前的计划和执行中的检查。这使工程组织可以基于最终结果的质量来管理其实践活动。

3 级：完善定义的过程。过程域的所有基本实践均应依照一组完善定义的操作规范来进行。这组规范是实施队伍根据以往经验制定出来的，其合理性是验证过的。

4 级：定量控制的过程。能够对实施队伍的表现进行定量的度量和预测。过程管理成为客观的和准确的实践活动。

5 级：持续改善的过程。为过程行为的高效和实用建立定量的目标。可以准确地度量过程的持续改善所收到的效益。

3. GAO/AIMD

1998 年 5 月，美国审计总署(GAO)出版了《信息安全管理指南——向先进公司学习》(GAO/AIMD-98-68)，并出版了其支持性文件《信息安全风险评估指南——向先进公司学习》(GAO/AIMD-99-139)，GAO/AIMD-99-139 风险评估指南有针对性地对风险评估过程进行了分析和阐述，是在开展类似公司风险评估工作的过程中可以参考和借鉴的标准。

1) GAO/AIMD-99-139 的组成

GAO/AIMD-99-139 由三个部分组成：

第 1 部分是引言，介绍了风险评估指南的产生背景、风险评估在风险管理中的地位、风险评估过程的基本要素，以及信息安全风险评估过程中的难点。

第 2 部分给出了第 3 部分案例研究的概述，分析了风险评估过程中关键的成功因素、风险评估工具，以及风险评估带来的益处。

第 3 部分案例分析，美国审计总署从调查的众多组织中挑选了有代表性的 4 个组织，对他们的风险评估过程进行了分析和阐述。

GAO/AIMD-99-139 风险评估指南给出了风险评估指南的目标和方法论。

2) 风险评估过程的基本要素

风险评估过程通常要包括下列要素：

(1) 识别可能危害关键运作和资产并对其造成负面影响的威胁。

(2) 在历史信息及有经验人员判断的基础上，估计此类威胁发生的现实可能性。

(3) 识别并评价可能受到此类威胁发生影响的运作和资产的价值、敏感度和关键度，以确定哪些运作和资产是重要的。

(4) 对最关键、最敏感的运作和资产，估计威胁发生可能造成的潜在损失或破坏，包括恢复成本。

(5) 识别经济有效的措施以减轻或降低风险。

(6) 将结果形成文件并建立活动计划。

4. TCSEC

1985 年，美国颁布了可信计算机系统评估标准(Trusted Computer System Evaluation Criteria，TCSEC)，该标准为计算机安全产品的评测提供了测试内容和方法，指导信息安全产品的制造和应用，通常称为信息安全橘皮书。它将安全分为 4 个方面(安全政策、可说明性、安全保障和文档)和 7 个安全级别(从低到高依次为 D、C1、C2、B1、B2、B3 和 A 级)。

5. ISO/IEC 15408(CC)

信息安全产品和系统安全性测评标准，是信息安全标准体系中非常重要的一个分支，这个分支的发展已经有很长历史了，期间经历了多个阶段，先后涌现了一系列的重要标准，包括 TCSEC、ITSEC、CTCPEC 等，而信息产品通用测评准则(Common Criteria，CC)则是最终的集大成者，是目前国际上最通行的信息技术产品及系统安全性评估准则，也是信息技术

安全性评估结果国际互认的基础。

CC 的发展经历了一个漫长而复杂的过程，如图 3-4 所示。

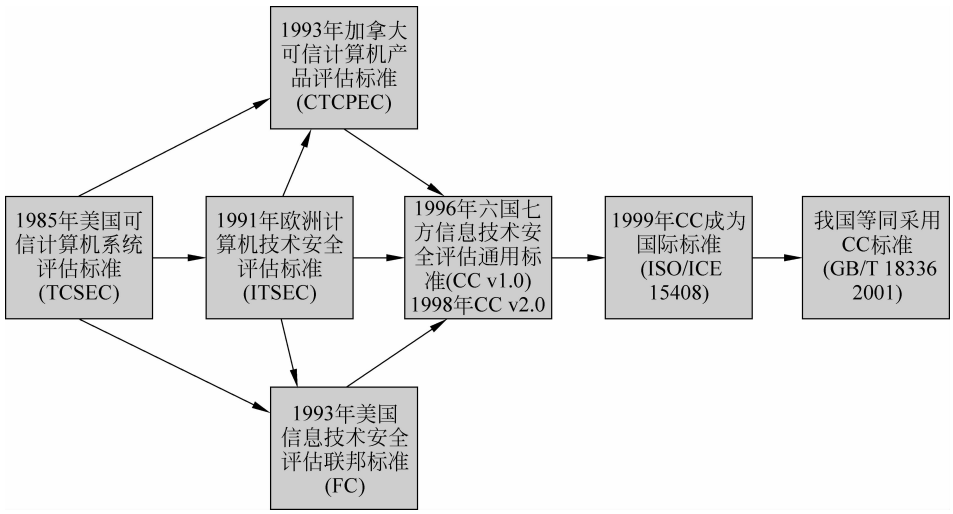

图 3-4　CC 的发展过程

从图 3-4 可以看出，CC 是由 TCSEC 等标准发展而来的；CC、ISO/IEC 15408 和 GB/T 18336 实际上是同一类标准，只不过 CC 是最早的称谓，ISO/IEC 15408 是正式的 ISO 标准，GB/T 18336 则是我国等同采用 ISO/IEC 15408 之后的国标。

CC 定义了评估信息技术产品和系统安全性所需的基础准则，是度量信息技术安全性的基准。它针对在安全评估过程中信息技术产品和系统的安全功能及相应的保证措施提出了一组通用要求，使各种相对独立的安全评估结果具有可比性，这有助于信息技术产品和系统的开发者或者用户确定产品或系统对其应用是否足够安全，以及在使用中存在的安全风险是否可以容忍。

CC 的主要目标读者是用户、开发者和评估者。CC 标准由三个文件构成，如表 3-3 所示。

表 3-3　CC 标准组成

代号	名　　称	简　　介
ISO/IEC 15408-1	Introduction and general model	介绍和一般模型。该部分定义了 IT 安全评估的基本概念和原理，提出了评估的通用模型
ISO/IEC 15408-2	Security functional requirements	安全功能要求。该部分按照“类-子类-组件”的方式提出了安全功能要求
ISO/IEC 15408-3	Security assurance requirements	安全保证要求。该部分定义了评估保证级别，介绍了“保护轮廓”和“安全目标”的评估，提出了安全保证要求

通过依据某个标准的风险评估或者得到该标准的评估认证，不但可为信息系统提供可靠的安全服务，而且可以树立单位的信息安全形象，提高单位的综合竞争力。

6. NIST SP800-30

NIST SP800-30 是由美国国家标准和技术学会(The National Institute of Standards and Technology,NIST)颁布的“信息技术系统风险管理指南”,提供了把风险减少到一个可接受水平的非强制性指导原则,这个指南为开发一个有效的风险管理程序奠定了基础,包括一些定义和评估与减少 IT 系统内的风险所需的实用指南。

风险管理对一个组织通过以有效方式保护和管理 IT 资源来完成其使命非常重要。风险管理也支持信息系统的认证和鉴定。

在风险管理中担任一定角色的关键人员如下:高级管理者、首席信息官(Chief Information Officer,CIO)、系统和信息的所有者、商业和部门经理、信息系统安全官员(Information System Security Officer,ISSO)、IT 安全从业人员、安全意识培训师。

NIST SP800-30 将风险定义为既定威胁源利用特定潜在漏洞的可能性和该负面事件对组织造成的影响的函数。

NIST SP800-30 定义风险管理具有以下三种成分:风险评估、风险缓解、风险评价。

风险评估包括以下步骤:系统表征、威胁识别、漏洞识别、控制分析、可能性判断、影响分析、风险确定、控制建议、结果文档。

风险缓解优先考虑从风险评估活动中得出的被推荐的控制措施。要对控制措施进行成本效益分析,以把风险限制到完成组织任务所需的一个可接受的水平。为了缓解风险,可以运用技术、管理和操作控制。风险缓解包括以下方面:风险规避、风险承担、风险限制、风险转移、风险规划和研发。

一个组织经常会经历人事、网络体系结构和信息系统的变动,因此风险管理是一个连续过程,需要不断进行评价和评估。

3.3.2 国内信息安全风险评估相关标准

1. GB/T 20984—2007 信息安全技术 信息安全风险评估规范

本标准提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法,以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。本标准适用于规范组织开展的风险评估工作。

随着我国信息化应用的逐步深入,信息安全问题也日益受到关注,针对我国没有信息安全风险评估标准的现状,2004 年,国信办组织专家启动信息安全风险评估的研究与标准的编制工作,标准编制工作于 2004 年 3 月正式启动,2007 年 7 月通过了国家标准化管理委员会的审查批准,标准编号和名称为 GB/T 20984—2007《信息安全技术 信息安全风险评估规范》,于 2007 年 11 月正式实施。

GB/T 20984—2007《信息安全技术 信息安全风险评估规范》包括正文和附录两部分,正文由前言、引言和 7 章内容组成,附录部分包括附录 A 和附录 B,均为资料性附录。

前言:对本标准的制定作了简单介绍。

引言:简单介绍了信息安全风险评估的重要性。

第 1 章 范围:阐述了本标准的范围。

第 2 章　规范性引用文件：阐述了本标准的规范性引用文件。

第 3 章　术语和定义：给出了信息安全风险评估中涉及的术语和它们的定义。

第 4 章　风险评估框架及流程：阐述了信息安全风险评估中各要素的关系、风险分析的原理、风险评估的实施流程。

第 5 章　风险评估实施：详细介绍了信息安全风险评估的实施过程及每一阶段的具体任务和职能。

第 6 章　信息系统生命周期各阶段的风险评估：阐述了信息安全风险评估在信息系统生命周期各阶段中的不同要求。

第 7 章　风险评估的工作方式：介绍了风险评估的两种形式、自评估和检查评估。

附录 A 风险的计算方法：详细介绍了目前比较常用的两种风险计算方法，即矩阵法和相乘法。

附录 B 风险评估工具：对当前的风险评估工具进行了分类和综述。

2. 其他标准

GB/T 18336—2001《信息技术　安全技术　信息技术安全性评估准则》是 2001 年参照国际标准 ISO/IEC 15408：1999，我国制定的在信息安全技术方面的第一个国家标准，作为评估信息技术产品与信息安全特性的基础准则。GB/Z24364—2009 是信息安全风险管理指南。

3.4　风险评估工具

风险评估工具是一种辅助性的手段，通过对某一个系统对象的自动化或半自动化的分析，反映出系统主要部件的客观状况。评估工具还能够将专家知识进行集中，通过专家知识的应用，在风险评估中发挥重要的辅助作用。根据工具应用的目标和在风险评估中的工作方式，可将风险评估工具分为：主动型评估工具、被动型评估工具、管理型评估工具三种类型。

主动型评估工具是基于某种固定的“询问—回答”模式，将某些人工指令操作集成在一起自动执行。“询问－回答”方式是建立在大量设备知识或协议知识基础上的，如通过对服务器某个端口的询问，并分析设备的返回结果而得到关于该设备端口状况的结论。主动型评估工具集成的知识可以弥补评估人员知识面的不足。各类扫描器是典型的主动型评估工具，如 Tenable Nessus、X-Scan、AppDetective、ISS DBScanner、Metasploit Framework 等。被动型评估工具是一种立足于“防御”的角度收集系统信息并进行简单分析的工具。最典型的被动型评估工具如入侵检测产品、网络监控流量分析产品、主机完整性检测产品等。与主动型评估工具不同，被动型评估工具并不主动“询问”评估对象，而是采用被动方式捕获目标信息系统数据，收集评估所需要的数据和资料，发现存在的薄弱点，帮助完成现状分析和趋势分析。目前比较常用的被动型评估工具有：SnifferPro、Wildpackets Etherpeek NX、Fluke DSP4000 等。管理型评估工具可以直接使用主动型评估工具的评估结果，甚至可以将主动型、被动型评估工具集成在系统中。目前比较常用的管理型评估工具有 CRAMM、COBRA、IAS 等。表 3-4 给出了几种典型的风险评估与管理工具的比较分析。

表 3-4 综合风险评估与管理工具的比较

工具名称	COBRA	RA	CRAMM	@RISK	BDSS
组织/国家	BSI/Britain	BSI/Britain	CCTA/Britain	Palisade/America	The Integrated Risk Management Group/American
体系结构	客户-服务器	单机版	单机版	单机版	单机版
采用方法	专家系统	过程式算法	过程式算法	专家系统	专家系统
定性/定量算法	定性/定量结合	定性/定量结合	定性/定量结合	定性/定量结合	定性/定量结合
数据采集形式	调查问卷	过程	过程	调查文件	调查问卷
对使用人员的要求	不需要有风险评估的专业知识	依靠评估人员的知识与经验	依靠评估人员的知识与经验	不需要有风险评估的专业知识	不需要有风险评估的专业知识
结果输出形式	风险等级与控制措施	风险等级与控制措施	风险等级与控制措施	决策支持信息	安全防护措施列表

思考题

1. 简单叙述风险评估依据的主要内容。
2. 简单叙述风险评估原则的主要内容。
3. 解释风险要素关系模型。
4. 叙述风险分析原理。
5. 论述风险评估方法。
6. 叙述风险评估实施流程。
7. 查阅资料,归纳国内外信息安全风险评估相关标准。