第 1 章　信息系统安全测评概述

近年来，以网络为基础的信息系统建设，正深刻改变着人们的日常生活和工作方式。人们在充分享受便利的同时，其安全威胁也愈演愈烈。2013 年的“棱镜门”事件给全世界政府和人民都敲响了“防信息泄露”的警钟。而云计算、移动互联网及大数据等新技术对信息的获取、处理、存储等方式的改变，也使得企业敏感数据甚至国家机密更容易泄露，信息系统安全问题面临前所未有的严峻挑战。

1.1　信息安全发展历程

信息安全的发展经历了通信安全、计算机安全、网络安全、信息安全保障及网络空间安全的阶段。

早期的通信安全阶段，其主要威胁是对通信内容的窃听，因此主要通过通信技术和密码技术来解决数据的安全传输问题。在该阶段主要强调保证数据的机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。机密性是指信息不泄露给未授权的访问者、实体和进程，或被其利用。完整性是指信息在存储或传输过程中保持未经授权不能改变的特性，即对抗主动攻击，保持数据一致性，防止数据被非法用户修改和破坏。可用性是指信息可被授权者访问并按需求使用的特性，即保证合法用户对信息和资源的使用不会被不合理地拒绝。

20 世纪七八十年代，信息安全进入了计算机安全阶段。该阶段强调计算机软硬件及其所存储数据的安全，其主要威胁来自于对信息的非法访问等，强调基于访问控制策略的安全操作系统等安全措施。在这一阶段，出现了最早的安全评估标准，即 1983 年美国国防部发布的《可信计算机系统评估准则》（Trusted Computer System Evaluation Criteria，TCSEC）。

随着网络的普遍使用，信息安全进入了第三个阶段：网络安全。该阶段的主要威胁来自于网络入侵破坏等，主要采用防火墙、入侵检测、防病毒、漏洞扫描等工具来保证信息安全。1991 年，欧洲英、法、德、荷兰四个国家参考 TCSEC，制定了欧洲统一的安全评估标准《信息技术安全评估准则》（Information Technology Security Evaluation Criteria，ITSEC）。

1994 年，在美国联合安全委员会提交给美国国防部长和中央情报局长的一份《重新定义安全》的报告中，明确建议美国“应该使用风险管理作为安全决策的基础”。1996 年，美国国防部第 5-3600.1 号令第一次提出了信息安全保障的概念，由此进入了以风险控制、风险管理为核心的信息安全保障阶段。在这一阶段，信息安全从原有的强调技术措施，上升为技术和管理并重，认为安全不必要也不可能做到完美无缺、面面俱到，应在考虑安全成本的条件下，利用风险分析，使系统安全处于可控范围内。在测评标准方面，国际标准化组织（ISO）于 1996 年发布了最初的国际通用评估准则《信息技术安全性评估通用准则》（Common Criteria，CC）。

2008 年后，随着移动互联网的应用，虚拟网络世界已经和现实世界密不可分，于是出现了“网络空间”（Cyberspace）一词。同时，作为国家安全极为重要的一部分，工控安全也被

重视起来，信息安全发展到了网络空间安全阶段。

在信息安全发展的五个阶段中，安全测评的最早提出是以《可信计算机系统评估准则》（TCSEC）为标志的。但是，最初的 TCSEC 评估主要强调操作系统安全。在网络安全阶段，由 TCSEC 演变而来的 ITSEC、CC 等标准，主要是针对信息系统安全进行评估的。在第四阶段，即信息安全保障阶段，强调信息系统全生命周期的风险管理，其管理基础就是对信息系统从规划、设计、实施、运行维护、废弃等各阶段的风险评估。在该阶段除了上述的测评标准外，出现了信息安全管理标准，最早是英国的《信息安全管理实施细则》（BS 7799），后来发展为 ISO 27000 信息安全管理体系系列标准。

从信息安全的发展和信息安全测评标准的演变可见，信息系统测评作为风险评估的有效方法，是从信息安全第二个阶段开始出现并发展起来的，如表 1-1 所示。

表 1-1　信息安全发展历程

阶段	时间	主要特征	信息安全测评标准发展
通信保密	20 世纪 40～70 年代	解决数据的安全传输，强调信息的机密性、完整性、可用性	无
计算机安全	20 世纪 70～80 年代	强调基于访问控制策略的安全操作系统安全	《可信计算机系统评估准则》TCSEC 出现
网络安全	20 世纪 90 年代	主要威胁来自于网络入侵破坏等，主要采用防火墙、入侵检测、防病毒、漏洞扫描等工具来保证信息安全	《信息技术安全评估准则》ITSEC
信息安全保障	20 世纪 90 年代末	强调风险管理，技术和管理并重	《可信计算机系统评估准则》（CC） 《信息安全管理实施细则》BS 7799GB/T 17859 《计算机信息系统安全防护等级划分准则》
网络空间安全	21 世纪	涉及计算机、网络、云环境、工控系统等多层次、多维度安全问题，具有整体性；安全问题具有动态性、高复杂性，且具有共通性、国际化的趋势	我国 GB/T 18336—2001《信息技术安全性评估准则》及等级保护系列标准

1.2　相关概念

信息安全测评是信息安全管理的重要组成部分，更是保证系统“可信可靠”构建信息安全保障体系中的一个重要环节。信息安全管理是信息安全保障的要素之一。

作为信息系统安全管理、信息系统安全保障的重要组成，要理清信息系统安全测评的基本概念及其作用，必须将其放在信息安全管理、信息安全保障体系这样大的概念背景下来谈。因此，本节主要对信息系统安全、信息系统安全管理及信息系统安全保障等相关概念和理论进行简要介绍。

1.2.1　信息系统安全

1．信息系统

信息是指有价值的数据。在信息产生、传输、存储、使用、销毁的整个生命周期里，需要各种载体。例如，常见的计算机、网络、人均是信息的载体。这些信息载体又处于相应实际的物理环境中。通俗来讲，信息系统就是信息及其所处环境。

信息系统不仅仅描述的是计算机软硬件，网络和通信设备，更是人和管理制度等的综合。因此，从信息系统组成的角度，将信息系统（Information System）定义为由计算机硬件、网

络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统；从过程的角度，将信息系统定义为输入输出的复杂系统，其复杂性体现在系统元素之间的耦合性（元素之间的关联强度）复杂；此外，系统一般是有输入和输出的，输入的变化会引起输出的变化，通常输入和输出之间是非线性关系，从安全的角度看，信息系统的输入和输出是主要风险来源。

2．信息安全

在谈信息系统安全之前，首先明确下信息安全的定义。迄今为止，对于信息安全的概念尚无统一定义。但谈到信息的安全或信息系统的安全，普遍认同的是 1.1 节所述关于信息的三个安全属性，即机密性、完整性和可用性。随着技术的发展，从这三个基本安全属性中又扩展出可控性、抗抵赖性等其他性质。

3．信息系统安全

信息系统安全有狭义和广义两种定义。狭义的信息系统安全是指信息及其所在系统能够保证信息的机密性、完整性、可用性、可控性、不可否认性等基本性质。广义的信息系统安全是从技术和管理两个方面能够保证信息及其所处环境的安全。具体技术方面包括物理安全、主机安全、网络安全、应用安全、数据安全及其备份恢复等；管理方面包括人员、制度、组织等方面的安全管理要求。可见，广义的信息系统安全不是单纯的技术问题，而是管理、技术、法律等问题相结合的产物。

1.2.2　信息系统安全管理

在信息安全发展之初，大家普遍认为信息安全是一个技术问题，当时的信息安全主要依赖各种密码技术的保护和防御。但是，随着各种威胁的不断增加，各国逐渐认识到，信息安全不是一个纯粹靠技术能够解决的问题，更多的安全事件是由于管理不善、操作失误等原因造成的。要实现信息安全目标，必须依靠强有力的信息安全管理。信息安全是一个动态的过程，需要人员、技术、操作三者紧密结合。

1．信息安全管理概念

管理，是指为了达到特定目标，管理主体对被管对象进行的计划、组织、指挥、协调和控制等一系列活动。

信息安全管理（Information Security Management，ISM），是指为实现信息安全目标，管理主体对被管对象进行的计划、组织、指挥、协调和控制等一系列活动。

信息系统安全管理是指为了实现信息系统的安全目标，对信息系统的资产进行的计划、组织、指挥、协调和控制等一系列活动。

信息系统安全管理的被管对象是系统的资产，包括人员、软件、硬件、信息等，同时包括信息安全目标、信息系统安全组织架构和信息系统安全策略规则等。

2．信息系统安全管理基本方法

信息安全管理基本方法有风险管理和过程方法两种。这两种方法都来自于管理学中的质量管理，而信息系统安全管理也主要依赖于这两种方法。

信息系统安全管理的目的是预防、阻止和减少信息系统中安全事件的产生。而要达到这一目标就是要将系统的安全风险降低到可控范围内。信息系统安全水平的高低遵循“木桶原理”。即：一只木桶的盛水量，取决于桶壁上最短的木板。因此，要控制安全风险，首先要了解信息系统中的最短板，也就是要进行风险要素识别和风险分析，了解系统中的脆弱点在哪里。

在风险管理中，风险评估是信息安全管理的基础，风险处理是信息系统安全管理的核心，控制措施是管理风险的具体手段。风险评估主要对系统的信息资产进行鉴定和估价，然后对系统资产面对的各种威胁和脆弱性进行评估，同时对已存在的或规划的安全控制措施进行界定。而风险处理是对风险评估活动识别出的风险进行决策，采取适当的控制措施处理不能接受的风险，将风险控制在可承受的范围。风险处理的最佳集合就是信息系统安全管理的控制措施集合。控制措施可以分为技术性措施、管理性措施、物理性措施和法律性措施等。

此外，过程方法也是信息系统安全管理的重要方法之一。其目的是通过识别信息系统中的关键和重点安全过程，并加以实施和管理，获得持续改进的动态循环，使得系统的信息安全水平得到显著提高。

ISO/IEC 27000:2009 将“过程”定义为将输入转化为输出的一组彼此相关的资源和活动。ISO/IEC 27001:2005 将“过程方法”定义为使组织的业务有效运作，需要识别和管理业务相关的活动。

在过程方法中，戴明环是管理学中的一个通用模型，也叫 PDCA 循环或质量环。PDCA 循环包括 Plan（计划）、Do（执行）、Check（检查）和 Action（行动）四个顺序步骤。由于 PDCA 循环不仅可以在质量管理体系中运用，也适用于一切循序渐进的管理工作。因此，它也是信息安全管理中基于过程方法常见的一种持续改进模型。

PDCA 模型有三个重要特点。

① P-D-C-A 四个步骤是按顺序进行的，且四个过程不是运行一次就结束，而是周而复始的进行。一个循环结束，解决一些问题，未解决的问题进入下一个循环，这样阶梯式上升。

② PDCA 模型中的 P-D-C-A 四个阶段，每个阶段又都可以按照 PDCA 循环进行，也就是说可以大环套小环，一层一层地解决问题。

③ 每次执行完 PDCA 循环，都要进行总结，提出新目标，再进行第二次 PDCA 循环。

信息安全管理体系（Information Security Management System，ISMS）就是基于过程方法的 PDCA 循环体。如图 1-1 所示。

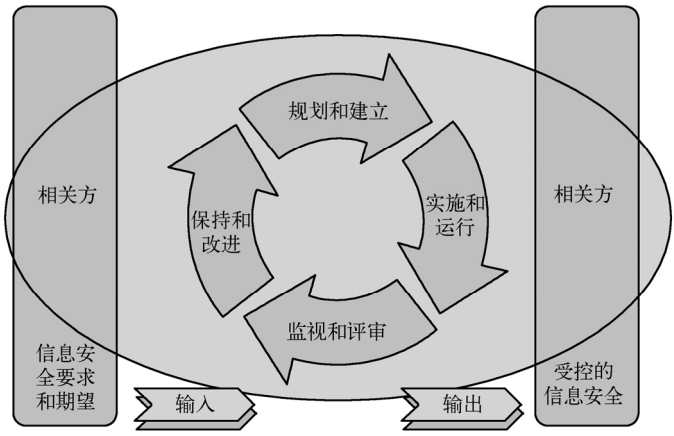

图 1-1　基于 PDCA 的信息安全管理体系

PDCA 循环是全面质量管理所应遵循的科学程序。全面质量管理活动的全部过程，就是质量计划的制订和组织实现的过程，这个过程就是按照 PDCA 循环，不停顿地周而复始地运转的。

3．信息系统安全管理实施

上述信息系统安全管理听起来概念性比较强，但目前我国实际的实施主要有两种方法。一个是图 1-1 所示的建设基于 PDCA 和风险管理的信息安全管理体系；第二个是实施信息安全等级保护。

（1）信息安全管理体系

信息安全管理体系（ISMS）是一种常见的全面、系统的信息安全管理方法。它是一种基于风险管理和过程方法的管理体系，是由 ISO 27001 定义的，其前身是英国的 BS 7799-2 标准。ISMS 包括周期性的风险评估、内部审核、有效性测量、管理评审四个必要活动，以确保 ISMS 进入良性循环，持续自我改进。

目前，ISO 27000 标准族日益完善，已经开发和计划开发的标准有 60 余项，包括 ISO 27000《信息安全管理体系概述和术语》、ISO 27001《信息安全管理体系要求》、ISO 27002《信息安全控制措施实用规则》、ISO 27003《信息安全管理体系实施指南》等。

（2）信息安全等级保护

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行全面、系统地管理的实施方法。根据《计算机信息系统安全保护等级划分规则》，计算机系统安全保护能力分为五个等级，分别是：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。二级以上需要到公安机关备案，三级以上每年需要进行信息安全测评。信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段。通过这五个阶段确保实现信息安全管理。

1.2.3 信息系统安全保障

1990 年，美国最早提出信息系统安全保障的概念，将信息安全的观念提升到“以预防、检测和反应能力的提高来确保信息系统的可用性、完整性、可鉴别性和不可否认性的全面保障阶段。”在此之前的信息安全重点是防御和保护，而信息安全保障强调的则是“防御保护、检测和响应”的综合。信息安全保障特别强调“检测和响应”，而检测响应的核心是风险管理，其基础是风险评估。

正如前文所提到的，在信息安全保障这一阶段，普遍的认同是，安全不必是完美无缺、面面俱到的，安全问题是一个成本问题，最佳的信息安全保障实际就是最佳的风险管理方式，信息安全测评是风险管理的有效手段。

我国信息安全保障工作起步较晚，先后经历了启动、逐步开展和深化落实阶段。

2001～2002 年，是我国信息安全保障工作的启动阶段。其标志是 2001 年国家信息化领导小组重组，网络与信息安全协调小组的成立。这一阶段的特点是，各种信息安全事件频繁发生，我国认识到信息安全不是一个局部的、技术性问题，信息安全是跨领域、跨部门、跨行业的问题，是一个关于国计民生、社会稳定和国家安全的问题。

2003～2005 年，是我国信息安全保障工作的逐步开展和积极推进阶段。其标志是 2003 年 7 月发布的《关于加强信息安全保障工作的意见》（中办发 27 号文件）。该文件明确了“积极防御、综合防范”的国家信息安全保障工作方针，提出了加强信息安全保障工作的总体要求和主要原则。在此阶段，各省（区、市）和有关部门陆续建立了网络与信息安全协调小组。信息安全等级保护、信息安全风险评估、网络信任体系建设、信息安全产品认证认可、信息安全标准制定、信息安全监控和信息安全应急处理等工作均取得了积极推进和明显进步。

2006 年至今，是我国信息系统安全保障深化落实阶段。围绕中办发 27 号文件，信息安全法律法规、标准化和人才培养工作取得新成果；信息安全等级保护和风险评估取得新进展。

1．信息安全保障技术框架

目前，较成熟的信息安全保障框架主要是由美国国家安全局（NSA）制定的信息安全保障技术框架（Information Assurance Technical Framework，IATF），该框架主要为保护美国政府和工业界的信息与信息技术设施提供技术指南。

该框架的主要思想是深度防御，该框架强调人、技术、操作这三个核心要素，提出了信息保障依赖于人、技术和操作来共同实现组织职能和业务运作的思想，从多种不同的角度对信息系统进行防护。同时，IATF 关注四个信息安全保障领域，即本地计算环境、区域边界、网络和基础设施及支撑性基础设施。此基础上，对信息系统就可以做到多层防护，实现组织的任务和业务运作，如图 1-2 所示。

在 IATF 模型中，人是信息保障体系的第一位要素，需要对其进行意识培训、组织管理、技术管理、操作管理等；其次，技术是实现信息保障的重要手段，包括由防护、检测、响应、恢复等部分组成的一个动态技术体系；最后，操作也叫运行，构成安全保障的主动防御体系，是将各方面技术紧密结合在一起的主动的过程，主要包括风险评估、安全监控、安全审计、跟踪告警、入侵检测、响应恢复等。如图 1-3 所示。

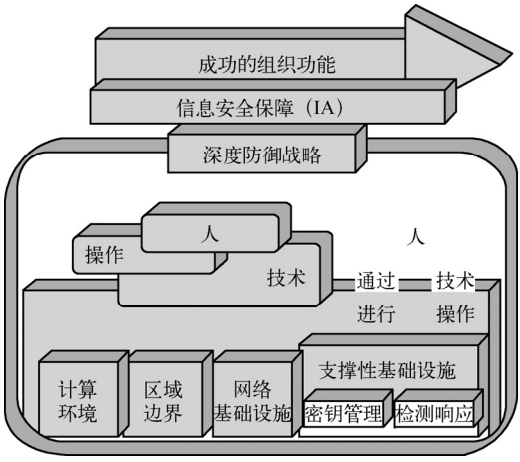

图 1-2　深度防御的信息安全保障技术框架

人员	技术	操作
培训	深度防御技术框架域	分析
意识	安全标准	监视
物理安全	获得IA/TA	入侵检测
人员安全	风险分析	警告
系统安全管理	证书与认证	恢复

图 1-3　IATF 三要素

IATF 定义的四个安全区域，分别是：

① 对计算机环境的保护：使用信息保障技术确保数据在进入、离开或驻留客户机和服

务器时具有保密性、完整性和可用性。

② 对区域边界的保护：这里的区域是指由单一授权通过专用或物理安全措施所控制的环境，包括物理环境和逻辑环境。而区域边界则是指区域的网络设备与其他网络设备的接入点。其主要保护方法是通过部署病毒、恶意代码检测、防火墙、入侵检测等设备对进出某区域（物理区域或逻辑区域）的数据流进行有效的控制与监视。

③ 对网络基础设施的保护：其目的是防止数据非法泄露，防止受到拒绝服务的攻击，以及防止受到保护的信息在发送过程中的时延、误传或未发送。

④ 支撑性基础设施建设：是为安全保障服务提供一套相互关联的活动与基础设施，主要包括密钥管理和检测响应两部分。

深度防御战略思想采用层次化保护策略，通过在主要位置实现适当的保护级别，同时为了降低保障成本，允许在不降低系统整体安全性的前提下，在适当的时候用低安全级的保障解决方案。

2．信息系统安全保障模型

基于我国的实际信息安全保障需求，GB/T 20274.1—2006《信息安全技术信息系统安全保障评估框架第一部分：简介和一般模型》将信息系统安全保障定义为：在信息系统的整个生命周期中，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。根据该定义，信息系统安全保障模型如图 1-4 所示。

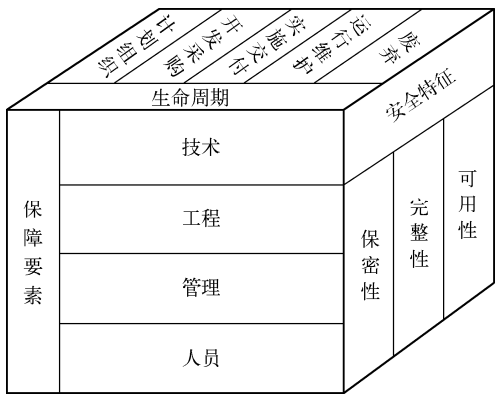

图 1-4　信息系统安全保障模型

信息系统安全保障模型是要保障信息系统在技术组织、开发采购、实施交付、运行维护到废弃整个生命周期中信息的保密性、完整性和可用性特征，从而实现和贯彻组织机构策略，并将风险降低到可接受程度。其保障要素包括技术、工程、管理和人员四部分。技术包括密码、访问控制、网络安全、漏洞及恶意代码防护等常见的安全技术；工程包括信息系统安全工程、安全工程能力成熟度模型等信息安全工程实现方法和模型；管理包括安全管理体系、风险管理、应急响应与灾难恢复等；人员包括对所有员工、信息系统岗位、安全专业人员的日常培训、管理等。

该模型提出保密性、完整性、可用性三个安全特征是信息系统安全要达到的基本要求；信息系统安全保障的生命周期是信息系统安全保障持续发展的动态特征；信息系统所处的运行环境、信息系统的生命周期和信息系统安全保障等概念的技术、工程、管理和人员等四个要素是综合保障，与 IATF 框架中的人、技术、操作有异曲同工之处。此外，该模型将风险和策略作为信息系统安全保障的基础策略，在生命周期、安全特征和保障要素中始终贯穿风险管理和策略部署。

1.3　信息系统安全测评作用

迄今为止，尚无对信息系统安全测评的统一定义。通俗地讲，信息系统安全测评，是一种合规性检测和评估活动，主要针对信息系统中可能存在的技术、管理等安全隐患，逐项对

照标准进行一一检测，并根据检测结果，分析评估出该系统的安全状况，根据其薄弱环节和潜在威胁等提出加固及整改建议，其测评对象是信息系统，其测评目的是为了防范并降低系统安全风险，测评的依据是测评标准。

建立合理规范的信息系统生命周期，是保证信息系统安全运行的前提。而信息安全测评与其他信息安全服务（如安全咨询、体系规划、安全管理、应急响应等）逐渐融为一体，构成了信息系统生命周期的一体化综合保障体系。

依据相关标准，信息安全测评从安全技术、功能和机制等角度对信息技术产品、信息系统、服务提供商及人员进行测试和评估。其中信息系统安全测评又包括信息系统风险评估、信息系统等级保护测评，以及信息系统安全保障测评。本书主要以等级保护测评为主线介绍信息系统安全测评方法，但在本节讨论信息安全测评的意义和作用时，不强调信息系统安全测评，统一称为信息安全测评。

1．信息安全测评是信息安全保障工作方法的重要组成

从上节介绍内容可知，信息安全保障体系是信息安全的顶层设计框架，其中信息安全管理、信息安全工程、信息安全技术和信息安全人员是其四个基本保障要素。

要将上述体系框架及要素落到工作实处，需要科学的方法。信息安全保障工作实际划分为确定安全需求、设计并实施信息安全方案、信息安全测评、监测和维护四个阶段。信息安全测评是确保信息安全保障体系落实的重要手段。

- 确定安全需求：是进行信息安全方案设计和安全措施实施的依据，通常从以下三个方面来确定需求。① 符合性要求，即其需求要遵循国家相关法律法规、标准、行业规定，例如，要符合等级保护标准要求；② 业务要求，即信息安全需求要具体考虑所承载业务正常运行的需求；③ 风险评估，即信息安全方案设计要考虑系统所面临的风险，重点消除影响最大或可能性最大的风险隐患。
- 设计并实施信息安全方案：根据安全需求，围绕动态的风险管控，根据成本预算、技术的可实现性、组织的具体文化等具体内容制订信息安全保障方案。
- 信息安全测评：在信息系统的生命周期内，根据组织机构的要求在信息系统的安全技术、安全管理和安全工程领域对信息系统的安全技术控制措施和技术架构能力、安全管理控制和管理能力及安全工程实施控制措施和工程实施能力进行评估综合，最终得出信息系统在其运行环境中安全保障措施是否满足其安全保障要求，以及信息系统安全保障能力的评估。
- 监控和维护：持续进行风险评估，持续监控信息系统安全风险变化，具体包括安全漏洞和隐患的检测、消除，应急响应和灾难恢复等工作。

2．信息安全测评是保障信息安全的首道防线

信息安全测评是依据一定的标准，通过对信息产品或信息系统的安全状态进行测试和评估，确定该产品和系统所能达到的安全级别和可信程度。因此，信息安全测评是维护信息系统或产品安全的基础性工作，可以说如果这项基础性工作不开展或开展得不好，就仿佛信息系统或产品的高楼大厦的地基不稳一般。未开展测评产品或系统，对于用户来说其安全性无从谈起。

信息安全测评可以降低信息系统或产品的安全风险，提高对信息系统或产品的安全管理

控制能力。信息系统安全测评为有关组织、部门、决策者有针对性地管理决策提供有力的手段和支撑。

3．信息安全测评对信息安全建设起到规范性作用

信息安全测评是一个合规性的工作，也就是以标准为衡量尺度，全面考察系统或产品的安全状况，并给出合规性客观评价。在进行信息安全测评时，所依据的标准主要以国际标准、国家标准、地区标准和行业标准为主。这些标准和依据对于指导业界的技术研究、产品开发，规范信息化应用、规范安全管理等工作都起着技术规范和指南的作用。通过安全测评，可以理清系统的脆弱点，认清技术的先进度，及时整改，为信息系统安全运行提供可靠的技术性保障。

4．信息系统安全测评是实现风险管理的重要手段

如前文所说，信息安全保障要求技术和管理并重，其基础是风险管理，基本手段是风险评估。在信息系统生命周期的每个阶段，有不同的信息安全目标，为了达到其安全目标，每一阶段都需要相应的风险管理作为支持。风险管理的前提是有效的风险评估。

风险评估，安全检查或检查评估，安全测评这三个概念经常容易混淆。风险管理是贯穿于信息系统“规划、设计、实施、运维、废弃”整个生命周期中的每一个阶段的。风险评估作为风险管理的首要步骤，也贯穿于信息系统整个生命周期的各阶段中。然而，由于实际上不同行业的信息系统，其业务、用户、制度、管理等千差万别，要在信息系统生命周期的各阶段开展各异的风险评估是十分困难的。

首先需要明确信息系统风险评估与信息系统安全测评之间的区别与联系。通俗来讲，基于等级保护的安全测评、安全检查等都是在既定安全基线（即国家标准）的基础上开展的符合性测评。其中，等级保护测评是符合国家安全要求的测评，而安全检查是符合行业主管安全要求的符合性测评。风险评估是在国家、行业安全要求的基础上，以被评估系统特定安全要求为目标而开展的风险识别、风险分析、风险评价活动。

GB/T 20984—2007《信息安全风险评估规范》将信息安全风险定义为人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。信息系统的风险评估，简单地说就是发现风险，进行定性或定量分析，为风险管理提供依据。而信息系统安全测评则是根据系统技术方案、安全策略等检验系统安全状况是否符合所定义的评估标准。

风险评估与安全测评是信息系统安全工程生命周期中不同阶段、不同目的的安全评价活动。风险评估是指针对确立的风险管理对象所面临的风险进行识别、分析和评价，即根据资产的实际环境对资产的脆弱性、威胁进行识别，对脆弱性被威胁利用的可能性和所产生的影响进行评估，从而确认该资产的安全风险及其大小。风险评估贯穿于整个信息系统安全工程生命周期，是风险管理的重要组成部分。两者区别如表 1-2 所示。

表 1-2　风险评估和安全测评的不同

	生命周期中阶段不同	目的不同
风险评估	贯穿于整个信息系统安全工程生命周期	为了发现系统中存在的风险，从而给出信息系统安全建设的相关建议
安全测评	从信息系统建设完毕到废弃之间	检验已建设完成的系统中的残余风险是否符合相关标准要求，为系统准入提供依据

信息系统安全测评是指从信息系统建设完毕到废弃之间这段时间内，由国家授权的信息安全测评部门所进行的，对信息系统已采取的安全控制措施（如管理措施、运行措施、技术措施等）的有效性进行验证，从而给出系统现有的安全状况是否符合相关规范要求的准确判断的活动。安全测评结果的有效期依据相关部门的要求确定，测评结果失效后必须重新进行测评。在实际工作中，往往用信息系统安全测评来督促检测系统是否达到标准要求的必要水平。测评往往由第三方测评认证机构开展，通过测评，则说明该信息系统达到了一定的安全级别和可信程度，有一定的抵抗风险能力。测评后给予认证，就代表第三方机构对达到评价准则和标准要求的信息系统进行了权威认可。

风险评估和安全测评都是安全测度方法，两者关系密切，风险评估报告是安全测评的依据之一，安全测评将进一步检验风险评估结果是否有效。虽然实施过程中，某些技术手段（如技术渗透性测试、安全扫描等）可以互用，但风险评估与安全测评是不同的安全评价活动。简单地说，风险评估目的是为了发现系统中存在的风险，从而给出信息系统安全建设的相关建议；安全测评目的是检验已完成安全建设的系统中的残余风险是否符合相关标准的要求，为系统准入提供依据。风险评估与安全测评互为补充。

因此，信息系统安全测评以合规性测评认证的方式保障了信息系统的安全风险管理。

1.4 信息安全标准组织

在具体介绍各种信息系统安全测评标准之前，首先介绍国内外的主要信息安全标准组织，信息系统安全测评所依照的标准也是由这些组织所制定的。

1．国际标准化组织（International Organization for Standardization，ISO）

该组织成立于 1947 年，是最大的非政府性标准化专门机构。ISO 是一个国际标准化组织，其成员由来自世界上 100 多个国家的国家标准化团体组成，中国是其常任理事国。其宗旨是“在世界上促进标准化及其相关活动的发展，以便于商品和服务的国际交换，在智力、科学、技术和经济领域开展合作”。ISO 通过下设的技术委员会 TC（Technology Committee），分技术委员会 SC（Sub Committee），工作组 WG（Working Group）和特别工作组来开展活动。与信息安全测评相关的重要标准有 ISO/IEC 15408《信息技术信息安全-IT 安全的评估准则》等。

2．ISO/IEC JTC1 SC27

国际电工委员会（International Electrotechnical Commission，IEC）成立于 1906 年，是成立最早的国际标准化机构。在信息安全标准化方面，主要与 ISO 成立了联合技术委员会 JTC1（Joint Technical Committee1），并下设分委会。 ISO/IEC JTC1 SC27 是联合技术委员会下专门从事信息安全标准化的分技术委员会，其前身是数据加密分技术委员会（SC20），主要从事信息技术安全的一般方法和技术的标准化工作，是信息安全领域中最具代表性的国际标准化组织。SC27 下设信息安全管理体系工作组 WG1、密码与安全机制工作组 WG2、安全评估准则工作组 WG3、安全控制与服务工作组 WG4 和身份管理与隐私技术工作组 WG5。其中 ISO/IEC 15408《信息技术信息安全-IT 安全的评估准则》就是该联合技术委员会制定的。

3．美国国家标准协会（American National Standards Institute，ANSI）

该组织成立于 1918 年，是非营利性质的民间标准化团体。ANSI 实际上已成为美国国家标准化中心，美国各界标准化活动都围绕它进行。ANSI 的技术委员会中美国国家信息科技标准委员会负责信息技术，承担着 JTC1 秘书处的工作。其中，分技术委员会 T4 专门负责 IT 安全技术标准化工作，对口 JTC1 的 SC27。

4．美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）

NIST 负责联邦政府非密敏感信息，NIST 制定的标准和规范称为 FIPS（Federation Information Processing Standards）。从 20 世纪 70 年代 NIST 公布数据加密标准 DES 开始，NIST 制定了一系列信息安全方面的标准，如 NIST SP800 系列等。

5．电气和电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）

IEEE 是一个国际性的电子技术与信息科学工程师的协会，是目前全球最大的非营利性专业技术学会。它主要提出了关于局域网、广域网安全方面的标准和公钥密码标准。1990 年，IEEE 成立 802.11 无线局域网工作组，在无线通信及安全方面做了大量工作。

6．中国国家标准化管理委员会

中国国家标准化管理委员会是我国最高级别的国家标准机构。其下设有全国信息安全标准化技术委员会，简称信安标委（TC260），由国家标准化委员会直接领导。TC260 下设多个工作组，主要包括：信息安全标准体系与协调工作组（WGl），负责研究信息安全标准体系，跟踪国际标准发展动态，研究信息安全标准需求，提出新工作项目，以及建议建立新工作组等；涉密信息系统安全保密工作组（WG2），负责制定和修订涉密信息系统安全保密标准；密码技术工作组（WG3），负责制定商用密码技术标准体系，负责研究制定商用密码算法、商用密码模块、商用密钥管理等相关标准；鉴别与授权工作组（WG4）负责研究制定鉴别与授权标准体系，调研国内相关标准要求，研究制定鉴别与授权标准；信息安全评估工作组（WG5）负责调研测评标准现状与发展趋势，研究我国统一测评标准体系的思路和框架，提出测评标准体系，研究制定急需的测评标准；通信安全标准工作组（WG6）负责调研通信安全标准现状与发展趋势，研究提出通信安全标准体系，研究制定急需的通信安全标准。信息安全管理工作组（WG7），负责研究信息安全管理动态，调研国内管理标准需求，提出信息安全管理标准体系，制定信息安全管理相关标准。

1.5 国外重要信息安全测评标准

1.5.1 TCSEC

国际上公认的最早的信息安全测评标准是 1983 年由美国国家计算机安全中心（NCSC）公布的“可信计算机系统评估准则”（Trusted Computer System Evaluation Criteria，TCSEC）。该标准于 1985 年被作为美国国防部标准（DoD5200.28-STD）发布实施。

TCSEC 对开发、测试和使用可信计算机系统有三方面的作用：一是作为测试标准，提供计算机系统可靠性测评准则；二是可作为可信计算机系统开发的安全要求；三是作为系统集

成的工程规范。

TCSEC 将产品的安全水平列为不同的评估等级，规定了不同等级的具体安全要求。这些安全要求分为安全策略（Security Policy）、问责（Accountablity）、安全保证（Assurance）、文档（Document）四类。TCSEC 将计算机系统的安全划分为四个等级（由下到上分别是 D、C、B、A）、七个级别（D1，C1，C2，B1，B2，B3，A），评估等级从低到高安全要求逐步增多。

D1 级的安全等级最低，只为文件和用户提供安全保护，最普通的形式是本地操作系统，或者是一个完全没有保护的网络。C 级能够提供审记的保护，并为用户的行动和责任提供审计能力。C 级安全等级可划分为 C1 和 C2 两类，C1 系统的可信任运算基础体制（Trusted Computing Base，TCB）通过将用户和数据分开来达到安全的目的。C2 系统和 C1 系统相比，加强了可调的审计控制。B 级安全等级可分为 B1、B2 和 B3 三类，B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B1 系统满足以下两个要求：系统对网络控制下的每个对象都进行灵敏度标记；系统使用灵敏度标记作为所有强迫访问控制的基础。B2 系统必须满足 B1 系统的所有要求，另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B3 系统必须满足 B2 系统的所有安全要求，B3 系统具有很强的监视委托管理访问能力和抗干扰能力，B3 必须产生一个可读的安全列表。A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别，A1 系统的设计者必须按照一个正式的设计规范来分析系统。

TCSEC 主要针对计算机安全测评，特别是操作系统安全，但实际的信息系统面临的安全问题要复杂得多，为了补充其不足，NCSC 又陆续出版了 20 多本详细的解释性指南，由于这些指南的封面颜色不同，也被称为“彩虹系列”标准。

1.5.2 ITSEC

美国建立 TCSEC 标准后，欧洲各国也纷纷开始制定自己国家的信息技术安全评估标准。1991 年，欧洲共同体委员会以英、法、德、荷兰四个国家为代表，共同制定了欧洲统一的安全评估标准（Information Technology Security Evaluation Criteria，ITSEC），适用于军队、政府商业等部门。ITSEC 较美国制定的 TCSEC 准则，在功能的灵活性和有关的评估技术方面均有很大的进步，该标准将安全概念分为功能与评估两部分。功能准则从 F1～F10 共分 10 级，F1～F5 级对应于 TCSEC 的 D 到 A，F6～F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性及机密性和完整性的网络安全。

与 TCSEC 不同，ITSEC 并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。另外，TCSEC 把保密作为安全的重点，而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。ITSEC 定义了从 E0（不满足品质）～E6（形式化验证）的 7 个安全等级，对于每个系统安全功能可分别定义。

这 7 个安全等级如下。

E0 级：该级别表示不充分的安全保证。

E1 级：该级别必须有一个安全目标和一个对产品或系统的体系结构设计的非形式化的描述，还需要有功能测试，以表明是否达到安全目标。

E2 级：除了 E1 级的要求外，还必须对详细的设计有非形式化描述。另外，功能测试的证据必须被评估，必须有配置控制系统和认可的分配过程。

E3 级：除了 E2 级的要求外，不仅要评估与安全机制相对应的源代码和硬件设计图，还要评估测试这些机制的证据。

E4 级：除了 E3 级的要求外，必须有支持安全目标的安全策略的基本形式模型。用半形式说明安全加强功能、体系结构和详细的设计。

E5 级：除了 E4 级的要求外，在详细的设计和源代码或硬件设计图之间需要有紧密的对应关系。

E6 级：除了 E5 级的要求外，必须正式说明安全加强功能和体系结构设计，使其与安全策略的基本形式模型一致。

除了 ITSEC 外，加拿大也参考美国的 TCSEC 及欧洲的 ITSEC，在 1993 年制定了加拿大可信计算机产品测评标准 CTCPEC。

1.5.3 CC 标准

1993 年 6 月，美国政府同加拿大及欧共体共同起草单一的通用准则（CC 标准）并将其推到国际标准。制定 CC 标准的目的是建立一个各国都能接受的通用的信息安全产品和系统的安全性评估准则。在美国的 TCSEC、欧洲的 ITSEC、加拿大的 CTCPEC、美国的 FC 等信息安全准则的基础上，由六个国家七方（美国国家安全局和国家技术标准研究所、加、英、法、德、荷）共同提出了“信息技术安全评价通用准则”（The Common Criteria for Information Technology security Evaluation，CC），简称 CC 标准。它综合了已有的信息安全的准则和标准，形成了一个更全面的框架，主要用来评估信息系统、信息产品的安全性。

CC 标准主要分为简介和一般模型、安全功能要求、安全保证要求三部分。CC 标准是国际通行的信息技术产品安全性评价规范，它基于保护轮廓和安全目标提出安全需求，具有灵活性和合理性，基于功能要求和保证要求进行安全评估，能够实现分级评估目标，不仅考虑了保密性评估要求，还考虑了完整性和可用性多方面安全要求。CC 标准定义了“保护轮廓”和“安全目标”，将评估过程分“功能”和“保证”两部分。CC 基于风险管理理论，对安全模型、安全概念和安全功能进行了全面系统描绘，强化了保证评估。CC 便于理解，是目前最全面的评价准则，它是一种通用的评估方法，其评估结果国际互认。1999 年，CC 标准正式成为国际标准 ISO/IEC 15408。

CC 中常用的三个术语分别是评估对象（Target of Evaluation，TOE），保护轮廓（Protection Profile，PP）和安全目标（Security Target，ST）。

TOE：通俗来讲，评估对象 TOE 就是被评估的产品或系统，包括信息技术产品、系统或子系统，比如防火墙、计算机网络、密码模块等，以及相关管理员指南、用户指南、设计方案等文档。

PP：保护轮廓 PP 类似用户的需求，是为了满足安全目标而提出的一整套相对应的功能和保证的需求，在标准体系中 PP 相当于产品标准，如《包过滤防火墙安全技术要求》。PP 与某个具体的 TOE 无关，它定义的是用户对这类 TOE 的安全需求。PP 主要包括需保护的对象、确定安全环境、TOE 的安全目的、IT 安全要求、基本原理等。

ST：ST 相当于产品和系统的实现方案。针对具体 TOE 而言，是某一款产品对某一 PP 要求的具体实现。包括该 TOE 的安全要求和用于满足安全要求的特定安全功能和保证措施。ST 包括的技术要求和保证措施可以直接引用该 TOE 所属产品或系统类的 PP。

CC 评估保证级（Evaluation Assurance Level，EAL）定义了划分 TOE 保证等级的预定义的评估尺度。一个保证等级（EAL）是评估保证要求的一个基线集合——保证包，保证包又是由一系列保证组件构成。每一评估保证级定义一套一致的保证要求，合起来构成一个预定义 CC 保证级尺度。表 1-3 给出了 CC 与 TCSEC 等级的对应关系。CC 中定义了以下 7 个评估保证级：

① 评估保证级 1（EAL1）功能测试；
② 评估保证级 2（EAL2）结构测试；
③ 评估保证级 3（EAL3）系统地测试和检查；
④ 评估保证级 4（EAL4）系统地设计、测试和复查；
⑤ 评估保证级 5（EAL5）半形式化设计和测试；
⑥ 评估保证级 6（EAL6）半形式化验证的设计和测试；
⑦ 评估保证级 7（EAL7）形式化验证的设计和测试。

表 1-3 CC 与 TCSEC 等级的对比

CC	TCSEC
-	D
EAL1	-
EAL2	C1
EAL 3	C2
EAL4	B1
EAL5	B2
EAL6	B3
EAL7	A1

1.6 我国信息安全测评标准

我国的信息安全标准体系大致分为基础标准、技术与机制标准、管理标准、测评标准、密码技术标准和保密技术标准六大类。

基础标准为其他标准制定提供支撑的公用标准，包括安全术语、体系结构、模型和框架标准四个子类；技术与机制标准包括标识与鉴别、授权与访问控制、实体管理和物理安全标准四个子类；管理标准包括管理基础标准、管理要求标准、管理支撑技术标准和工程与服务管理标准四个子类；密码技术标准包括基础标准、技术标准和管理标准三个子类；保密技术标准包括技术标准和管理标准两个子类；测评标准包括测评基础标准、产品测评标准和系统测评标准三个子类。这六大类标准之间相互有关联，比如测评标准也涉及基础标准、管理标准等其他标准的内容。

具体来说，我国的信息安全测评标准是参考国外标准，在其基础上修改演变而来的。国内测评标准与国外测评标准之间的关系参看图 1-5。

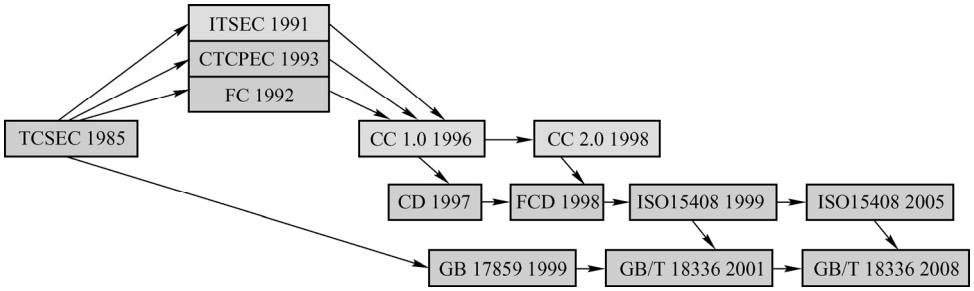

图 1-5 国内外信息安全测评标准发展演化关系图

我国国家标准分为以 GB 开头的强制性国家标准，以 GB/T 开头的推荐性国家标准和以 GB/Z 开头的标准化指导技术文件。强制性国家标准具有法律属性，一经颁布，必须贯彻执行，违反则要受到经济制裁或承担相应的法律责任。推荐性国家标准属于自愿采用的标准，但一经法律或法规引用，或各方商定同意纳入商品、经济合同之中，就成为共同遵守的技术依据，具有法律上的约束性，必须严格贯彻执行。国家标准化指导技术文件是仍处于技术发

展中，或由于其他原因，将来可能就国家标准取得一致意见的指导性技术文件。

1.6.1 GB/T 18336《信息技术安全性评估准则》

2001 年我国颁布了 GB/T 18336《信息技术安全性评估准则》。2008 年，对其进行了修订，修订后的 GB/T 18336 包括三部分：第一部分，简介和一般模型；第二部分，安全功能要求；第三部分，安全保证要求。

GB/T 18336.1—2008《信息技术安全性评估准则》等同于美国 CC 标准，也等同于 ISO 15408《信息技术-安全技术 IT 评估准则》。GB/T 18336 是测评标准类中的测评基础标准子类中的重要标准，该标准定义了与 CC 相同的三个概念：评估对象 TOE，保护轮廓 PP 和安全目标 ST。

1.6.2 GB/T 20274《信息系统安全保障评估框架》

GB/T 20274《信息系统安全保障评估框架》是测评标准类中的测评基础标准子类中的重要标准。该标准是 GB/T 18336 在信息系统评估领域的扩展和补充，以 GB/T 18336 为基础，吸收其思想和结构，并同其他国内外信息系统评估领域的标准和规范相结合，形成了描述和评估信息系统安全评估保障内容和能力的通用框架。

该标准包括四部分：第一部分，简介和一般模型；第二部分，技术保障；第三部分，管理保障；第四部分，工程保障。

1.6.3 信息系统安全等级保护测评标准

为了规范我国信息安全等级保护工作，全国信息安全标准化技术委员会、公安部信息系统安全标准化技术委员会，以及其他单位组织制定了信息安全等级保护工作系列标准，形成了信息安全等级保护标准体系，为开展等级保护工作提供了标准保障。信息安全等级保护标准体系是围绕信息系统预备、定级、建设、测评、整改的生命周期来设计的。

1．等级划分

1999 年，我国制定并颁布了带有法律效力的强制性国家标准 GB 17859—1999《计算机信息系统安全保护等级划分准则》，该准则主要参考了美国的“彩虹系列”标准 TCSEC，主要定义了安全保护等级的五个级别。这五级分别是：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。该标准主要适用于对计算机信息系统安全保护技术能力等级的划分，随着安全保护等级的增高，对计算机信息系统安全保护能力的要求逐渐增强。

2．定级

在信息系统安全等级保护定级阶段，其标准主要有 GB/T22240—2008《信息系统安全等级保护定级指南》，该标准规定了定级的依据、对象、流程、方法及等级变更等内容。

3．建设

在信息系统安全等级保护安全建设/整改阶段，主要有 GB/T 22239—2008《信息系统安全等级保护基本要求》，GB/T 25070—2010《信息系统等级保护安全设计技术要求》，GB/T

20271—2008《信息系统通用安全技术要求》，GB/T 20269—2006《信息系统安全管理要求》，GB/T 20282—2006《信息系统安全工程管理要求》等标准。其中，GB/T 22239—2008 规定了不同安全保护等级信息系统的基本保护要求，包括基本技术要求和基本管理要求两部分，适用于指导分等级的信息系统的安全建设和监督管理，所谓的基本要求是指信息系统要达到的最低要求；GB/T 25070—2010《信息系统等级保护安全设计技术要求》提出了安全环境、安全区域边界、安全通信网络、安全管理中心等各方面的安全设计技术要求；GB/T 20271—2008《信息系统通用安全技术要求》从信息系统安全保护等级划分的角度说明实现 GB/T 20269—2006 中每一个安全保护等级的安全功能要求应采取的安全技术措施，以及各安全保护等级的安全功能在具体实现上的差异；GB/T 20269—2006《信息系统安全管理要求》阐述了安全管理的具体要求及其强度；GB/T 20282—2006《信息系统安全工程管理要求》是对信息安全工程中所涉及的需求方、实施方与第三方工程实施指导性文件。

4．测评

这里重点要提到的是 2012 年颁布的与信息系统安全测评相关的 GB/T 28448《信息系统安全等级保护测评要求》和 GB/T 28449《信息系统安全等级保护测评过程指南》。

GB/T 28448《信息系统安全等级保护测评要求》主要规定了对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统安全等级保护状况进行安全测试评估的具体要求，该标准略去对第五级信息系统进行单元测评的具体内容要求。该标准针对信息系统中的单项安全措施和多个安全措施的综合防范，对应地提出单元测评和整体测评的技术要求，用以指导测评人员从信息安全等级保护的角度对信息系统进行测试评估。单元测评对安全技术和安全管理上各个层面的安全控制提出不同安全等级的测试评估要求，其测评内容主要针对《信息安全技术信息系统安全等级保护基本要求》规定的各单项安全控制措施在信息系统中的落实情况。整体测评根据安全控制间、层面间和区域间相互关联关系，以及信息系统整体结构对信息系统整体安全保护能力的影响提出测试评估要求。但该标准主要给出了等级测评结论中应包括的主要内容，未规定给出测评结论的具体方法和量化指标，具体测评操作时需要测评者根据不同的被测内容，凭借经验选取适宜的测评指标，选择合适的测评方法进行。该标准适用于信息安全测评服务机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评估，信息安全监管职能部门依法进行的信息安全等级保护监督检查也可以参考使用。

GB/T 28449《信息系统安全等级保护测评过程指南》规定了对信息系统实施安全等级保护测评工作的具体测评流程及流程中每个步骤的具体任务，其附录内容还给出了确定测评对象的要求和方法及测评方案及测评报告编制案例等。该标准既适用于测评机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全自测试评价，也适用于信息系统的运营使用单位在信息系统定级工作完成之后，对信息系统的安全保护现状进行的测试评价，获取信息系统的全面保护需求。

1.6.4 信息系统安全分级保护测评标准

信息系统安全等级保护标准主要针对的是非涉密系统，按照其重要程度，对其进行等级划分，不同级别采取不同的保护措施。针对涉密信息系统，主要采用分级保护的方法，并按照信息系统安全分级保护测评标准进行测评。

分级保护针对涉密信息系统，根据其涉密等级涉密信息系统的重要性，遭到破坏后对国计民生造成的危害性，以及涉密信息系统必须达到的安全保护水平等划分为秘密级、机密级和绝密级三个等级。在建设、运行等环节按照其涉密等级实行分级保护。国家保密测评中心是我国唯一的涉密信息系统安全保密测评机构。国家保密测评中心隶属于国家保密局，在各省市下设国家保密测评分中心，专门负责对涉密信息系统进行安全测评。国家保密局专门对涉密信息系统如何进行分级保护制定了一系列的管理办法和技术标准，即 BMB 系列标准，信息系统分级保护测评的依据就是 BMB 标准。

1.7 信息系统安全等级保护工作

《网络安全法》第二十一条要求“国家实施网络安全等级保护制度”，安全测评工作可分为风险评估和等级保护测评。因国家实施网络安全等级保护工作上升到法律，因此，本章重点介绍网络安全等级保护工作，从概念、分工、工作流程、基本要求和基本原则角度来阐述，使读者对安全测评工作能够有一个整体认识。

1.7.1 等级保护概念

1．基本概念

信息安全等级保护是指对国家秘密信息、法人、其他组织和公民的专有信息，以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。信息安全等级保护是提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。

《网络安全法》制定以来，等级保护术语中出现“信息系统安全等级保护”和“网络安全等级保护”并用的情况。由于目前权威部门并未对两种术语做出严格定义和区分，因此，本书不严格区分两种说法。但本书认为：信息系统安全等级保护的对象是信息系统，网络安全等级保护的对象主要包括网络基础设施、信息系统、大数据、云计算平台、物联网、工控系统等。

2．核心内涵

国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。在国家统一政策指导下，各单位、各部门依法开展等级保护工作，有关职能部门对信息安全等级保护工作实施监督管理。实行信息安全等级保护，是信息安全保障工作中国家意志的体现，具有明显的强制性。

3．等级划分

信息安全等级保护是将全国的信息系统（包括网络）按照重要性和遭受损坏后的危害程度分成五个安全保护等级，从第一级到第五级，逐级增高。各信息系统在坚持自主定级、自主保护的原则下，应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息

系统遭到破坏后对国家安全、社会秩序、公共利益及公民、法人和其他组织的合法权益的危害程度等因素确定保护等级。

信息系统安全等级由低到高分为五个等级。

第一级为自主保护级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级为指导保护级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级为监督保护级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级为强制保护级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级为专控保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。

表 1-4 所示为安全保护等级定级标准参考。

表 1-4　安全保护等级参考表

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4．等级监管

国家通过制定统一的管理规范和技术标准，组织行政机关、公民、法人和其他组织根据信息和信息系统的不同重要程度开展有针对性的保护工作。国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策。

第一级，依照国家管理规范和技术标准进行自主保护；

第二级，在信息安全监管职能部门指导下，依照国家管理规范和技术标准进行自主保护；

第三级，依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查；

第四级，依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查；

第五级，依照国家管理规范和技术标准进行自主保护，国家指定专门部门、专门机构进行专门监督。

5．等级保护的五个目标

通过实施信息安全等级保护，信息系统达到五方面目标：一是信息系统安全管理水平明显提高；二是信息系统安全防范能力明显增强；三是信息系统安全隐患和安全事故明显减少；四是有效保障信息化健康发展；五是有效维护国家安全、社会秩序和公共利益。

6．等级保护制度特点

等级保护制度具有以下特点：一是紧迫性，信息安全滞后于信息化发展，重要信息系统的安全保障需求迫切；二是全面性，内容涉及广泛，各单位各部门落实；三是基础性，等级保护是国家的一项基本制度、基本国策；四是强制性，要求公安机关等监管部门进行监督、检查、指导等级保护工作；五是规范性，国家出台系列政策和标准，保障等级保护工作的开展。

1.7.2 工作角色和职责

1．国家监管部门

公安机关负责信息安全等级保护工作的监督、检查、指导，是等级保护工作的牵头部门；国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导；国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导；涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理；国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

2．等级保护协调工作小组

负责信息安全等级保护工作的组织领导，制定本地区、本行业开展信息安全等级保护的工作部署和实施方案，并督促有关单位落实，研究、协调、解决等级保护工作中的重要工作事项，及时通报或报告等级保护实施工作的相关情况。

3．信息系统主管部门

负责依照国家信息安全等级保护的管理规范和技术标准，督促、检查和指导本行业、本部门或者本地区信息系统运营和使用单位的信息安全等级保护工作。

4．信息系统运营、使用单位

负责依照国家信息安全等级保护的管理规范和技术标准，确定其信息系统的安全保护等级，有主管部门的，应当报其主管部门审核批准；根据已经确定的安全保护等级，到公安机关办理备案手续；按照国家信息安全等级保护管理规范和技术标准，进行信息系统安全保护的规划设计；使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品和信息安全产品，开展信息系统安全建设或者改建工作；制定、落实各项安全管理制度，定期对信息系统的安全状况、安全保护制度及措施的落实情况进行自查，选择符合国家相关规定的等级测评机构，定期进行等级测评；制定不同等级信息安全事件的响应、处置预案，对信息系统的信息安全事件分等级进行应急处置。

5．信息安全服务机构

负责根据信息系统运营、使用单位的委托，依照国家信息安全等级保护的管理规范和技术标准，协助信息系统运营、使用单位完成等级保护的相关工作，包括确定其信息系统的安全保护等级，进行安全需求分析、安全总体规划，实施安全建设和安全改造等。

6．信息安全等级测评机构

负责根据信息系统运营、使用单位的委托或根据国家管理部门的授权，协助信息系统运营、使用单位或国家管理部门，按照国家信息安全等级保护的管理规范和技术标准，对已经完成等级保护建设的信息系统进行等级测评；对信息安全产品供应商提供的信息安全产品进行安全测评。

7．信息安全产品供应商

负责按照国家信息安全等级保护的管理规范和技术标准，开发符合等级保护相关要求的信息安全产品，接受安全测评；按照等级保护相关要求销售信息安全产品并提供相关服务。

8．信息安全等级保护专家组

宣传等级保护相关政策、标准；指导备案单位研究拟定贯彻实施意见和建设规划、技术标准的行业应用；参与定级和安全建设整改方案论证、评审；协助发现树立典型、总结经验并推广；跟踪国内外信息安全技术最新发展，开展等级保护关键技术研究；研究提出完善等级保护政策体系和技术体系的意见和建议。

1.7.3 工作环节

根据《信息安全等级保护管理办法》的规定，等级保护主要由五个环节组成：定级、备案、建设整改、等级测评、安全监管。

1．定级

定级是信息安全等级保护的首要环节和关键环节，通过定级可以梳理各行业、各部门、各单位的信息系统类型、重要程度和数量等基本信息，确定分级保护的重点。定级不准，系统备案、建设、整改、等级测评等后续工作都会失去意义，信息系统安全就没有保证。

依据《关于开展全国重要信息系统安全等级保护定级工作的通知》的要求，信息系统定级按照自主定级、专家评审、主管部门审批、公安机关备案的工作流程进行。

首先，开展信息系统基本情况的摸底调查。各行业主管部门、运营使用单位开展对所属信息系统的摸底调查，全面掌握信息系统的数量、分布、业务类型、应用或服务范围、系统结构等基本情况，按照《信息安全等级保护管理办法》和《信息系统安全等级保护定级指南》的要求，确定定级对象。各行业主管部门要根据行业特点提出指导本地区、本行业定级工作的具体意见。

其次，初步确定定级对象的安全保护等级，起草定级报告。跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。涉密信息系统的等级确定按照国家保密局的有关规定和标准执行。

接着，专家评审和主管单位审批。初步确定信息系统安全保护等级后，可以聘请专家进行评审。对拟确定为第四级以上的信息系统，由运营使用单位或主管部门请国家信息安全保护等级专家评审委员会评审。运营使用单位或主管部门参照评审意见最后确定信息系统安全保护等级，形成定级报告。当专家评审意见与信息系统运营使用单位或其主管部门意见不一致时，由运营使用单位或主管部门自主决定信息系统安全保护等级。信息系统运营使用单位有上级行业