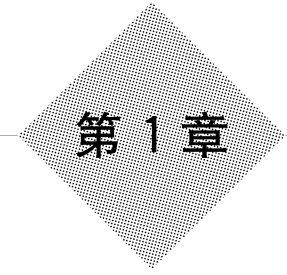

信息安全风险评估发展状况

1.1 信息安全风险评估概述

信息安全风险评估通过对信息系统的资产、面临威胁、存在的脆弱性、采用的安全控制措施等进行分析，从技术和管理两个层面综合判断信息系统面临的风险。

1.1.1 基本概念

信息安全风险是人为或自然的威胁利用系统存在的脆弱性引发的安全事件，并由于受损信息资产的重要性而对机构造成的影响。

信息安全风险评估，就是从风险管理角度，运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，并为防范和化解信息安全风险，或者将风险控制在可接受的水平，从而最大限度地保障网络和信息安全提供科学依据。

信息安全风险评估是信息安全保障体系建立过程中的重要的评价方法和决策机制。没有准确及时的风险评估，将使得各个机构无法对其信息安全的状况做出准确的判断。因为任何信息系统都会有安全风险，信息安全建设的宗旨之一，就是在综合考虑成本与效益的前提下，通过安全措施来控制风险，使残余风险降低到可接受的范围内。

1.1.2 现实意义

通过信息安全风险评估可以有助于认清信息安全环境和信息安全状况，明确信息化建设中各级的责任，采取或完善更加经济有效的安全保障措施，保证信息安全策略的一致性和持续性，并进而服务于国家信息化发展，促进信息安全保障体系的建设，全面提高信息安全保障能力。其现实意义具体体现在以下几个方面：

1. 风险评估是加强信息安全工作的客观需要

信息安全的实现是一个不断变化的复杂过程，它贯穿于信息系统建设的整个生命周期。信息安全的威胁可能来自内部破坏、外部攻击、内外勾结进行的破坏以及信息系统本身所产生的意外事故。只有按照风险管理的思想，适时开展风险评估工作，才能妥善应对可能发生的问题。因此，加强风险评估工作是信息安全新形势下的客观需要。

2. 风险评估是信息安全建设和管理的关键环节

所有信息系统的安全建设和管理都应该在科学的风险评估的基础上进行，只有正确而全面地了解和掌握系统安全风险后，才能在控制风险、减少风险和转移风险之间做出正确的判断，从而决定调动多少资源、以多大的代价、采取什么样的应对措施去化解、控制风险。因此，在信息系统安全建设和管理的全过程中都要充分重视风险评估工作。

3. 风险评估是需求主导和突出重点原则的具体体现

信息安全工作的实践告诉我们，风险是客观存在的，试图完全消灭风险或完全避免风险是不现实的。要根据信息及信息系统的价值、威胁的大小和可能出现的问题的严重程度，以及在信息化建设不同阶段的信息安全要求，坚持从实际出发、需求主导、突出重点、分级防护，科学评估风险并有效地控制风险。

4. 风险评估是科学分析并确定风险的过程

任何系统的安全性都可以通过风险的大小来衡量。科学地分析系统的安全风险，综合平衡风险和代价构成了风险评估的基本过程。风险评估是风险评估理论和方法在加强信息系统安全中的运用，是科学地分析理解信息和信息系统

在机密性、完整性和可用性等方面所面临的风险，通过转移、避免和对抗等措施减少风险，确保把风险控制在可以接受的范围内。

1.2　国外信息安全风险评估发展状况

1.2.1　美国信息安全风险评估状况

1. 发展阶段

美国是国际上对风险评估研究历史最长和工作经验最丰富的国家。随着信息化应用需求的牵引，安全事件的驱动和信息安全技术、信息安全管理概念的深化，对风险评估的认识也逐步加深。美国从最初关注计算机的保密发展到目前关注信息系统基础设施的安全保障，大体经历了以下三个阶段：

(1) 第一个阶段(20 世纪 60 年代至 70 年代)：以计算机为对象的保密阶段

由于计算机开始应用于政府军队，信息保密问题引起关注。1967 年 11 月，美国国防科学委员会委托兰德公司、迈特公司(MITIE)及其他和国防工业有关的一些公司，开始研究计算机安全问题。到 1970 年 2 月，经过将近两年半的工作，主要对当时的大型机、远程终端进行了研究分析，进行了第一次比较大规模的风险评估。

在 20 世纪 70 年代、80 年代，美苏几乎同时着力加强了信息安全标准建设。特别是美国，先是在 70 年代完成了电磁泄漏(即 TEMPEST)对抗标准的制定，并于 70 年代末、80 年代初推出了密码标准，接着又制定了“联邦信息处理标准”和“国家计算机安全标准”等系列标准。在这一时期，美国国防部(DoD)开始制定有关计算机安全的比较重要的法规、指令和标准(5200. 28、5200. 28M、5200. 28 STD)，并正式提出了关于加强美国联邦政府和国防系统计算机安全的倡议，NBS、美国空军、兰德公司、迈特公司等都积极参与其中，开始大规模地研究计算机安全的理论、系统结构以及有关加强安全的手段，产生了 BLP 模型，形成了早期的访问控制的模型。

这一阶段的特点是仅重点针对计算机系统的保密性问题提出要求，因此对安全的评估只限于保密性。

(2) 第二个阶段(20 世纪 80 年代至 90 年代)：以网络为对象的保护阶段

随着计算机系统网络化应用的开展，出现了初期的针对美国军方计算机的

黑客行为，1988 年至 1989 年，美国的计算机网络出现了一系列重大事件。美国的审计总署(GAO)对美国国内主要由国防部使用的计算机网络进行了大规模的持续评估。

在这一阶段，评估标准也有了较大发展。1981 年至 1985 年，美国国防部组织了很大的研究力量研究橘皮书。后来，在这个基础上，网络、审计以及其他方面的安全工作形成了一套大约包括四十多个标准的彩虹系列。这就形成了美国早期的一套比较完整的从理论到方法的有关信息安全评估的准则。1993 年美国和欧洲四国(英、法、德、荷)、加拿大以及国际标准化机构(ISO)开始共同制定信息技术安全通用评估准则(CC)，1999 年成为国际标准 ISO/IEC 15408。

除机密性之外，完整性、可用性等安全属性被逐步认识，同时从对操作系统安全的关注扩展到操作系统、网络和数据库等多个领域。

这一阶段保障系统安全的重点是对安全产品的质量保证和测评，奠定了安全产品测评认证的基础和工作程序。

(3) 第三个阶段(20 世纪 90 年代末到 21 世纪初)：以信息基础设施为对象的保障阶段

2000 年前后，计算机网络系统成为关键基础设施的核心，国际范围内出现了大规模黑客攻击，以及信息战的理论逐步走向成熟，信息攻防成为战争手段和国家综合利用的一种方式，且美国的军事、政治、经济和社会活动对信息基础设施的依赖程度达到了空前的高度，迫使美国又开始了对信息系统新一轮的评估和研究，产生了一些新的概念、法规和标准。

在军方提出信息保障(IA)概念的基础上，克林顿和布什两届总统持续数年进行了国家信息安全保护计划和信息保障战略的研究。到目前为止，形成了与国家安全、反恐战略、国土安全等国家战略相配套的网络空间信息保障的国家战略。各个行业也逐步提出了本行业的信息安全战略，风险评估思想在其中得到了重要的贯彻。

在研究制定信息系统安全认证和认可制度的过程中，美国明确提出了 CC 标准和 FIPS 140-2 仅仅适合实验室环境的安全产品测评认证。虽然它们可以看成是对信息系统进行认证认可的基础，但是仍不能够满足实践的需要。现实世界中，系统的评估除了技术因素外还要关注管理、人员和运行安全。而以 SP 800-37 为核心的一组指南就是为了这个问题提出的。这些指南突出了与法律的一致性，明确了风险评估贯穿于信息系统生命周期各个阶段的任务。

2. 认证认可计划

自 9.11 事件以来，美国政府高度重视信息安全问题。于 2002 年通过的《联邦信息安全管理法案》(FISMA)规定必须对联邦政府信息系统进行安全评估并备案，为美国政府机构信息系统改善信息安全问题设定了目标，也被称作美国电子政务法案。FISMA 为美国联邦政府信息安全设定了目标，却没有规定如何实现这些目标。为此，美国国家技术与标准局(NIST)负责为实现这些目标制定最低的安全要求，NIST 因此专门启动了信息系统安全认证认可计划，该计划后来被更名为信息系统安全计划。该计划分为两个阶段：第一阶段是制定联邦信息和信息系统的分类，联邦信息系统选择和规定安全控制，验证联邦信息系统安全控制的有效性等标准和指南；第二阶段将在美国国内建立一个国家级的基于 NIST 标准和指南的安全评估服务机构，为联邦政府提供经济高效的、高质量的评估服务。

为此，NIST 定义了总体的信息系统安全框架图，如图 1.1 所示。

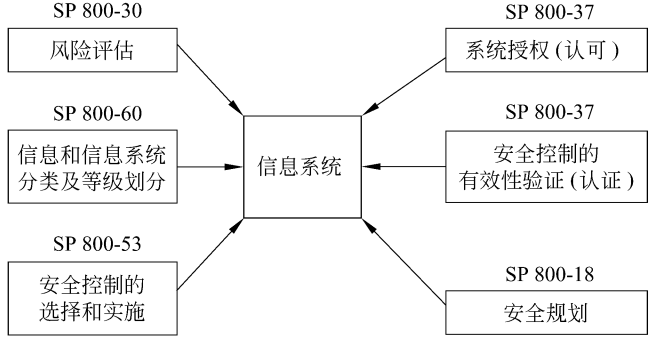

图 1.1　信息系统安全框架

从图 1.1 中可见，新建或再建的信息系统必须实施定期的风险评估(SP 800-30)，分析信息系统面临的威胁、信息系统存在的脆弱性，以确定信息系统遇到安全事件后可能的损失及由此导致的风险；同时，风险评估将为信息系统确定其安全需求；随后，应根据风险评估中确定的信息系统在机密性、完整性和可用性方面存在的风险，确定信息系统的安全类别和等级(FIPS 199)；针对信息系统的安全类别和等级，为其选择有效的安全控制(SP 800-53)，以实现合适的安全等级(SP 800-60)。上述过程确定的安全需求、安全控制均将列入信息系统的安全计划(SP 800-18)并得到实施(SP 800-53)。此后，应定期通过风险评估来衡量信息系统中安全控制的有效性，即信息系统安全认证工作(SP 800-37)；最终，

基于安全控制的有效性和残余风险值，由联邦机构的高级官员决定是否授权信息系统投入运行，即信息系统的安全认可工作(SP 800-37)。而且由于信息技术的发展、业务需求的变革、外部环境的变化均可能使信息系统的安全态势发生改变，因此上述过程是动态的，且需定期重复。

综上可见，美国联邦政府信息系统的安全工作是在信息系统整个生命周期中进行的，而整个信息系统安全工作的关键控制点则是信息安全风险评估。

1.2.2 英国 BS 7799 标准

1. 标准概述

BS 7799 标准是由英国标准协会(BSI)制定的信息安全管理标准，是目前国际上具有代表性的信息安全管理体系标准。英国标准协会是全球领先的国际标准、产品测试、体系认证机构。我们所熟知的 ISO 9000(质量管理体系)、ISO 14001(环境管理体系)、OHSAS 18001(职业健康与安全管理体系)、QS-9000 / ISO/TS 16949(汽车供应行业的质量管理体系)以及 TL 9000(电信供应行业的质量管理体系)均是由英国标准协会发起制定的。因此，如果企业已经实施了 ISO 9000，就很容易整合实施其他的管理标准，当然也包括 BS 7799。

BS 7799 主要提供了有效地实施 IT 安全管理的建议，介绍了安全管理的方法和程序。用户可以参照这个完整的标准制订出自己的安全管理计划和实施步骤，为公司发展、实施和估量有效的安全管理实践提供参考依据。BS 7799 信息安全管理体系标准强调风险管理的思想。传统的信息安全管理基本上还处在一种静态的、局部的、少数人负责的、突击式、事后纠正式的管理方式，导致的结果是不能从根本上避免、降低各类风险，也不能降低信息安全故障导致的综合损失。而 BS 7799 标准基于风险管理的思想，指导机构建立信息安全管理体系(ISMS)。ISMS 是一个系统化、程序化和文件化的管理体系，基于系统、全面、科学的安全风险评估，体现预防控制为主的思想，强调遵守国家有关信息安全的法律法规及其他合同方要求，强调全过程和动态控制，本着控制费用与风险平衡的原则合理选择安全控制方式保护机构的关键信息资产，使安全风险的发生概率和结果降低到可接受的水平，确保信息的机密性、完整性和可用性，保持机构业务运作的持续性。

2000 年 12 月，BS 7799-1 通过国际化标准机构认可，正式成为国际标准 ISO 17799，这是通过 ISO 表决最快的一个标准，足见世界各国对该标准的关注

和接受程度。在该标准中，信息安全已不只是人们传统意义上的安全，即添加防火墙或路由器等简单的设备就可保证安全，而是成为一种系统和全局的观念。信息安全是指使信息避免一系列威胁，保障商务的连续性，最大限度地减少业务的损失，从而最大限度地获取投资和商务的回报。

2. 主要内容

标准包括两部分：BS 7799-1:1999《信息安全管理实施细则》和 BS 7799-2:2002《信息安全管理体系规范》。标准第一部分为第二部分的具体实施提供了指南。但标准中的控制目标、控制方式的要求并非信息安全管理的全部，机构可以根据需要考虑另外的控制目标和控制方式。

BS 7799-1:1999《信息安全管理实施细则》是机构建立并实施信息安全管理体系的一个指导性的准则，主要为机构制定信息安全策略和进行有效的信息安全控制提供一个通用的方案。信息安全管理实施细则，是作为国际信息安全指导标准 ISO/IEC 17799 基础的指导性文件，主要是给负责开发的人员作为参考文档使用，从而在他们的机构内部实施和维护信息安全。这一部分包括十大管理要项、36 个执行目标、127 种控制方法，其详细内容如图 1.2 所示。

<table>
<tr><td colspan="4">一、安全策略(Security Policy)(1,2)</td></tr>
<tr><td colspan="4">二、安全机构(Security Organization)(3,10)</td></tr>
<tr><td colspan="4">三、资产分级与控制(Asset Classification and Control)(2,3)</td></tr>
<tr><td>四、人员安全(Personnel Security)(3,10)</td><td>五、物理与环境(Physical and Environmental Security)(3,13)</td><td>六、通信与操作管理(Communications and Operations Management)(7,24)</td><td rowspan="2">八、系统开发与维护(Systems Development and Maintenance)(5,18)</td></tr>
<tr><td colspan="3">七、访问控制(Access Control)(8,31)</td></tr>
<tr><td colspan="4">九、业务持续管理(Business Continuity Management)(1,5)</td></tr>
<tr><td colspan="4">十、符合性(Compliance)(3,11)</td></tr>
</table>

注：(m,n)——m：执行目标的数目；n：控制方法的数目。

图 1.2　信息安全管理实施细则包括的内容

BS 7799-2:2002《信息安全管理体系规范》则规定了建立、实施和文件化信

息安全管理体系(ISMS)的要求,规定了根据机构需要实施安全控制的要求,详细说明了建立、实施和维护信息安全管理系统(ISMS)的要求,提出了应如何建立信息安全管理体系的步骤。

新版标准较 BS 7799-2:1999 没有引入任何新的审核和认证要求,新标准完全兼容并依据 BS 7799-2:1999 建立、实施和保持的信息安全管理体系(ISMS)。新版标准没有增加任何控制目标和控制方式,所有的控制目标和控制方式都是来自 ISO/IEC 17799:2000。只是新版标准将原来 BS 7799-2:1999 的第四部分作为附件 A 放在了标准后面,而且采用了不同的编号方式,将 BS 7799-2:1999 和 ISO/IEC 17799:2000 结合起来了。表 1.1 给出新旧版本的对比。

表 1.1 新旧版本的对比

ISO/IEC 17799:2000	修订版 2nd 17799 (2.18)	修订版 FCD 17799 (6.17)
前言	前言	前言
引言 什么是信息安全 为什么需要信息安全 如何确立安全要求 评估安全风险 选择控制措施 信息安全起点 关键的成功因素 开发自己的指南	引言 什么是信息安全 为什么需要信息安全 如何确立安全要求 评估安全风险 选择控制措施 信息安全起点 关键的成功因素 开发自己的指南	引言 什么是信息安全 为什么需要信息安全 如何确立安全要求 评估安全风险 选择控制措施 信息安全起点 关键的成功因素 开发自己的指南
1 范围	1 范围	1 范围
2 术语和定义	2 术语和定义 2.1 定义	2 术语和定义 2.1 定义
	3 本标准的结构 3.1 条款 3.2 安全控制区域	3 本标准的结构 3.1 条款 3.2 主要的安全种类
		4 风险评估和处理 4.1 评估安全风险 4.2 处理安全风险
3 安全策略 3.1 信息安全策略 3.1.1 信息安全策略文档 3.1.2 评审和评价	4 安全策略 4.1 信息安全策略 4.1.1 信息安全策略文档 4.1.2 信息安全策略的评审	5 安全策略 5.1 信息安全策略 5.1.1 信息安全策略文档 5.1.2 信息安全策略的评审

续表

ISO/IEC 17799:2000	修订版 2nd 17799 (2.18)	修订版 FCD 17799 (6.17)
4 机构的安全 4.1 信息安全基础设施 4.1.1 管理信息安全协调小组 4.1.2 信息安全协作 4.1.3 信息安全职责的分配 4.1.4 信息处理设施的批准过程 4.1.5 专家的信息安全建议 4.1.6 机构间的合作 4.1.7 信息安全的独立评审 4.2 第三方访问的安全 4.2.1 标识来自第三方访问的风险 4.2.2 第三方合同中的安全要求 4.3 外包 4.3.1 外包合同中的安全要求	5 机构信息安全 5.1 内部机构 5.1.1 管理层的信息安全承诺 5.1.2 信息安全协作 5.1.3 信息安全职责的分配 5.1.4 信息处理设施的批准过程 5.1.5 与权威保持联系 5.1.6 与特殊的感兴趣的机构保持联系 5.1.7 信息安全的独立评审 5.2 外部团体 5.2.1 标识与外部团体相关的风险 5.2.2 在第二方协定中提出安全 5.2.3 在第三方协定中提出安全	6 机构信息安全 6.1 内部机构 6.1.1 管理层的信息安全承诺 6.1.2 信息安全协作 6.1.3 信息安全职责的分配 6.1.4 信息处理设施的批准过程 6.1.5 机密协定 6.1.6 与权威保持联系 6.1.7 与特殊的感兴趣的机构保持联系 6.1.8 信息安全的独立评审 6.2 外部团体 6.2.1 标识与外部团体相关的风险 6.2.2 在和顾客交涉时提出安全 6.2.3 在第三方协定中提出安全
5 资产分类和控制 5.1 资产的可核查性 5.1.1 资产清单 5.2 信息分类 5.2.1 分类指南 5.2.2 信息标记和处理	6 资产管理 6.1 资产的可核查性 6.1.1 资产清单 6.1.2 资产所有关系 6.2 信息分类 6.2.1 分类指南 6.2.2 信息标记与处理	7 资产管理 7.1 对资产的职责 7.1.1 资产清单 7.1.2 资产所有关系 7.1.3 资产的可接受用途 7.2 信息分类 7.2.1 分类指南 7.2.2 信息标记与处理
6 人员安全 6.1 岗位设定和人力资源的安全 6.1.1 岗位职责中包括的安全 6.1.2 人员筛选和策略 6.1.3 机密协定 6.1.4 雇用条款和条件 6.2 用户培训 6.2.1 信息安全教育和培训	7 人力资源 7.1 雇用之前 7.1.1 角色和职责 7.1.2 筛选 7.1.3 雇用的条款和条件 7.1.4 机密协定 7.2 雇用过程中 7.2.1 管理层职责 7.2.2 信息安全意识、教育和培训 7.2.3 惩罚过程	8 人力资源安全 8.1 雇用之前 8.1.1 角色和职责 8.1.2 筛选 8.1.3 雇用的条款和条件 8.2 雇佣过程中 8.2.1 管理层职责 8.2.2 信息安全意识、教育和培训 8.2.3 惩罚过程

续表

ISO/IEC 17799:2000	修订版 2nd 17799 (2.18)	修订版 FCD 17799 (6.17)
6.3 对安全事件和故障的响应 6.3.1 报告安全事件 6.3.2 报告安全弱点 6.3.3 报告软件故障 6.3.4 从事件中学习 6.3.5 惩罚过程	7.2.4 信息资产的可接受用途 7.3 雇佣终止 7.3.1 终止职责 7.3.2 返回资产 7.3.3 消除访问权	8.3 雇佣终止或变更 8.3.1 终止职责 8.3.2 返回资产 8.3.3 消除访问权
7 物理和环境的安全 7.1 安全区域 7.1.1 物理安全周边 7.1.2 物理实体控制措施 7.1.3 安全办公室、房间和设施 7.1.4 在安全区域中工作 7.1.5 隔离的传递和装载区域 7.2 设备安全 7.2.1 设备安装安置和保护 7.2.2 电源供应 7.2.3 电缆安全 7.2.4 设备维护 7.2.5 离开建筑物的设备的安全 7.2.6 安全丢弃或重用设备 7.3 一般控制措施 7.3.1 桌面清理和屏幕清理策略 7.3.2 财产的移动	8 物理和环境安全 8.1 安全区域 8.1.1 物理安全周边 8.1.2 物理实体控制措施 8.1.3 安全办公室、房间和设施 8.1.4 防范外部和环境威胁 8.1.5 在安全区域内工作 8.1.6 公共访问、传递和装载区域 8.2 设备安全 8.2.1 设备安装安置和保护 8.2.2 支持设施 8.2.3 电缆安全 8.2.4 设备维护 8.2.5 离开建筑物的设备的安全 8.2.6 安全丢弃或重用设备 8.2.7 财产的移动	9 物理和环境安全 9.1 安全区域 9.1.1 物理安全周边 9.1.2 物理实体控制措施 9.1.3 安全办公室、房间和设施 9.1.4 防范外部和环境威胁 9.1.5 在安全区域内工作 9.1.6 公共访问、传递和装载区域 9.2 设备安全 9.2.1 设备安置和保护 9.2.2 支持设施 9.2.3 电缆安全 9.2.4 设备维护 9.2.5 离开建筑物的设备的安全 9.2.6 安全丢弃或重用设备 9.2.7 财产的移动
8 通信和操作管理 8.1 操作规程和职责 8.1.1 文档化的操作规程 8.1.2 操作变更控制 8.1.3 事件管理规程 8.1.4 责任分割 8.1.5 开发和操作设施的分离 8.1.6 外部设施管理 8.2 系统规划和验收	9 通信和操作管理 9.1 操作规程和职责 9.1.1 文档记录操作规程 9.1.2 变更管理 9.1.3 职责分割 9.1.4 开发、测试和运行设施的分离 9.2 第三方服务传递管理 9.2.1 服务传递 9.2.2 监控和评审第三方服务	10 通信和操作管理 10.1 操作规程和职责 10.1.1 文档记录操作规程 10.1.2 变更管理 10.1.3 职责分割 10.1.4 开发、测试和运行设施的分离 10.2 第三方服务传递管理 10.2.1 服务传递 10.2.2 监控和评审第三方服务