Information Security Management Guidance
ISMG-005-2006

BS7799 标准全面解析（新版）

Overall Explanation for BS7799 new version

张耀疆

CISSP，BS7799LA，CISA

上海安言信息技术有限公司
邮箱：yaojiang@aryasec.com
网址：www.aryasec.com
MSN：zhangyaojiang@hotmail.com

内容摘要

整个 2005 年，信息安全业界发生很多新气象，特别引人瞩目的就是 BS7799 标准的改版和国际化。BS7799 是英国标准协会（British Standards Institute，BSI）最早发布的一个关于信息安全管理的标准，其两个组成部分目前已分别成为 ISO17799 和 ISO27001 标准，以 ISO27001 标准为认证目标的信息安全管理体系实施活动正在国际和国内盛行起来。本文在 ISMG-005 最初版本的基础上，聚焦于 ISO17799:2005 和 ISO27001:2005 新标准，以问答的形式，概述其来龙去脉、价值所在、框架内容、认证要求，以及围绕此标准开展信息安全管理体系建设与审核活动的相关事项，目的在于为读者提供一份直接了解 BS7799 并加强信息安全管理实践的指南和参考文件。

在行文过程中，作者参考了大量文献资料，并将长期积累的实践经验融合进来，最终成此专题。由于目前可见于公众的此方面专题资料并不是很多，加上真正以 BS7799 为指导的信息安全管理活动商未被普遍认知，所以本文内容难免有偏颇之处，作者个人经验显见其中，读者请自行揣摩，决定取舍。另外，虽然目前 BS7799 已有了新的名称，但鉴于思维惯性，所以本文还是以 BS7799 名称泛指，具体条文阐述，则以 ISO17799 或 ISO27001 论之。

若有建议和意见，欢迎直接致函作者，交朋纳友乃作者平生之好。

关于 ISMG

本文作为“信息安全管理指导文件（Information Security Management Guidance，ISMG”系列之一而提供。ISMG 系列文件是安言咨询围绕信息安全管理这一实践主题而编写的一系列指导性文件，目的在于为信息安全管理实践者提供有效的建议和帮助。ISMG 系列文件的主题主要涉及信息安全风险管理、信息安全体系建设、信息安全服务过程、信息安全策略编写、业务连续性管理、BS7799 标准实施等。

欢迎有志于 ISMG 文件编写的专业人士与我们联系，加入到我们这个队伍中来，共同为国内信息安全事业的整体发展尽心尽力。

关于安言咨询

上海安言信息技术有限公司（简称安言咨询），是一家从事信息安全管理咨询的专业化机构。公司致力于兼收并蓄国际上最先进的信息安全和 IT 服务管理理念，结合国内行业特点，以独立咨询客观立场，为客户提供量身定做并且符合国际标准要求的信息安全解决方案。

安言咨询凭借多年经营积累起来的信息安全培训体系和咨询服务体系，以充足而完备的内容和资源，将 BS7799、BS15000、ISO13335、SSE-CMM、ITIL、CoBit 等最佳实践的精

髓恰当地移植给企业客户，充分发掘企业真正的需求，提升企业信息安全整体意识，增强相关人员的技术技能，巩固和完善企业信息安全管理体系，开拓 IT 服务管理的眼界和思维，建立稳妥的业务持续性计划，使信息安全和 IT 服务真正成为企业整体发展的助动之力。

安言咨询是一个由精英人才凝聚而成的团队，拥有多年电信、金融、制造、政府等行业背景，持有包括 CISSP、CISA、BS7799LA、ITIL、CCIE 等在内的众多信息管理或技术领域顶级资质。与此同时，公司还与包括 BSI、DNV、（ISC）2、ISACA、上海交通大学、上海信息中心等国内外著名机构保持着紧密的合作关系。

相信借助我们长期积累的经验和先进的理念，加上不懈而严谨的努力，定能为客户开启信息安全管理和 IT 服务管理的胜利之门。

公司网址：www.aryasec.com

关于作者

本文作者张耀疆（CISSP、CISA、BS7799LA、ITIL Foundation、CCNA、MCSE、MCSD），信息安全专业硕士，在 IT 及信息安全领域从业多年，先后在西安、深圳、上海等地多家公司从事过软件开发、系统集成、咨询评估、专业培训等项工作，积累了丰富的专业经验，这些经验先后汇集成《聚焦黑客－攻击手段与防护策略》、《CISSP 认证考试指南》等多部著译作。作者目前就任上海安言信息技术有限公司 CTO，负责信息安全咨询服务和专业培训相关工作。

作者联系方式：

Mobile：13816683689
MSN：zhangyaojiang@hotmail.com
QQ：3304964
Email：yaojiang@aryasec.com

版本信息

文档名称	**BS7799 标准全面解析（新版）**		
文档管理编号	ISMG-005-2006		
保密级别		文档版本号	1.0
制作人	张耀疆	制作日期	2006 年 1 月 24 日（V1.0）
复审人		复审日期	
分发范围	共享		
分发批准人			

目录

1. 概述篇

1.1 什么是信息？

ISO/IEC 的 IT 安全管理指南（GMITS，即 ISO/IEC TR 13335）对信息（Information）的解释是：信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。

一般意义上的信息概念是指事物运动的状态和方式，是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。通常情况下，我们可以把信息可以理解为消息、信号、数据、情报和知识。信息本身是无形的，借助于信息媒体以多种形式存在或传播，它可以存储在计算机、磁带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络、打印机、传真机等方式进行传播。

对现代企业来说，信息是一种资产，包括计算机和网络中的数据，还包括专利、标准、商业机密、文件、图纸、管理规章、关键人员等，就象其它重要的商业资产那样，信息资产具有重要的价值，因而需要进行妥善保护。

需要注意的是，从安全保护的角度去考察信息资产，并不能只停留在静态的一个点或者一个层面上。信息是有生命周期的，从其创建或诞生，到被使用或操作，到存储，再到被传递，直至其生命期结束而被销毁或丢弃，各个环节各个阶段都应该被考虑到，安全保护应该兼顾信息存在的各种状态，不能够有所遗漏。

1.2 什么是信息安全？

信息安全是一个广泛而抽象的概念，不同领域不同方面对其概念的阐述都会有所不同。建立在网络基础之上的现代信息系统，其安全定义较为明确，那就是：保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。在商业和经济领域，信息安全主要强调的是消减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降低到最低程度。

信息作为一种资产，是企业或组织进行正常商务运作和管理不可或缺的资源。从最高层次来讲，信息安全关系到国家的安全；对组织机构来说，信息安全关系到正常运作和持续发展；就个人而言，信息安全是保护个人隐私和财产的必然要求。无论是个人、组织还是国家，保持关键的信息资产的安全性都是非常重要的。信息安全的任务，就是要采取措施（技术手段及有效管理）让这些信息资产免遭威胁，或者将威胁带来的后果降到最低程度，以此维护组织的正常运作。

总的来说，凡是涉及到保密性、完整性、可用性、可追溯性、真实性和可靠性保护等方面的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

1.3 信息安全发展过程是怎样的？

信息安全自古以来就是受到人们关注的问题，但在不同的发展时期，信息安全的侧重点和控制方式是有所不同的。

大致说来，信息安全在其发展过程中经历了三个阶段。

早在 20 世纪初期，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在

的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全，即 COMSEC（Communication Security）。

20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，即 INFOSEC（Information Security），具有代表性的成果就是美国的 TCSEC 和欧洲的 ITSEC 测评标准。

20 世纪 80 年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性三个原则了，由此衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也从单一的被动防护向全面而动态的防护、检测、响应、恢复等整体体系建设方向发展，即所谓的信息保障（Information Assurance），这一点，在美国的 IATF 规范中有清楚的表述。

1.4 信息安全有哪些基本目标？

信息安全通常强调所谓 CIA 三元组的目标，即保密性、完整性和可用性（如图 1 所示）。CIA 概念的阐述源自信息技术安全评估标准（InformationTechnology Security Evaluation Criteria，ITSEC），它也是信息安全的基本要素和安全建设所应遵循的基本原则。

- **保密性（Confidentiality）——** 确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。
- **完整性（Integrity）——** 确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。
- **可用性（Availability）——** 确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

图 1. 信息安全 CIA 三元组

当然，不同机构和组织，因为需求不同，对 CIA 原则的侧重也会不同，如果组织最关心的是对私秘信息的保护，就会特别强调保密性原则，如果组织最关心的是随时随地向客户提供正确的信息，那就会突出完整性和可用性的要求。

除了 CIA，信息安全还有一些其他原则，包括可追溯性（Accountability）、抗抵赖性（Non-repudiation）、真实性（Authenticity）、可控性（Controllable）等，这些都是对 CIA 原则的细化、补充或加强。

与 CIA 三元组相反的有一个 DAD 三元组的概念，即泄漏（Disclosure）、篡改（Alteration）和破坏（Destruction），实际上 DAD 就是信息安全面临的最普遍的三类风险，是信息安全实践活动最终应该解决的问题。

1.5 什么是信息安全的根本目标？

对一个企业来说，生存发展是头等大事，而企业的生存和发展，有赖于企业所特有的各项业务活动的健康有序的进行。对现代企业来说，高度信息化是必然之道，是企业一切业务、管理和运作活动所依赖的基础之一。由此看来，信息系统是否能够稳定、可靠、有效运转，直接关系到企业各项业务活动是否能够持续。而要保证业务活动能够健康有效地持续下去，信息系统必然要提供所需的保障。

之前我们提到了，信息安全的目标是保密性、完整性和可用性，或者再加上可控性、抗抵赖性等，但对现代企业来说，对 CIA 的追求只是一种简单抽象的理解，是信息安全的直接目标，其实企业最关心的，是其关键业务活动的持续性和有效性，这是企业命脉所在，就信息安全来说，是其根本目标。当然，要让依赖于信息环境的业务活动能够持续，就必然要保证信息环境的安全，业务持续性对信息环境提出了 CIA 的要求，而信息环境 CIA 的实现支持着业务持续性目标的实现。

企业从自身利益出发，把着眼点归结到业务活动的切实需求上，信息安全才能做到真正的有始而发和有的放矢。

1.6 信息安全需求来自哪里？

对组织来说，信息是需要采取措施加以保护的重要资产，但在具体采取安全措施之前，组织必须先明确自己的安全需求，需要保护哪些信息资产？需要投入多大力度？应该达到怎样的保护程度？这些都要通过需求分析来加以明确。

一般来讲，组织的信息安全需求有三个来源。

（1） 法律法规与合同条约的要求

与信息安全相关的法律法规是对组织的强制性要求，组织应该对现有的法律法规加以识别，将适用于组织的法律法规转化为组织的信息安全需求。这里所说的法律法规有三个层次，即国家法律、行政法规和各部委和地方的规章及规范性文件。此外，组织还要考虑商务合作者和客户对组织提出的具体的信息安全要求，包括合同约定、招标条件和承诺等。例如，合同中可能会明确要求组织的信息安全管理体系遵循 BS7799 标准。

（2） 组织的原则、目标和规定

组织从自身业务和经营管理的需求出发，必然会在信息技术方面提出一些方针、目标、原则和要求，据此明确自己的信息安全要求，确保支持业务运作的信息处理活动的安全性。

（3） 风险评估的结果

除了以上两个信息安全需求的来源之外，确定安全需求最主要的一个途径就是进行风险评估，组织对信息资产的保护程度和控制方式的确定都应建立在风险评估的基础之上。一般来讲，通过综合考虑每项资产所面临的威胁、自身的弱点、威胁造成的潜在影响和发生的可能性等因素，组织可以分析并确定具体的安全需求。风险评估是信息安全管理的基础。

1.7 如何做好信息安全整体规划？

信息安全目标的实现并非一日之功，也不能一蹴而就，必须是一个整体考虑、充分规划、持续运作、长治久安的过程。在整个过程中，组织的最高管理者必须发挥积极的作用。一方面，最高管理者应该为信息安全活动提供资源支持，协调各个方面的关系，更重要的，要想实现信息安全长效目标，最高管理者必须明确信息安全目标和方针，在战略决策上指引正确的方向，在整体规划上确定清晰的蓝图。

什么事情都是从计划开始的，信息安全也是如此，计划有多种，具体某项事务有短期的实施计划，阶段性任务的完成和目标的实现有赖于中期计划，而根本目标的实现则必须有较长期的战略计划做依托。对组织的高级管理者来说，制定健全而有效的信息安全战略规划，是其必然的责任。

一般来说，组织在信息安全建设方面都会有较长期（例如 2 到 3 年）的整体规划，明确信息安全目标和原则，发掘信息安全需求，落实信息安全组织和责任，做好阶段计划和成果诉求。有了这样的规划作为方向指引，信息安全各项工作就能在有序的状态下逐渐开展了。

信息安全整体规划最终会落脚在一幅可以预期的蓝图上，这便是组织信息安全整体所呈现出来的架构和模式，图 2 所示即一个很好的例子。

图 2. 信息安全蓝图

这副蓝图中有以下几项要素：

- **目标 Objective**：蓝图中首先明确的是信息安全建设的核心目标，即实现信息安全的 CIA 并最终确保业务持续性，这是 InfoSec 所代表的含义。
- **对象 Object**：信息安全必须有明确的保护对象，即信息资产，包括各种关键数据、应用系统、实物资产、设施和环境，以及人员。信息资产的明确界定，将使信息安全控制的实施有引而发。而对这些资产的保护，将直接关系到业务持续性这一最终目标的实现与否。
- **规范 Document**：为了实现核心目标，我们还必须明确信息安全方面的现实需求，并且用确定的、无矛盾的、可实施的一套方针、标准、指南、程序和规范要求来体现，这些层次化的文件将为所有信息安全活动提供指导，最终导入信息安全需求的实现。其实，信息安全管理体系是一个文件化的体系，文件所约定的各项管理要求和操作规范，能够体现信息安全目标实现的持久、统一和权威性，也是 ISMS 的具

体表现形式。

- **过程 Process**：为了对信息资产实施保护，我们必须采取一定措施，经历一番努力和过程，最终才能实现既定目标。信息安全的建设过程，表现为一系列流程的实现，最终体现出的是所谓 PDCA 的过程模型：信息安全先做规划，明确需求，制定应对方案；实施解决方案；通过检查，巩固成果，发现不足；采取后续措施，改进不足，推动信息安全持续进步。

1.8 怎样实现信息安全？

为了消减信息和信息系统面临的众多风险，满足既定的信息安全需求，人们能想到的最直接做法，就是选择并使用各种能够解决信息安全问题的技术和产品。

与信息安全的发展历程一样，信息安全技术在不同的阶段也表现出不同的特点。在通信安全阶段，针对数据通信的保密性需求，人们对密码学理论和技术的研究及应用逐渐成熟了起来。随着计算机和网络技术的急遽发展，信息安全阶段的技术要求集中表现为 ISO 7498-2 标准中陈述的各种安全机制上面，这些安全机制的共同特点就是对信息系统的保密性、完整性和可用性进行静态的防护。到了互联网遍布全球的时期，以 IATF（信息保障技术框架）为代表的标准规范为我们勾画出了更全面更广泛的信息安全技术框架，这时的信息安全技术，已经不再是以单一的防护为主了，而是结合了防护、检测、响应和恢复这几个关键环节在一起的动态发展的完整体系。

归纳起来，典型的信息安全技术包括：

- **物理安全技术**：环境安全、设备安全、媒体安全；
- **系统安全技术**：操作系统及数据库系统的安全性；
- **网络安全技术**：网络隔离、访问控制、VPN、入侵检测、扫描评估；
- **应用安全技术**：Email 安全、Web 访问安全、内容过滤、应用系统安全；
- **数据加密技术**：硬件和软件加密，实现身份认证和数据信息的 CIA 特性；
- **认证授权技术**：口令认证、SSO 认证（例如 Kerberos）、证书认证等；
- **访问控制技术**：防火墙、访问控制列表等；
- **审计跟踪技术**：入侵检测、日志审计、辨析取证；
- **防病毒技术**：单机防病毒技术逐渐发展成整体防病毒体系；
- **灾难恢复和备份技术**：业务连续性技术，前提就是对数据的备份。

解决信息及信息系统的安全问题不能只局限于技术，更重要的还在于管理。安全技术只是信息安全控制的手段，要让安全技术发挥应有的作用，必然要有适当的管理程序的支持，否则，安全技术只能趋于僵化和失败。如果说安全技术是信息安全的构筑材料，那信息安全管理就是真正的粘合剂和催化剂，只有将有效的安全管理从始至终贯彻落实于安全建设的方方面面，信息安全的长期性和稳定性才能有所保证。

现实世界里大多数安全事件的发生和安全隐患的存在，与其说是技术上的原因，不如说是管理不善造成的，理解并重视管理对于信息安全的关键作用，对于真正实现信息安全目标来说尤其重要。我们常说，信息安全是三分技术七分管理，可见管理对于信息安全的重要性。

从概念上讲，信息安全管理（Information Security Management）作为组织完整的管理体系中一个重要的环节，构成了信息安全具有能动性的部分，是指导和控制组织的关于信息安全风险的相互协调的活动，其针对对象就是组织的信息资产。

安全管理牵涉到组织的信息评估、开发和文档化，以及对实现保密性、完整性和可用性目标的策略、标准、程序及指南的实施。安全管理要求识别威胁、分类资产，并依据脆弱性分级来有效实施安全控制。

同其他管理问题一样，安全管理也要解决组织、制度和人员这三方面的问题，具体来说就是：建设信息安全管理的组织机构并明确责任，建立健全的安全管理制度体系，加强人员的安全意识并进行安全培训和教育，只有这样，信息安全管理才能实现包括安全规划、风险管理、应急计划、意识培训、安全评估、安全认证等多方面的内容。

应该注意的是，人们对信息安全管理的认识是在信息安全技术之后才逐渐深入和发展起来的，关于信息安全管理的标准和规范也没有安全技术那么众多，最有代表性的，就是 BS 7799 和 ISO 13335。

1.9 为什么要一再强调信息安全管理？

长久以来，很多人自觉不自觉地都会陷入技术决定一切的误区当中，尤其是那些出身信息技术行业的管理者和操作者。最早的时候，人们把信息安全的希望寄托在加密技术上面，认为一经加密，什么安全问题都可以解决。随着互连网络的发展，一段时期我们又常听到“防火墙决定一切”的论调。及至更多安全问题的涌现，入侵检测、PKI、VPN 等新的技术应用被接二连三地提了出来，但无论怎么变化，还是离不开技术统领信息安全的路子。可这样的思路能够真正解决安全问题吗？也许可以解决一部分，但却解决不了根本。实际上，对安全技术和产品的选择运用，这只是信息安全实践活动中的一部分，只是实现安全需求的手段而已。信息安全更广泛的内容，还包括制定完备的安全策略，通过风险评估来确定需求，根据需求选择安全技术和产品，并按照既定的安全策略和流程规范来实施、维护和审查安全控制措施。归根到底，信息安全并不是技术过程，而是管理过程。

之所以有这样的认识误区，原因是多方面的，从安全产品提供商的角度来看，既然侧重在于产品销售，自然从始至终向客户灌输的都是以技术和产品为核心的理念。而从客户角度来看，只有产品是有形的，是看得见摸得着的，对决策投资来说，这是至关重要的一点，而信息安全的其他方面，比如无形的管理过程，自然是遭致忽略。

正是因为有这样的错误认识，我们就经常看到：许多组织使用了防火墙、IDS、安全扫描等设备，但却没有制定一套以安全策略为核心的管理措施，致使安全技术和产品的运用非常混乱，不能做到长期有效和更新。即使组织制定有安全策略，却没有通过有效的实施和监督机制去执行，使得策略空有其文成了摆设而未见效果。

实际上对待技术和管理的关系应该有充分理性的认识：技术是实现安全目标的手段，管理是选择、实施、使用、维护、审查包括技术措施在内的安全手段的整个过程，是实现信息安全目标的必由之路。

在现实的信息安全管理决策当中，必须关注以下几点：

- 应该制定信息安全方针和多层次的安全策略，以便为各项信息安全管理活动提供指引和支持；
- 应该通过风险评估来充分发掘组织真实的信息安全需求；
- 应该遵循预防为主的理念；
- 应该加强人员安全意识和教育；
- 管理层应该足够重视并提供切实有效的支持；
- 应该持有动态管理、持续改进的思想；
- 应该以业务持续发展为目标，达成信息安全控制的力度、使用的便利性以及成本投入之间的平衡。

1.10 信息安全管理应该遵循何种模式？

在信息安全管理方面，BS7799 标准为我们提供了指导性建议，即基于 PDCA（Plan、Do、Check 和 Act，即戴明环）的持续改进的管理模式，如图 3 所示。

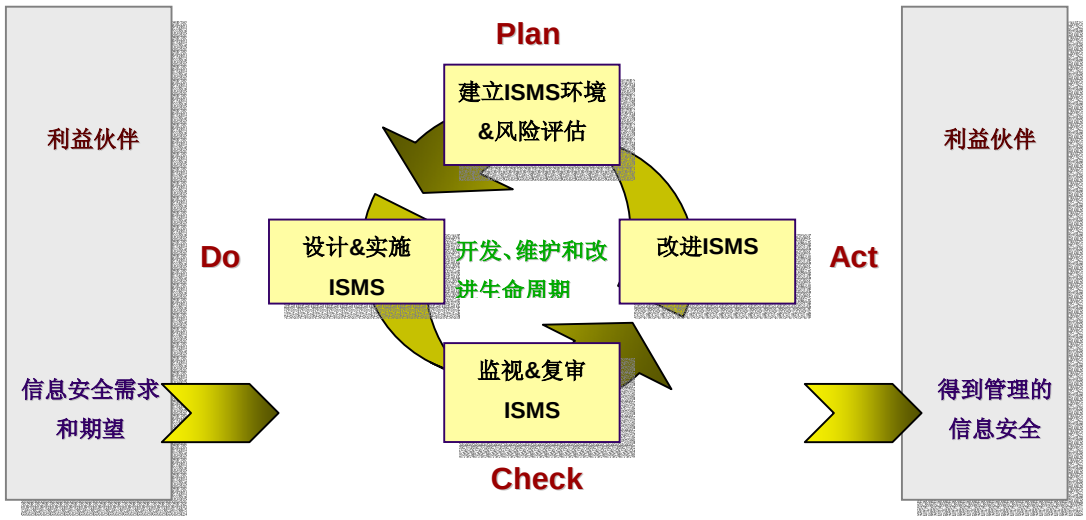

图 3.　PDCA 信息安全管理模式

PDCA（Plan、Do、Check 和 Act）是管理学惯用的一个过程模型，最早是由休哈特（Walter Shewhart）于 19 世纪 30 年代构想的，后来被戴明（Edwards Deming）采纳、宣传并运用于持续改善产品质量的过程当中。随着全面质量管理理念的深入发展，PDCA 最终得以普及。

作为一种抽象模型，PDCA 把相关的资源和活动抽象为过程进行管理，而不是针对单独的管理要素开发单独的管理模式，这样的循环具有广泛的通用性，因而很快从质量管理体系（QMS）延伸到其他各个管理领域，包括环境管理体系（EMS）、职业健康安全管理体系（OHSMS）和信息安全管理体系（ISMS）。

为了实现 ISMS，组织应该在计划（Plan）阶段通过风险评估来了解安全需求，然后根据需求设计解决方案；在实施（Do）阶段将解决方案付诸实现；解决方案是否有效？是否有新的变化？应该在检查（Check）阶段予以监视和审查；一旦发现问题，需要在措施（Act）阶段予以解决，以便改进 ISMS。通过这样的过程周期，组织就能将确切的信息安全需求和期望转化为可管理的信息安全体系。

概括起来，PDCA 模型具有以下特点，同时也是信息安全管理工作的特点：

- PDCA 顺序进行，依靠组织的力量来推动，像车轮一样向前进，周而复始，不断循环，持续改进；
- 组织中的每个部门，甚至每个人，在履行相关职责时，都是基于 PDCA 这个过程的，如此一来，对管理问题的解决就成了大环套小环并层层递进的模式；
- 每经过一次 PDCA 循环，都要进行总结，巩固成绩，改进不足，同时提出新的目标，以便进入下一次更高级的循环。

2. 标准篇

2.1 什么是 BS7799？

BS7799 是英国标准协会（British Standards Institute，BSI）针对信息安全管理而制定的一个标准，最早始于 1995 年，后来几经改版，成为了目前由两部分内容构成的并且被广泛接受的信息安全管理标准。

BS7799 分两个部分，第一部分，也就是刚刚被 ISO 组织吸纳成为 ISO/IEC 17799:2005 标准的部分，是信息安全管理实施细则（Code of Practice for Information Security Management），主要供负责信息安全系统开发的人员作为参考使用，其中分十一个标题，定义了 133 项安全控制（最佳惯例）。BS7799 标准的第二部分内容，即最新的 ISO/IEC 27001:2005，是建立信息安全管理体系（ISMS）的一套规范（Specification for Information Security Management Systems），其中详细说明了建立、实施和维护信息安全管理体系的要求，可用来指导相关人员去应用 ISO/IEC 17799，其最终目的，在于建立适合企业需要的信息安全管理体系（ISMS）。

虽然 BS7799 最初是以所谓的“英国标准（British Standard）”而推出的，但并非只适用于英国，BS7799（目前准确来说应该是 ISO/IEC 17799:2005 和 ISO/IEC 27001:2005）所包含的最佳惯例可以在不同的法律和文化背景下实施。由于 BS7799 两个部分都已经先后转化成正式的国际标准，从发展眼光来看，今后几年时间里，以该标准为参照的信息安全相关活动，势必在全球范围内广泛开展起来。

顺便提及的是，英国标准协会（BSI）是世界上最早的全国性标准化机构，同时也是国际标准化组织的核心成员之一，它不受政府控制但得到了政府的大力支持。BSI 制定和修订的许多英国标准最终都转化成了国际标准，其在 ISO 中的贡献率达到了 17%，包括 ISO9000 质量管理体系（源自 BS5750）、ISO14000 环境管理体系（源自 BS7750）和 OHSAS18000 职业健康和安全管理体系（源自 BS8800）等。

2.2 BS7799 的发展历程是怎样的？

BS7799 从诞生到现在只不过 10 年间的事情，但基本上可以看出一个标准“源于生活，高于生活”的发展特点，也就是说，一个真正普遍适用并能被普遍接受的标准，必然是能体现相关领域最佳惯例并能为最佳惯例的推广起指导作用的。

BS7799 最初是由英国贸工部（DTI）立项的，是业界、政府和商业机构共同倡导的，旨在开发一套可供开发、实施和测量有效安全管理惯例并提供贸易伙伴间信任的通用框架。负责标准开发和管理工作的 BSI-DISC Committee BDD/2 是由来自贸易和工业部门的众多代表共同组成的，其成员在各自的领域都具有足够的影响力，包括金融业的英国保险协会、渣打会计协会、汇丰银行等，通信行业有大英电讯公司，还有像壳牌、联合利华、毕马威（KPMG）等这样的跨国机构。

1995 年，BS7799-1:1995《信息安全管理实施细则》首次出版（其前身是 1993 年发布的 PD0005），它提供了一套综合性的、由信息安全最佳惯例构成的实施细则，目的是为确定各类信息系统通用控制提供唯一的参考基准。

在随后一段时间里，由于电子商务的发展，由此引发客户、供应商、贸易伙伴间对各自信息保护能力的信任问题，促使第三方认证成为一个急需。信息安全管理遵循一套最佳惯例，但怎样做的？执行程度如何？是否完备？这就需要有一个共同的尺度来进行衡量。

1998 年，BS7799-2:1998《信息安全管理体系规范》公布，这是对 BS7799-1 的有效补充，它规定了信息安全管理体系的要求和对信息安全控制的要求，是一个组织信息安全管理体系评估的基础，可以作为认证的依据。至此，BS7799 标准初步成型。

1999 年 4 月，BS7799 的两个部分被重新修订和扩展，形成了一个完整版的 BS7799:1999。新版本充分考虑了信息处理技术应用的最新发展，特别是在网络和通信领域。除了涵盖以前版本所有内容之外，新版本还补充了很多新的控制，包括电子商务、移动计算、远程工作等。

由于 BS7799 日益得到国际认同，使用的国家也越来越多，2000 年 12 月，国际标准化组织 ISO/IEC JTC 1/SC27 工作组认可 BS7799-1:1999，正式将其转化为国际标准，即所颁布的 ISO/IEC 17799:2000《信息技术——信息安全管理实施细则》。作为一个全球通用的标准，ISO/IEC 17799 并不局限于 IT，也不依赖于专门的技术，它是由长期积累的一些最佳实践构成的，是市场驱动的结果。

2002 年，BSI 对 BS7799:2-1999 进行了重新修订，正式引入 PDCA 过程模型，以此作为建立、实施、持续改进信息安全管理体系的依据，同时，新版本的调整更显示了与 ISO9001:2000、ISO14001:1996 等其他管理标准以及经济合作与开发组织（OECD）基本原则的一致性，体现了管理体系融合的趋势。2004 年 9 月 5 日，BS7799-2:2002 正式发布，随即提交 ISO 并迈入“快速通道”。

2005 年 6 月，ISO/IEC 17799:2000 经过改版，形成了新的 ISO/IEC 17799:2005，新版本较老版本无论是组织编排还是内容完整性上都有了很大增强和提升。紧接着，被期待已久的 BS7799-2:2002 也终于被 ISO 组织所采纳，于同年 10 月推出了 ISO/IEC 27001:2005。至此，BS7799 标准的两个部分，都成为了正式的国际标准，作为一套完整的国际性的认证标准框架，BS7799 已经有了新的面貌。

据 BSI 官方消息，BS7799 标准在今后几年时间里还将有较大的扩充，最终形成的，将会是类似 ISO9000 形式一样的一个全面指导信息安全工作的标准体系。

在 BSI 的官方网站（www.bsi-global.com）上对 BS7799 是这么命名的：

- ISO/IEC 17799:2005 Code of practice for Information Security Management
- ISO/IEC 27001:2005 Information Security. Security techniques. Information security management systems. Requirements

2.3 BS7799 的现状如何？

在还没有成为国际标准的过去几年时间里，虽然有着不少争议，但以 BS7799 为参照的信息安全管理最佳惯例，依然在全球范围被接受和采用。如今，BS7799 已经成为国际标准，BS7799 所掀起的“浪潮”势必更加激烈和高迈。据统计，截至目前，已有二十多个国家和地区引用 BS7799 作为本国（地区）标准，并有四十多个国家和地区开展了于此相关的业务，其中包括：

- 澳大利亚/新西兰（前国标 AS/NZS 4444，现在国标 AS/NZS 7799）
- 巴西
- 捷克
- 芬兰
- 爱尔兰
- 冰岛

- 荷兰（SPE 20003）
- 挪威
- 意大利
- 瑞典（SS 627799）
- 日本（JIS X 5080，相当于 BS7799-1）
- 印度

我国的台湾和香港地区也已经采用并推广了 BS7799 标准。在台湾，BS7799-1:1999 被引用为 CNS 17799，而 BS7799-2:2002 则被引用为 CNS 17800。在中国大陆，BS7799 标准的国标化一直是个热点议题（目前，ISO17799:2000 已被转化为 GB/T 19716:2005），而相关的 ISMS 认证工作正在试点运行。

2.4 BS7799 将来还会有什么发展和变化？

按照 BSI 的规划（包括 ISO 的考虑），未来两年里，以 ISO/IEC 27001 为核心的信息安全管理标准将逐渐发展成为一套完整的标准族，具体包括：

- ISO/IEC 27000，基础和术语。
- ISO/IEC 27001，信息安全管理体系要求，已于 2005 年 10 月 15 日正式发布（ISO/IEC 27001:2005）。
- ISO/IEC 27002，信息安全管理体系最佳实践，将会在 2007 年 4 月直接由 ISO/IEC 17799:2005（已于 2005 年 6 月 15 日正式发布）转换而来。
- ISO/IEC 27003，ISMS 实施指南，正在开发。
- ISO/IEC 27004，信息安全管理度量和改进，正在开发。
- ISO/IEC 27005，信息安全风险管理指南，以 2005 年底刚刚推出的 BS7799-3（基于 ISO/IEC 13335-2）为蓝本。

这些标准或指南，相互支持和参照，共同为组织实施信息安全最佳实践和建立信息安全管理体系而发挥作用。

2.5 什么是 ISMS 国际用户组织？

ISMS International Users Group（简称 ISMS IUG），即信息安全管理体系国际用户组织，是英国商贸部（Department of Trade and Industry，DTI）于 1997 年成立的一个非营利组织，目的是促进国际上对 BS7799 标准的采用，推动标准应用方面经验的共享。这十多年来，DTI 一直积极支持 ISMS IUG，将其作为推动商业领域最佳实践活动的一个重要部分。

ISMS IUG 是全世界范围内信息安全管理体系用户共享最佳实践心得的一个平台，它经常会组织一些在线讨论活动，或者在全球各地组织研讨会。ISMS IUG 在全球很多地方都有成员组织，在各自国家范围内的讨论活动中扮演着重要的角色。

目前，ISMG IUG 的成员遍及 40 多个国家和地区，并且在澳大利亚、巴西、加拿大、德国、印度、日本、韩国、香港、挪威、波兰、新加坡、瑞典、美国等国家和地区建立有成员机构。

ISMG IUG 的网址是 http://www.xisec.com，该网站除了提供一些常识性信息外，还会提供 BS7799 相关研讨会、活动及最新发展动态的信息，包括对全球 BS7799 认证的最新统计。

实际上，IUG 这种组织形式不仅仅显现于信息安全管理体系，作为国际用户组织，IUG 通常都是围绕某一产品或者服务而由其用户成立的非营利组织，用于交流和共享经验，例如

Oracle 国际用户组织（International Oracle User Group，IOUG）。

2.6 还有哪些与 BS7799 类似或相关的标准或规范？

BS7799 作为一项通行的信息安全管理标准，旨在为组织实施信息安全管理体系（ISMS）提供指导性框架，尽管 BS7799 的第一部分也提供了诸多控制措施，但更多体现的是一种目标要求，总体来说，BS7799 并没有提及实施的细节，这是作为通行标准必然的局限。对组织来说，要真正将 BS7799 的要求和指导落到实处，必须补充必要的可实施内容，在这方面，有很多国际上相关的标准和规范可做参照。

2.6.1 PD 3000

BS7799 标准本身是不具有很强的可实施性的，为了指导组织更好地建立 ISMS 并应对 BS7799 认证审核的要求，BSI DISC 提供了一组有针对性的指导文件，即 PD 3000 系列，如表 1 所列。

表 1　　PD 3000 系列简介

代号	名称	内容简介
PD 3001	Preparing for BS7799 Certification	全面阐述信息安全本质、ISMS 定义以及 PDCA 过程规范，并对文档体系要求、文档记录控制、管理层责任、管理层复查、认证审计及审计报告等事项给予描述。附录给出一个策略声明的例子。
PD 3002	Guide to Risk Assessment and Risk Management	这里引用了很多 GMITS 的基本概念和方法描述。详细解释了风险评估的途径（基本的 RA、详细的 RA、组合的 RA）和过程。附录给出威胁和弱点例子、RA 的可行工具和方法。
PD 3003	Are you ready for a BS7799 Audit?	这份指南主要用于组织内部的符合性检查，首先是识别 ISMS 范围，其次进行 ISMS 过程检查（提供了一套对 ISMS 过程进行检查的问卷），最后是控制检查（提供了一套对控制实施进行检查的问卷）。
PD 3004	Guide to BS7799 Auditing	这份指南主要是为实施 ISMS 控制要求提供指导的，同时也为审计现有控制实施提供帮助。以 36 个控制目标和 127 项控制为内容结构，每个控制都从实施和审计两个方面提出一些要点。
PD 3005	Guide to the selection of BS7799 controls	描述了选择控制目标和控制的基本过程和考虑因素，并从法律要求、业务要求、风险评估结果三个方面，列举了各种可选的控制项，最后，还对各项控制如果缺乏会造成什么问题进行了列表描述。

这几个指导文件相互的关系如图 4 所示。

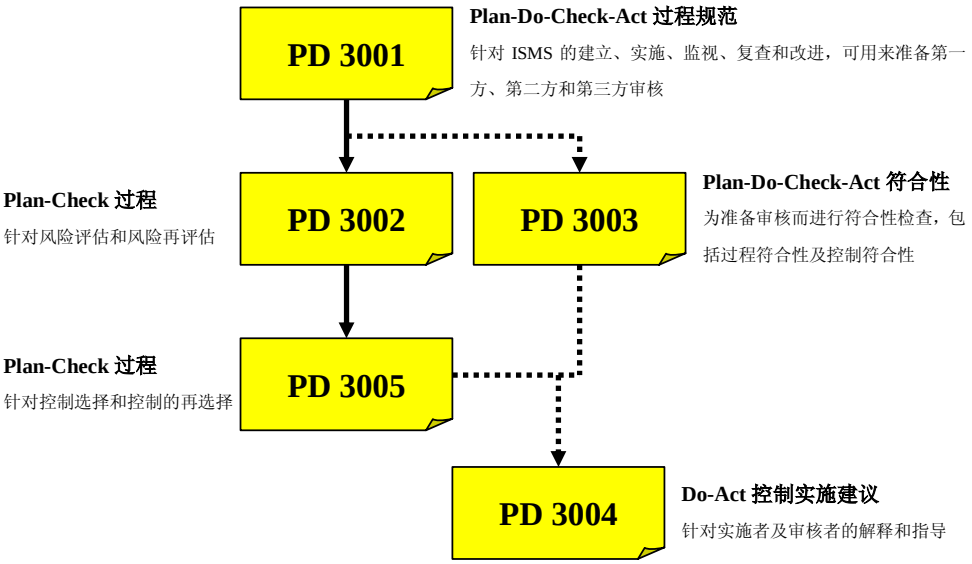

图 4.　PD3000 文件系列相互关系

总之，PD 3000 系列指导文件，不失为信息安全管理体系实施很好的助手。

2.6.2 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 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（Common Criteria）的发展经历了一个漫长而复杂的过程，图 5 所示能够比较清晰地看到这个过程。

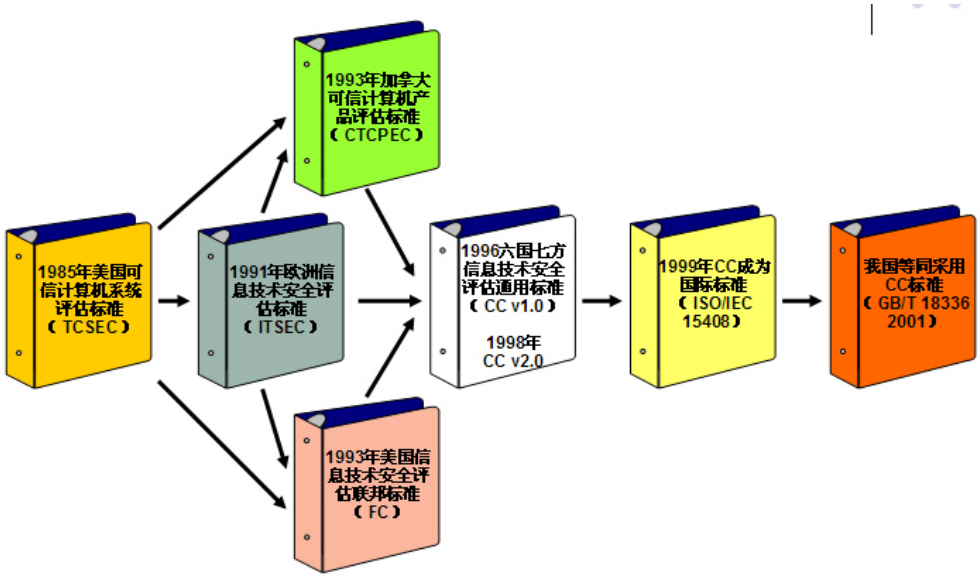

图 5.　CC 的发展过程

从图 5 我们可以看到，我们经常讲的 CC、ISO/IEC 15408、GB/T 18336，实际上是同一

个标准，只不过 CC 是最早的称谓，15408 是正式的 ISO 标准，18336 则是我国等同采用 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 3 个文件构成，如表 2 所列（以 ISO/IEC 15408 为例）。

表 2　　CC 标准组成部分

代号	名称	内容简介
ISO/IEC 15408-1	Introduction and general model	介绍和一般模型。这部分定义了 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。这部分按照“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。这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。

与 BS7799 标准相比，CC 的侧重点放在系统和产品的技术指标评价上，这和更广泛更高层次的管理要求是有很大区别的。BS7799 在阐述信息安全管理要求时，虽然涉及到某些技术领域，但并没有强调技术细节。一般来说，组织在依照 BS7799 标准来实施 ISMS 时，一些牵涉系统和产品安全的技术要求，可以借鉴 CC 标准。当然，从对信息安全的定义、对风险的认定等基本理念方面看，CC 与 BS7799 是一致的，毕竟关注的都是信息安全这一共同的领域。

2.6.3 ISO/IEC TR 13335

ISO/IEC TR 13335，早前被称作“IT 安全管理指南”（Guidelines for the Management of IT Security，GMITS），最新改版后，被称作“信息和通信技术安全管理”（Management of Information and Communications Technology Security，MICTS），是由 ISO/IEC JTC1 制定的技术报告，是一个信息安全管理方面的指导性标准，其目的是为有效实施 IT 安全管理提供建议和支持。

ISO/IEC TR 13335 分成 5 个部分，作为 GMITS，其完整框架如表 3 所列。

表 3　　ISO/IEC TR 13335 标准组成部分

代号	名称	内容简介
ISO/IEC13335-1:1996	Concepts and models for IT Security	IT 安全概念与模型。这部分包含了对 IT 安全和安全管理中一些基本概念和模型的解释。（已撤销）
ISO/IEC13335-2:1997	Managing and planning IT Security	IT 安全管理和计划。这部分建议性地介绍了 IT 安全管理和计划的方式和要点。（已撤销）

ISO/IEC133 35-3:1998	Techniques for the management of IT Security	IT 安全管理技术。这部分描述了风险管理技术、IT 安全计划的开发、实施和测试，还包括策略审查、事件分析、IT 安全教育等后续内容。（在修订）
ISO/IEC133 35-4:2000	Selection of safeguards	安全措施的选择。这部分描述了针对一个组织特定环境和安全需求可以选择的安全措施，不仅仅是技术性措施。（在修订）
ISO/IEC133 35-5:2001	Management guidance on network security	网络安全管理指南。这部分提供了关于网络和通信安全管理的指导性内容。该指南为识别和分析建立网络安全需求时需要考虑的通信相关因素提供支持，也包括对可能的安全措施方面的简要介绍。（在修订）

目前，ISO/IEC 13335-1:1996 已经被新的 ISO/IEC 13335-1:2004（MICTS 第 1 部分：信息和通信技术安全管理的概念和模型）所取代，ISO/IEC 13335-2:1997 也将被正在开发的 ISO/IEC 13335-2（MICTS 第 2 部分：信息安全风险管理）取代，GMITS 的其他三个部分都在重新修订当中。

与 BS7799 相比，ISO/IEC TR 13335 只是一个技术报告和指导性文件，并不是可依据的认证标准，也不像 BS7799 那样给出一个全面而完整的信息安全管理框架，但 13335 在信息安全尤其是 IT 安全的某些具体环节切入较深（相对 BS7799 而言），对实际的工作具有较好的指导价值，从可实施性上来说要比 BS7799 好些。比如说，13335 对信息安全风险及其构成要素间关系的描述非常具体，以至于成为各类信息安全相关文件经常引述的一个概念。此外，13335 所描述的风险评估方法过程很清晰，可用来指导实施。还有就是，13335 对安全计划、安全策略、控制措施选择等内容的阐述要比 BS7799 具体很多。

总之，作为一个框架、总体要求和目标选择，BS7799 是我们信息安全管理体系建设过程当中始终要贯彻的指导方针，而这期间一些具体的活动则可以参考 ISO/IEC TR 13335，比如风险评估。

2.6.4 AS/NZS 4360

AS/NZS 4360:1999 Risk Management 是澳大利亚和新西兰颁布的一个关于风险管理的标准，在国际上具有一定的影响力。在涉及风险评估与风险管理的具体方法和过程方面，AS/NZS 4360 可以为促进组织 ISMS 的 BS7799 符合性提供帮助。

AS/NZS 4360 定义了风险管理过程的 5 个步骤：

- 环境建立（Contexts established）—— 建立在风险管理过程中会用到的策略、组织和背景。
- 风险识别（Risks identified）—— 识别会出现的风险和出现的原因，为进一步分析打好基础。
- 风险分析（Risks analysed）—— 识别在现有控制作用下的风险后果和可能性，进一步估计风险程度。
- 风险评价（Risks evaluated）—— 将估计的风险等级与预先建立的标准进行比较，得到按等级排列的风险，以便识别管理的优先顺序。
- 风险处理（Risks treated）—— 接受并监控低优先级的风险，而对其他风险，应该建立并实施特定的管理计划，包括对所需资金的考虑。

2.6.5 ISO/TR 13569

ISO/TR 13569，是 ISO TC68/SC2/WG4 制定的银行和相关金融服务信息安全指南（Banking and related financial services-Information security guidelines）。该文件为金融服务行业开发信息技术风险评估提供了指导，其中包含一个风险分析过程的例子，以及对选择并实施安全控制措施的考虑，还包含在现代金融服务组织内部进行 IT 安全风险管理必要的其他一些要素，例如安全策略、安全组织和人员责任、安全意识等。

2.6.6 SSE-CMM

CC 是侧重信息安全技术的标准，BS7799 是针对信息安全管理的标准，但二者都没有对信息安全建设过程进行具体阐述，也没有考虑实施者在信息安全建设过程中表现出来的能力和水平，在这方面，SSE-CMM 是一个不错的参照。

SSE-CMM（System Security Engineering Capability Maturity Model）模型是 CMM 在系统安全工程这个具体领域应用而产生的一个分支，是美国国家安全局（NSA）领导开发的，是专门用于系统安全工程的能力成熟度模型。SSE-CMM 第一版于 1996 年 10 月出版，1999 年 4 月。SSE-CMM 模型和相应评估方法 2.0 版发布。2001 年，美国将 SSE-CMM 2.0 提交给 ISO JTC1 SC27 年会，申请作为国际标准，即《ISO/IEC DIS 21827 信息技术－系统安全工程－能力成熟度模型》。

SSE-CMM 描述了一个组织的系统安全工程过程必须包含的基本特性，这些特性是完善安全工程的保证，也是系统安全工程实施的度量标准，同时还是一个易于理解的评估系统安全工程实施的框架。

SSE-CMM 将系统安全工程成熟度划分为 5 个等级，如图 6 所示。

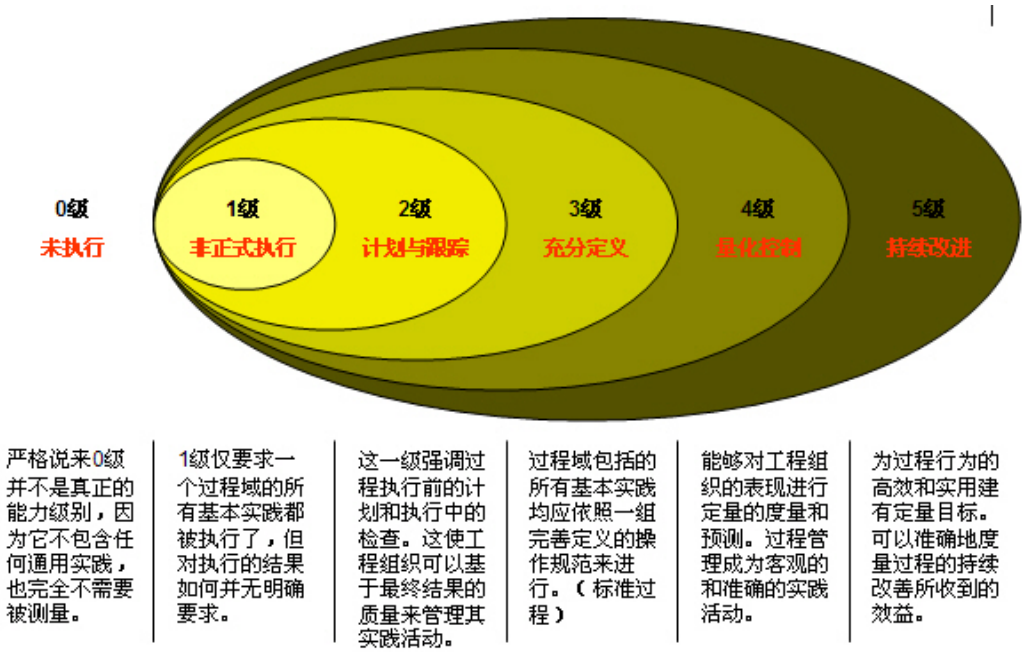

图 6.　SSE-CMM 系统安全工程能力等级

SSE-CMM、CC、BS7799 在很多文中经常会同时出现，但其间的区别还是很明显的。

SSE-CMM 和 CC 都是评估标准，都可以将评估对象划分为不同的等级，但 CC 针对的

是安全系统或安全产品的测评，而 SSE-CMM 针对的是安全工程过程。

SSE-CMM 和 BS 7799 都提出了一系列最佳惯例，二者之间也有映射关系，但不同之处在于：BS 7799 是一个认证标准（第二部分），提出了一个可供认证的 ISMS 体系，组织应该将其作为目标，通过选择适当的控制措施（第一部分）去实现，但具体如何实现，需要哪些过程，BS 7799 都没有规定。SSE-CMM 是一个评估标准，它定义了实现最终安全目标所需要的一系列过程，并对组织执行这些过程的能力进行等级划分。因此，二者可以互补使用。

实际上，SSE-CMM 更适合作为评估工程实施组织（例如安全服务提供商）能力与资质的标准，对用户组织来说，则是选择服务提供商的一个参照。我国国家信息安全测评认证中心在审核专业机构信息安全服务资质时，基本上就是依据 SSE-CMM 来审核并划分等级的。

2.6.7 NIST SP 800 系列

美国国家标准技术协会（National Institute of Standards and Technology，NIST）发布的 Special Publication 800 文档是一系列针对信息安全技术和管理领域的实践参考指南，其中有多篇是有关信息安全管理的，包括：

- SP 800-12：计算机安全介绍（An Introduction to Computer Security: The NIST Handbook）
- SP 800-30：IT 系统风险管理指南（Risk Management Guide for Information Technology Systems）
- SP 800-34：IT 系统应急计划指南（Contingency Planning Guide for Information Technology Systems）
- SP 800-26：IT 系统安全自我评估指南（Security Self-Assessment Guide for Information Technology Systems）

这些文件可以作为实施 ISMS 过程中一些关键任务的指导和参照（例如风险评估、应急计划等），是对 BS7799 标准很好的补充和细化。

2.6.8 ITIL

信息技术基础设施库（IT infrastructure Library），是由英国中央计算机与电信局（CCTA）发布的关于 IT 服务管理最佳实践的建议和指导方针，旨在解决 IT 服务质量不佳的情况。此后，CCTA 又在 HP、IBM、BMC、CA、Peregrine 等主流 IT 资源管理软件厂商近年来所做出的一系列实践和探索的基础之上，总结了 IT 服务的最佳实践经验，形成了一系列基于流程的方法（充分地体现在 40 多本出版物中），用以规范 IT 服务的水平。后来 CCTA 并入英国政府商务部（OGC），目前 ITIL 的版权、发行都属于 OGC 所有。

作为一种基于流程的管理方法，ITIL特别适用于企业的IT部门，有助于其以一种可控和训练有素的方式向终端用户提供IT服务。

ITIL 的精髓都体现在了其“十大流程”和“一大功能”上了。一大功能即服务台（Service Desk），十大流程包括：

- 服务支持（Service Support）：
  - 事件管理（Incident Management）
  - 问题管理（Problem Management）
  - 变更管理（Change Management）
  - 发布管理（Release Management）
  - 配置管理（Configuration Management）

- 服务交付（Service Delivery）：
  - 服务水平管理（Service Level Management）
  - 可用性管理（Availability Management）
  - IT 服务财务管理（Financial Management for IT Services）
  - 容量管理（Capacity Management）
  - IT 服务持续性管理（IT Service Continuity Management）

与 BS7799 相比，ITIL 关注面更为广泛（信息技术），而且更侧重于具体的实施流程。不过，尽管 IT 领域包含信息安全的议题，但 ITIL 对此没有专门论及，从这一点来看，ISMS 实施者可以将 BS7799 作为 ITIL 在信息安全方面的补充，同时引入 ITIL 流程的方法，以此加强信息安全管理的实施能力。

2001 年，英国标准协会在国际 IT 服务管理论坛（itSMF）上正式发布了以 ITIL 为核心的英国国家标准 BS15000。这成为 IT 服务管理领域具有历史意义的重大事件。

BS15000 有两个部分，目前都已经转化成国际标准了。

- ISO/IEC 20000-1:2005 信息技术服务管理-服务管理规范（Information technology service management. Specification for Service Management）
- ISO/IEC 20000-2:2005 信息技术服务管理-服务管理最佳实践（Information technology service management. Code of Practice for Service Management）

2.6.9 CobiT

信息及相关技术控制目标（Control Objectives for Information and related Technology，CobiT），是美国信息系统审计与控制协会（Information Systems Audit and Control Association）针对 IT 过程管理制定的一套基于最佳实践的控制目标，是目前国际上公认的最先进、最权威的安全与信息技术管理和控制标准。

CobiT 架构的主要目的是为业界提供关于 IT 控制的一个清晰的政策和发展的良好典范，这个架构包括 34 个 IT 过程，分成 4 个领域：PO（Planning & Organization）、AI（Acquisition & Implementation）、DS（Delivery and Support）、和 Monitoring，所有的过程中又包含了 318 个控制目标，全都提供了最佳的施行指导。

与 ITIL 一样，CobiT 关注的是广泛的 IT 控制，但更强调目标要求和度量指标，这和 ITIL 强调实施流程是有所不同的，而相比之下，BS7799 则要更有针对性一些。具体到 ISMS 建设上，CobiT 的框架和目标、ITIL 的流程都可以供 BS7799 实践者借鉴，而 BS7799 最终所追求的，则只是 CobiT 及 ITIL 框架下一个分支而已。

2.7 BS7799 新版本（2005）与老版本有什么异同？

我们知道，2005 年对信息安全的发展来说是非常重要的一年，这一年里，BS7799 标准的两个部分先后经过修订并被正式采纳成为目前的 ISO/IEC 17799:2005 和 ISO/IEC 27001:2005，这两个标准脱胎于先前的 ISO/IEC 17799:2000 以及 BS7799-2:2002，自然是继承和发扬了原标准的“优良传统”的，但之所以能够让世人瞩目和期待，则是因为新标准在全面性、可操作性和更广泛的认同方面有了长足进步。

我们先来看 ISO 17799:2005，相比前一版本，新标准无论在结构上还是内容上都有了很大变化。从表 4 中我们就能大致看出这种区别来。

表 4　　ISO/IEC 17799 新老版本内容比较

ISO/IEC 17799:2000	ISO/IEC 17799:2005
Security policy	Security policy
Security organisation	Organizing information security
Asset classification & control	Asset management
Personnel security	Human resources security
Physical and environmental security	Physical and environmental security
Communications and operations management	Communications and operations management
Access control	Access control
Systems development and maintenance	Information systems acquisition, development and maintenance
	Information security incident management
Business continuity management	Business continuity management
Compliance	Compliance

从内容上来看，ISO 17799 从原来的（2000 版）10 个方面、36 个控制目标和 127 项控制转变成现在的（2005 版）11 个方面、39 个控制目标和 133 项控制。这种变化体现在以下三个方面：

- 新增加了 17 项控制，在客户往来安全、资产属主定义、人员离职管理、第三方服务交付管理、漏洞管理、取证等方面对原标准做了全新阐释或补充。
- 去掉了原标准中的 9 项控制，这些控制或者是不再适应信息通信技术的发展，或者是已经并入到新标准的其他控制内容中了。
- 对原标准中的多项控制进行了重新编排，这部分改动也是比较大的。

除了内容上的变化，新标准在对各项控制的阐述上也有结构性的变化。老版本的标准对控制措施的阐述是“平铺直叙”的，没有结构和层次之分，而新版本做了更清晰的界定，每一项控制都从以下三个方面进行阐述：

- **控制（Control）**：对满足控制目标的控制措施进行说明。
- **实施指南（Implementation guidance）**：为了实施该控制，应该采取哪些行动。有些活动可能并不适用于所有情况，可能需要补充其他活动。这部分的指南有助于组织实现有效的安全。
- **其他信息（Other information）**：作为补充选项，这部分对控制的实施进行相关说明，包括实施控制时应该考虑的各种因素（例如法律）。

接下来再看 ISO 27001，虽然说是一个全新的 ISO 标准，但 ISO 27001:2005 更像是直接从 BS 7799-2:2002 直接移植过来的，当然，为了保证标准附录部分对 ISO17799 各项控制目标及控制的一致性，ISO 27001:2005 做了相应扩充和调整，保证其对应于 ISO 17799:2005。

相比 BS 7799-2:2002，ISO 27001:2005 的变化主要是两个方面：

- 将原标准的条款 6（管理评审）分割成新标准的条款 6（内审）和条款 7（管理评审）两个部分，即原来的条款 6.4 变成新标准的条款 6，原标准的条款 6.1～6.3 变成新标准的 7.1～7.3。
- 附录 A 引向 ISO 17799:2005，即原标准的 A.3～A.12 变成新标准的 A.5～A.15。

2.8 ISO17799:2005 主要内容是怎样的？

ISO 17799:2005，即信息安全管理实施细则（Code of Practice for Information Security Management），从 11 个方面定义了 133 项控制措施，可供信息安全管理体系实施者参考使用，这 11 个方面是：

- 安全策略（Security policy）；
- 组织信息安全（Organizing information security）；
- 资产管理（Asset management）；
- 人力资源安全 （Human resources security）；
- 物理和环境安全（Physical and environmental security）；
- 通信和操作管理（Communication and operation management）；
- 访问控制（Access control）；
- 信息系统获取、开发和维护（Information systems acquisition, development and maintenance）；
- 信息安全事件管理（Information security incident management）；
- 业务连续性管理（Business continuity management）；
- 符合性（Compliance）。

这其中，除了访问控制、信息系统获取开发和维护、通信和操作管理这几个方面跟技术关系更紧密之外，其他方面更侧重于组织整体的管理和运营操作，信息安全所谓“三分靠技术、七分靠管理”在这里得到了比较好的体现。

表 5 列举了 ISO 17799:2005 对信息安全管理 11 个方面的内容阐述（各条目前面的编号代表其在标准文件中的章节号）。

表 5　　信息安全控制目标及控制

领域	控制目标	控制措施
5. 安全策略	5.1 信息安全策略 为信息安全提供与业务需求和法律法规相一致的管理指示及支持。	5.1.1 信息安全策略文件 5.1.2 信息安全策略复查
6. 组织信息安全	6.1 内部组织 在组织内建立发起和控制信息安全实施的管理框架。	6.1.1 管理层对信息安全的责任 6.1.2 信息安全协调机制 6.1.3 分派信息安全责任 6.1.4 信息处理设施的批准程序 6.1.5 保密协议 6.1.6 保持和权威机构的联系 6.1.7 保持和专业团队联系 6.1.8 对信息安全做独立评审
	6.2 外部伙伴 维护被外部伙伴访问、处理和管理的组织的信息处理设施和信息资产的安全。	6.2.1 识别与外部伙伴相关的风险 6.2.2 和客户交往时注意安全 6.2.3 在第三方协议中注明安全

7. 资产管理	7.1 资产责任 保持对组织资产的恰当的保护。所有资产都应该责任到人。	7.1.1 资产清单 7.1.2 资产属主 7.1.3 对资产的可接受使用
	7.2 信息分类 确保信息资产得到适当级别的保护。	7.2.1 分类指南 7.2.2 信息标注与处理
8. 人力资源安全	8.1 聘用前的控制 确保雇员、合同工和第三方用户理解其自身责任，适合角色定位，减少偷窃、欺诈或误用设施带来的风险。	8.1.1 角色和责任 8.1.2 人员筛选（Screening） 8.1.3 聘用条件和条款
	8.2 聘用期间 确保所有雇员、合同工和第三方用户都意识到信息安全威胁、利害关系、责任和义务，并在其正常工作当中支持组织的安全策略，减少人为错误导致的风险。	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 惩罚机制
	8.3 解聘和职位变更 确保雇员、合同工和第三方用户按照既定方式离职或变更职位。	8.3.1 解聘责任 8.3.2 返还资产 8.3.3 去除访问权限
9. 物理与环境安全	9.1 安全区域 防止非授权物理访问、破坏和干扰组织的安全区边界。	9.1.1 物理安全边界 9.1.2 物理入口控制 9.1.3 保护办公场所、房间和设施 9.1.4 防止外部和环境威胁 9.1.5 在安全区内工作 9.1.6 公共访问和交接区域
	9.2 设备安全 防止资产的丢失、损害和破坏，防止业务活动被中断。	9.2.1 设备的安置与保护 9.2.2 供电 9.2.3 电缆安全 9.2.4 设备维护 9.2.5 场外设备的安全 9.2.6 设备报废或重用时的安全 9.2.7 财物迁移
10. 通信与操作管理	10.1 操作程序和责任 确保正确并安全地操作信息处理设施。	10.1.1 操作程序的文档化 10.1.2 变更管理 10.1.3 职责分离 10.1.5 开发、测试和运营设施的分离
	10.2 第三方服务交付管理 根据第三方服务交付协议，实施并保持恰当的信息安全和服务交付水平。	10.2.1 服务交付 10.2.2 监督和复查第三方服务

		10.2.3　第三方服务变更管理
	10.3 系统规划及验收 减少系统故障带来的风险。	10.3.1　容量管理 10.3.2　系统验收
	10.4 抵御恶意和移动代码 保护软件和信息的完整性。	10.4.1　恶意代码控制 10.4.2　移动代码控制
	10.5 备份 维护信息和信息处理设施的完整性及可用性。	10.5.1　信息备份
	10.6 网络安全管理 确保网络中的信息以及支持技术设施得到保护。	10.6.1　网络控制 10.6.2　网络服务的安全
	10.7 介质处理 防止非授权泄漏、篡改、废除和破坏资产，防止业务活动中断。	10.7.1　移动计算机介质的管理 10.7.2　介质的处置 10.7.3　信息处理程序 10.7.4　系统文件的安全
	10.8 信息的交换 保持组织内部和与外部实体间进行信息交换的安全性。	10.8.1　信息交换策略和程序 10.8.2　交换协议 10.8.3　传输中的物理介质 10.8.4　电子信息交换 10.8.5　业务信息系统
	10.9 电子商务服务 确保电子商务服务的安全性，保证安全使用电子商务服务。	10.9.1　电子商务 10.9.2　在线交易 10.9.3　公共可用信息
	10.10 监视 发现非授权活动。	10.10.1　审计日志 10.10.2　监视系统使用 10.10.3　保护日志信息 10.10.4　管理员和操作日志 10.10.5　故障日志 10.10.6　时钟同步
11 访问控制	11.1 访问控制的业务需求 控制对信息的访问。应该根据业务和安全需求对信息、系统和业务流程加以控制，还应该考虑信息传播和授权的策略。	11.1　访问控制策略
	11.2 用户访问管理 确保授权用户的访问，防止非授权访问信息系统。	11.2.1　用户注册 11.2.2　特权管理 11.2.3　用户口令管理

		11.2.4 用户访问权限的复审
	11.3 用户责任 防止非授权用户访问、破坏、窃取信息及信息处理设施。	11.3.1 口令使用 11.3.2 无人值守的用户设备 11.3.3 桌面清理和清屏策略
	11.4 网络访问控制 保护网络服务，防止非授权访问，对内部和外部的网络访问都应该得到控制。	11.4.1 网络服务使用策略 11.4.2 对外部连接用户进行身份认证 11.4.3 识别网络中的设备 11.4.4 远程诊断和配置端口的保护 11.4.5 网络隔离 11.4.6 网络连接控制 11.4.7 网络路由控制
	11.5 操作系统访问控制 防止对信息系统的非授权访问。	11.5.1 安全的登录程序 11.5.2 用户身份识别与认证 11.5.3 口令管理系统 11.5.4 系统工具的使用 11.5.5 会话超时 11.5.6 限制连接时间
	11.6 应用和信息访问控制 防止非授权访问信息系统中的信息。	11.6.1 信息访问限制 11.6.2 敏感系统的隔离
	11.7 移动计算和通信 确保使用移动计算和通讯设施时的信息安全。	11.7.1 移动计算和通信 11.7.2 远程工作
12. 信息系统获取、开发与维护	12.1 信息系统的安全需求 确保安全内建于信息系统中。	12.1.1 安全需求分析与规范
	12.2 应用程序中正确的处理 防止应用程序中的信息出错、丢失、被非授权篡改或误用。	12.2.1 输入数据的验证 12.2.2 内部处理控制 12.2.3 消息认证 12.2.4 输出数据的验证
	12.3 密码控制 通过加密手段，保护信息的保密性、真实性或完整性。	12.3.1 密码控制使用策略 12.3.2 密钥管理
	12.4 系统文件的安全 控制对系统文件和程序源代码的访问，使 IT 项目及其支持活动安全进行，确保系统文件的安全性。	12.4.1 控制运营系统上的软件 12.4.2 保护系统测试数据 12.4.3 对源代码的访问控制
	12.5 开发和支持过程的安全 维护应用系统软件和信息的安全。应该严格控制	12.5.1 变更控制程序 12.5.2 运营系统变更后对应用做技

	项目和支持环境。	术评审 12.5.3 限制对软件包的变更 12.5.4 信息泄漏 12.5.5 外包的软件开发
	12.6 技术漏洞管理 **防止因为利用已发布漏洞而实施的破坏。**	12.6.1 控制技术漏洞
13. 信息安全事件管理	13.1 报告信息安全事件和缺陷 **确保与信息系统相关的信息安全事件和缺陷能够及时发现，以便采取纠正措施。**	13.1.1 报告信息安全事件 13.1.2 报告安全缺陷
	13.2 管理信息安全事件和改进 **确保采取一致和有效的方法来管理信息安全事件。**	13.2.1 责任和程序 13.2.2 从信息安全事件中吸取教训 13.2.3 证据搜集
14. 业务连续性管理	14.1 业务连续性管理的信息安全方面 **减少业务活动的中断，保护关键业务过程不受重大事故或灾害的影响，确保其及时恢复。**	14.1.1 在业务连续性管理过程中考虑信息安全 14.1.2 业务连续性和风险评估 14.1.3 开发和实施包含信息安全的连续性计划 14.1.4 业务连续性计划框架 14.1.5 测试、维护和再评估业务连续性计划
15. 符合性	15.1 符合法律要求 避免违反任何法律、条令、法规或者合同义务，以及任何安全要求。	15.1.1 识别适用的法律 15.1.2 知识产权（IPR） 15.1.3 保护组织记录 15.1.4 数据保护和个人信息的隐私 15.1.5 防止对信息处理设施的滥用 15.1.6 加密控制的规定
	15.2 符合安全策略和标准 **确保遵守组织的安全策略和标准。**	15.2.1 符合安全策略 15.2.2 技术符合性检查
	15.3 信息系统审计的考虑 **发挥系统审计过程的最大效用，并把干扰降到最低。**	15.3.1 信息系统审计控制 15.3.2 保护信息系统审计工具

在标准列举的 133 个控制项中，很多还包含一些更具体的子控制项，虽然新的 ISO 17799:2005 对每项控制都提供了实施指南，但从实施角度来看，还不够具体和细致。此外，标准也特别声明，并不是所有的控制都适合任何组织，组织可以根据自己的实际情况来选择。当然，133 项控制也不一定能包含全部，组织可以根据自身需要来增加额外的控制。

在 ISO 17799:2005 开篇处提到了所谓的信息安全最佳起点，列举了一共 10 项适用于几

乎所有组织和大多数环境的控制措施，这些控制措施或者是和法律要求相关的，或者是信息安全方面最惯用的实践。对于还没有在信息安全方面有任何举措的组织来说，选择这些控制去实施自然是没错的。不过，虽然说是最佳起点，但并非说只有这些就足够了，从建立完整的信息安全管理体系来看，组织通常面临的信息安全问题和需求，远不止 10 项控制就能覆盖和解决，组织必须还得从实际出发，通过业务分析、法律探询、风险评估来全面洞察自身需求，继而进行有效的风险处理。

以下列出这 10 项控制（后面括号内是该控制所在的目录编号）：

- 与法律相关的控制措施：
  - **知识产权（Intellectual Property Rights）**：遵守知识产权保护和软件产品保护的法律（15.1.2）
  - **保护组织的记录**：保护重要的记录不丢失、破坏和伪造（15.1.3）
  - **数据保护和个人信息隐私**：遵守所在国的数据保护法律（15.1.4）
- 与最佳实践相关的控制措施：
  - **信息安全策略文件**：高管批准发布信息安全策略文件，并广泛告知（5.1.1）
  - **信息安全责任的分配**：清晰地定义所有的信息安全责任（6.1.3）
  - **信息安全意识、教育和培训**：全员员工及相关人员应该接受恰当的意识培训（8.2.2）
  - **正确处理应用程序**：防止应用程序中的信息出错、损坏或被非授权篡改及误用（12.2）
  - **漏洞管理**：防止利用已发布的漏洞信息来实施破坏（12.6）
  - **管理信息安全事件和改进**：确保采取一致和有效的方法来管理信息安全事件（13.2）
  - **业务连续性管理**：减少业务活动中断，保护关键业务过程不受重大事件或灾难影响（14）

2.9 ISO27001:2005 主要内容是怎样的？

ISO 27001:2005 是建立信息安全管理系统（ISMS）的一套需求规范（Information Security. Security techniques. Information security management systems. Requirements），其中详细说明了建立、实施和维护信息安全管理体系的要求，指出实施机构应该遵循的风险评估标准，当然，如果要得到最终的认证（对依据 ISO 27001:2005 建立的 ISMS 进行认证），还有一系列相应的注册认证过程。作为一套管理标准，ISO 27001:2005 指导相关人员怎样去应用 ISO 17799:2005，其最终目的，还在于建立适合组织需要的信息安全管理系统（ISMS）。

表 6 以标准原文目录格式，列举说明了 ISO 27001:2005 的主要内容。

表 6　　ISO 27001:2005 标准主要内容

一级目录	二级目录	内容简介
前言		发布者，目的，内容概要，其他说明。
0. 简介	0.1 概要	本标准对组织的价值所在。
	0.2 过程方法	对过程方法进行解释，引入 PDCA 模型。
	0.3 与其他管理体系的兼容	强调与 ISO9001 和 ISO14001 的一致性。
1. 范围	1.1 概要	本标准规定了 ISMS 建设的要求及根据需要实施

		安全控制的要求。
	1.2 应用	本标准适用于所有的组织。控制选择与否应根据风险评估和适用法规需求。
2. 标准引用		引用 ISO9001、ISO17799 和 ISO Guide 73:2002
3. 术语和定义		资产，CIA，信息安全，信息安全事件，ISMS，风险评估与管理，SOA 等。
4. 信息安全管理体系	4.1 一般要求	在组织全面的业务活动和风险环境中，应该开发、实施、维护并持续改进一个文档化的 ISMS。
	4.2 建立并管理 ISMS	4.2.1 建立 ISMS（Plan） • 定义 ISMS 的范围 • 定义 ISMS 策略 • 定义系统的风险评估途径 • 识别风险 • 评估风险 • 识别并评价风险处理措施 • 选择用于风险处理的控制目标和控制 • 准备适用性声明（SoA） • 取得管理层对残留风险的承认，并授权实施和操作 ISMS 4.2.2 实施和操作 ISMS（Do） • 制定风险处理计划 • 实施风险处理计划 • 实施所选的控制措施以满足控制目标 • 实施培训和意识程序 • 管理操作 • 管理资源（参见 5.2） • 实施能够激发安全事件检测和响应的程序和控制 4.2.3 监视和复查 ISMS（Check） • 执行监视程序和控制 • 对 ISMS 的效力进行定期复审 • 复审残留风险和可接受风险的水平 • 按照预定计划进行内部 ISMS 审计 • 定期对 ISMS 进行管理复审 • 记录活动和事件可能对 ISMS 的效力或执行力度造成影响 4.2.4 维护并改进 ISMS（Act） • 对 ISMS 实施可识别的改进 • 采取恰当的纠正和预防措施 • 与所有利益伙伴沟通 • 确保改进成果满足其预期目标
	4.3 文件要求	4.3.1 概要 － 说明 ISMS 应该包含的文件。

		4.3.2 对文件的控制 － ISMS 所要求的文件应该妥善保护和控制。 4.3.3 对记录的控制 －应该建立并维护记录。
5. 管理层责任	5.1 管理层责任	说明管理层在 ISMS 建设过程中应该承担的责任。
	5.2 对资源的管理	5.2.1 资源提供 －组织应该确定并提供 ISMS 相关所有活动必要的资源 5.2.2 培训、意识和能力 －通过培训，组织应该确保所有在 ISMS 中承担责任的人能够胜任其职
6. ISMS 内部审计		组织应该通过定期的内部审计来确定 ISMS 的控制目标、控制、过程和程序满足相关要求。
7. ISMS 管理评审	7.1 概要	管理层应该对组织的 ISMS 定期进行评审，确保其持续适宜、充分和有效。
	7.2 评审输入	评审时需要的输入资料，包括内审结果。
	7.3 评审输出	评审成果，应该包含任何决策及相关行动。
8. ISMS 改进	8.1 持续改进	组织应该借助信息安全策略、安全目标、审计结果、受监视的事件分析、纠正性和预防性措施、管理复审来持续改进 ISMS 的效力。
	8.2 纠正措施	组织应该采取措施，消除并实施和操作 ISMS 相关的不一致因素，避免其再次出现。
	8.3 预防措施	为了防止将来出现不一致，应该确定防护措施。所采取的预防措施应与潜在问题的影响相适宜。
附录 A 控制目标和控制	A.5 安全策略 A.6 组织信息安全 A.7 资产管理 A.8 人力资源管理 A.9 物理和环境安全 A.10 通信和操作管理 A.11 访问控制 A.12 信息系统获取、开发和维护 A.13 信息安全事件管理 A.14 业务连续性管理 A.15 符合性	以列表（表 A.1）方式展示：A.5 到 A.15 所列的控制目标和控制，是直接从 ISO/IEC 17799:2005 正文 5 到 15 那里引用过来的。此处列举的控制目标和控制，应该被 4.2.1 规定的 ISMS 过程所选择。
附录 B OECD 准则和本标准		OECD 在信息系统和网络安全方面的指导原则，在依据 PDCA 模型建立 ISMS 的本标准中有对应。表 B.1 给出了这种对应关系。
附录 C ISO 9001:2000，ISO 14001:1996 和本标准之		以列表方式（表 C.1）展示 ISO27001:2005 与 ISO9001:2000、ISO14001:1996 目录（内容）的一致性。

BS7799 标准之所以能被广为接受，一方面是它提供了一套普遍适用且行之有效的全面的安全控制措施，而更重要的，还在于它提出了建立信息安全管理体系的目标，这和人们对信息安全管理认识的加强是相适应的。与以往技术为主的安全体系不同，ISO 27001:2005 提出的信息安全管理体系（ISMS）是一个系统化、程序化和文档化的管理体系，这其中，技术措施只是作为依据安全需求有选择有侧重地实现安全目标的手段而已。

ISO 27001:2005 标准指出 ISMS 应该包含这些内容：用于组织信息资产风险管理、确保组织信息安全的、包括为制定、实施、评审和维护信息安全策略所需的组织机构、目标、职责、程序、过程和资源。

ISO 27001:2005 标准要求的建立 ISMS 框架的过程：制定信息安全策略，确定体系范围，明确管理职责，通过风险评估确定控制目标和控制方式。体系一旦建立，组织应该实施、维护和持续改进 ISMS，保持体系的有效性。

ISO 27001:2005 非常强调信息安全管理过程中文件化的工作，ISMS 的文件体系应该包括安全策略、适用性声明文件（选择与未选择的控制目标和控制措施）、实施安全控制所需的程序文件、ISMS 管理和操作程序，以及组织围绕 ISMS 开展的所有活动的证明材料。

作为刚刚颁布的国际标准，ISO 27001:2005 势必在未来几年里在信息安全领域掀起一股热潮，并且对全球范围内的各类组织和企业在信息化发展方面带来深远的影响。

3. 认证篇

3.1 什么是 ISO27001 认证？

所谓认证，即由认证机构依据特定的审核准则，按照规定的程序和方法对受审核方实施审核，以确定特定事项的符合性的活动。

针对 ISO27001 的受认可的认证，是对组织信息安全管理体系（ISMS）符合 ISO27001 要求的一种认证。这是一种通过权威的第三方审核之后提供的保证：受认证的组织实施了信息安全管理体系，并且符合 ISO27001 标准的要求。通过认证的组织，将会被注册登记，并且与认证委员会、DTI 以及 ISMS IUG 的国际网络相联系。

需要注意的是，ISO 27001:2005 是 2005 年 10 月才正式颁布的，在此之前，相对应的是 BS7799-2:2002 认证，即组织建立符合 BS7799-2:2002 标准要求的信息安全管理体系继而得到了权威机构的审核，获得了相应的合格证明。

ISO 27001:2005 的颁布宣告BS 7799-2:2002 正式退出历史舞台，对于持有老版证书的组织，升级转版时限为 18 个月，也就是说，组织可以在 2007 年 4 月之前，选择在后续的跟踪审核时完成升级转版工作。从 2006 年 4 月起，认证机构将不再提供针对旧版标准的新认证，所有新的认证都将直接针对ISO 27001:2005。

3.2 为什么要接受 ISO27001 认证？

我们都知道，万事没有绝对，100％的安全是不现实也不可行的，对组织来说，符合 ISO27001 标准并且获得相应证书，其本身并不能证明组织达到了 100％的安全，除非停止所有的组织活动。但不管怎么说，作为一个全球公认的最权威的信息安全管理标准，ISO27001 能给组织带来的将是由里到外全面的价值提升，就像表 7 所列举的那样。

表 7　　ISO27001 认证价值所在

针对性	获益点	简单说明
法律法规	遵守适用法律	证书的获得，可以向权威机构表明，组织遵守了所有适用的法律法规。从一定角度讲，ISO27001 标准是对适用法律法规的补充和注解，因为 ISO27001 标准本身的制订，是参照了业界最通行的实践措施的，而这些实践措施，在很多国家相关的信息保护法规中都有体现（例如美国的 SOX 法案、HIPAA、个人隐私法、计算机安全法、GLBA、政府信息安全修正法案等）；另一方面，很多国家所推行的相关的行业指导性文件及要求，又可能是参照 ISO27001 而拟定的。因此，通过 ISO27001 认证，可以使组织更有效地履行国家法律和行业规范的要求。
外部期望	提升信誉，增强信心	当合作伙伴、股东和客户看到组织为保护信息而付出的努力时，其对组织的信心将得到加强。同样的，证书的获得，有助于确定组织在同行业内的竞争优势，提升其市场地位。事实上，现在很多国际

		性的投标项目已经开始要求 ISO17799 符合性了。
管理层	履行责任	证书的获得，本身就能证明组织在各个层面的安全保护上都付出了卓有成效的努力，表明管理层履行了相关责任。
员工	增强意识、责任感和相关技能	提升员工的安全意识，增强其责任感，减少人为原因造成的不必要的损失。
核心业务	保证持续运行	全面的信息安全管理体系的建立，意味着组织核心业务所赖以持续的各项信息资产得到了妥善保护，并且建立有效的业务持续性计划框架。
信息环境日常运作	实现风险管理	有助于更好地了解信息系统，并找到存在的问题以及保护的办法，保证组织自身的信息资产能够在一个合理而完整的框架下得到妥善保护，确保信息环境有序而稳定地运作。
财务状况	减少损失，降低成本	ISMS 的实施，本身也能降低因为潜在安全事件发生而给组织带来的损失，另外，也有可能减少保险金支出。

3.3 ISO27001 认证适合哪些对象？

ISO27001 中明确指出，标准中规定的要求是通用的，适用于所有的组织，无论其类型、规模和业务性质怎样。

如果由于组织及其业务性质而导致标准中有不适用之处，可以考虑对要求进行删减，但是务必要保证，这种删减不影响组织为满足由风险评估和适用的法律所确定的安全需求而提供信息安全的能力和责任，否则就不能声称是符合 ISO27001 标准的。

ISO27001 可以作为评估组织满足客户、组织本身以及法律法规所确定的信息安全要求的能力的依据，无论是自我评估还是独立第三方认证。

就目前国内发展来看，最先确定实施 ISMS 并考虑接受 ISO27001 认证的组织，其驱动力都比较明显，这种驱动力可以是外部的，也可以是发自内部的。这些组织主要集中在以下几个行业：

- 半导体行业：尤其是主业为集成电路芯片制造的组织。由于国内最近几年 IC 产业发展迅猛，大量国外设计企业的制造订单都飞往国内一些大型的芯片制造企业，鉴于 IP（知识产权）保护的重要性，来自国外客户的明确要求，使得国内芯片制造企业必须在信息安全管理方面做出保证，ISO27001 证书就是最好的选择。
- 软件开发行业：情况与芯片制造企业类似，近年来，承担软件定制开发的很多企业，也面临外部客户明确提出的信息保护的要求，特别是承接日本、欧美等国外软件开发订单业务的大型软件企业。
- 金融业和保险业：一直以来，金融和保险行业对信息安全的重视都是非常高的，保护客户信息、保证业务运转的可靠性和持续性，这都是此行业组织实施 ISMS 并寻求认证的驱动力。加之金融和保险早些年已经陆续完成了信息基础设施的建设，今后的工作重点将逐渐向全面的信息安全管理方向发展。
- 通讯行业：特别是一些大型的通信设备提供商，由于牵涉到对自身核心技术的保护，对信息安全加以重视并全面实施信息安全管理体系就成了这些企业必然的选择。
- 其他行业：只要是牵涉到 IP 保护的、牵涉到行业规范和法律法规要求的、牵涉到自身发展需求的，组织都会逐渐在信息安全建设上加强力度，就拿美国

Sarbanes-Oxley 法案（萨班斯法案，简称 SOX 法案）来说，由于对在 SEC 注册的上市公司提出了内部控制审核的要求，相关组织必然会在信息安全方面投入关注，因为信息安全控制是企业内部控制必不可少的一个部分。

3.4 目前 ISO27001 认证的发展状况如何？

我们知道，所谓的 BS7799 认证目前特指的是 ISO27001:2005 认证（之前一直是 BS 7799-2:2005），而大家经常提到的 ISO17799 只是一个控制目标和控制的集合，其本身并不能作为认证的依据。所以，组织需要做的，就是符合 ISO17799 的控制要求，然后接受 ISO 27001:2005 认证。

当然，对一些组织来说，按照 ISO27001:2005 标准的要求来建设 ISMS 可能更重于获得 ISO27001 证书，这是一种务实的心态，事实上这也和长久以来标准在全球的发展状态有关。BS7799 标准从正式发布到现在的十年时间里，全球接受并且按照 BS7799（包括以前的 BS7799-2 和现在的 ISO27001）最佳实践来实施 ISMS 的组织达到了 10 万多家，其中很多都是国际上知名的企业，例如富士通、KPMG、Insight、三星电子、东芝、索尼、Symantec 等。不过，最终成功获得 BS7799/ISO27001 证书的机构至今刚刚超过 2000 家。

表 8 列举了截至 2006 年 2 月中旬，各个国家和地区通过 BS7799/ISO27001 认证的组织数量（数据来自 ISMS IUG，http://www.xisec.com）。

表 8　　获得 BS7799/ISO27001 证书的组织数量统计

国家/地区	数字	国家/地区	数字	国家/地区	数字	国家/地区	数字
日本	1271*	挪威	13	阿联酋	3	英国	225
捷克	6	土耳其	6	亚美尼亚	1	巴林群岛	1
斯洛伐克	2	智利	1	克罗地亚	4	黎巴嫩	1
菲律宾	4	立陶宛	1	卢森堡	1	马其顿	1
中国大陆	25	哥伦比亚	2	印度	151	奥地利	9
塞尔维亚	1	法国	2	泰国	1	沙特阿拉伯	4
科威特	3	新西兰	1	罗马尼亚	1	加拿大	2
埃及	1	德国	54	冰岛	4	俄罗斯	1
韩国	37	波兰	8	曼岛群岛	2	台湾	76
瑞典	7	澳门	2	意大利	42	瑞士	13
马来西亚	2	荷兰	27	巴西	5	摩洛哥	1
香港	20	希腊	5	卡塔尔	1	美国	32
墨西哥	3	斯络文尼亚	1	澳大利亚	18	阿根廷	3
南非	2	芬兰	15	比利时	2	新加坡	11
丹麦	2	匈牙利	24	西班牙	5	爱尔兰	11

合计：相对数字 **2195**，绝对数字 **2183**（*号代表相对数字中包含仅适用于日本的证书）

稍微分析一下就会看到，实际上这种反差（实施 BS7799 最佳实践的多，接受认证的少）很好理解。毕竟 BS7799 标准从颁布到现在的发展时间还不长，其成熟也有个过程，作为最佳实践集合的第一部分早已经被公众认可和接受，但作为认证准则的第二部分，由于旧版本在很多方面存在不足，被接受度就不是太高。不过，随着改版以及转换为真正的国际标准，新的 ISO27001 认证很快就会进入一个突飞猛进的发展阶段，这种发展趋势已经在近一年来表现非常明显了，如图 7（引自 http://www.gammassl.co.uk/）所示。

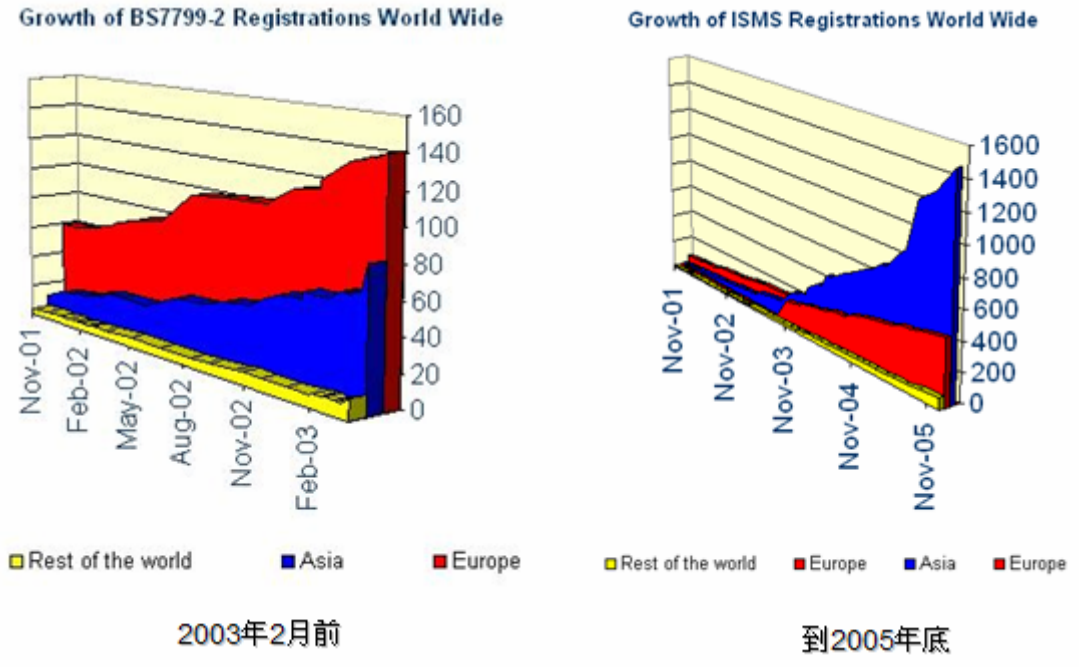

图 7.　BS7799 认证发展趋势对比

中国大陆地区目前已经通过 BS7799/ISO27001 认证的组织已经有近 30 家，很多都是最近一年多涌现出来的，统计数据如表 9 所列（数据来自 ISMS IUG）。（笔者注：此数据并不完全）。

表 9　　中国大陆通过 BS7799/ISO27001 认证的机构统计

企业名称	证书编号	认证机构
上海先进半导体制造有限公司 Advanced Semiconductor Manufacturing Corporation Limited	07513-2004-AI-ROT-UK AS	DNV
Beijing Core Software Co.,Ltd	07633-2005-AIS-LDN-U KAS	DNV
北京移动数据中心 Beijing Mobile Communication Co Ltd., Data Center 47190007	IS 87929	BSI
北京中海神鹰科技发展有限公司 Beijing Zhong Hai Shen Ying Technology Development Co Ltd	IS 82006	BSI
大连华信计算机技术有限公司 Dalian Hi-Think Computer Technology Co.,Ltd	07627-2005-AIS-LDN-U KAS	DNV
广东生益科技股份有限公司 Guangdong Shengyi Sci. Tech. Co., Ltd	02063-2002-AIS-LDN-U KAS	DNV

山东黄岛发电厂 Huangdao Power Plant of Shandong	02020-2001-AIS-LDN-UKAS	DNV
华为技术有限公司 Huawei Technologies Co., Ltd.	07507-2004-AI-ROT-UKAS	DNV
益德穿梭科技（大连）有限公司 Infodeliver Technology Service (Dalian) Co., Ltd	IS 99776	BSI
金德精密五金有限公司 Kingdom Fine Metal Limited	IS 72876	BSI
中国人民财产保险股份有限公司厦门分公司 PICC, Xiamen Branch	07502-2004-AIS-LDN-UKAS	DNV
深圳平安保险信息管理中心 Ping An Insurance (Group) Company of China, Ltd. Information Management Centre	07642-2005-AIS-LDN-UKAS	DNV
清溢精密光电（深圳）有限公司 Supermask Co Ltd	IS 77644	BSI
理光（深圳）工业发展有限公司 Ricoh Asia Industry (Shenzhen) Ltd	IS 85241	BSI
中芯国际集成电路制造有限公司 Semiconductor Manufacturing International (Shanghai) Corporation	IS 96866	BSI
上海超级计算中心 Shanghai Computer Center	IS 97482	BSI
上海华虹 NEC 电子有限公司 Shanghai Hua Hong NEC Electronics Company Limited	IS 84261	BSI
上海理光传真机有限公司 SHANGHAI RICOH FACSIMILE CO., LTD	IS 85241	BSI
天嘉信电脑科技（深圳）有限公司 Tech Aggression Limited	IS 84120	BSI

由于亚洲正日益成为全球最大的经济增长热点，国际间交流的急剧增多，势必提升对信息安全保护的要求，所以我们看到，从 2004 下半年开始，亚洲地区，特别是印度、香港、中国大陆、台湾、日本、新加坡等经济发展独具特色的国家和地区，寻求通过 BS7799 认证的企业正日益增多，并且正呈现急剧增长的态势。。

3.5 可提供 ISO27001 认证的机构有哪些？

ISMS 认证是由一个受认可的 BS7799/ISO27001 认证团体（Certification Body，CB）来负责的。作为独立第三方，认证团体可以评估和证实组织的 ISMS 是否与 BS7799-2/ISO27001 的要求相符合。认证团体应该具备特定的能力和资格，根据一定的认证程序而获得认可机构的认可之后才能专门从事认证业务。

目前全球具备 BS7799/ISO27001 认证资格的认证机构有数十家，如表 10 所列。

表 10　　BS7799/ISO27001 认证机构

BM TRADA Certification Limited	National Quality Assurance
BSI	Nemko (Norway)

BVQI (Bureau Veritas Quality International)	PSB Certification (Singapore)
Certification Europe	RINA S.p.A. (Italy)
CIS (Austria)	SAI Global Limited (Australia)
DNV (Det Norske Veritas)	SFS Certification (Finland)
DQS GmbH (Germany)	SGS ICS Limited
JACO-IS (Japanese Audit and Certification Organisation)	SQS (Swiss Quality System)
JQA (Japanese Quality Assurance)	STQC Certification Services (India)
KEMA (Netherlands)	Teknologisk institutt Sertifisering AS (Norway)
KPMG Audit plc	TÜV Rheinland Group (Germany)
KPMG SA	UIMCert (Germany)
LRQA	United Registrar of Systems Limited

许多认证团体在全球各地都有自己的分之机构，可以为各个国家和地区的客户提供认证服务。在中国大陆，目前能够提供 BS7799/ISO27001 认证服务的，主要是 BSI（英国标准化协会）和 DNV（挪威船级社），另外，TÜV（德国莱茵 TÜV 集团）、SGS（瑞士通用公证行）和 BVQI（法国船级社）等老牌的认证机构也都开始着手开展该项业务了。随着 BS7799/ISO27001 国标化转换进程的加快，相信不久之后，国内认证机构也都能够承担相应的认证工作。

3.6 什么是认可机制？

认证（Certification）和认可（Accreditation）是两个紧密相关的概念，但也有明显的区别。

认证是第三方依据程序对产品、过程、服务符合规定要求给予的书面保证（合格证书），其基础是相关标准。根据对象的不同，认证通常分为产品认证和体系认证。通过认证，组织可以对外提供某种信任和保证。

认可是由某权威机构依据程序对某团体（例如对认证机构的认可）或个人（例如对审核员资格的认可）具有从事特定任务的能力给予的正式承认。

就 ISO27001 来说，受认可的认证机构（accreditated certification/registration body）负责评估并认证组织的 ISMS 是否符合 ISO27001 的要求。认证机构要通过认可，则必须向认可机构表明其完全满足相关的国家和国际标准的要求，包括 EN 45012（1998）、ISO/IEC Guide 62（1996）、EA 7/03 认可指南以及其他认可机构要求的补充文件。EN 45012 和 ISO/IEC Guide 62 都是对从事质量体系评估及认证任务的团体的一般性要求，区别只在于前者是欧洲标准，后者是国际标准。EA 7/03（EA Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems）是一个规定了对实施 ISMS 评估及认证的机构的一般性要求的文件，其内容主要源自前两个文件。

认可机构都是具有国家授权从事资格认可的权威机构，遵循权威的国家认可制度，英国 UKAS、荷兰 RvA、瑞典 Swedac 都是比较著名的认可机构。此外，为了增强国际贸易伙伴之间的互信，避免充分认证，国际认可领域相继成立国际互认组织以推动国际间的认证互认工作，影响较大的有 IAF（国际认可论坛）、PAC（太平洋认可合作组织）、IATCA（国际审核员培训与注册协会）等。

3.7 ISO27001 认证体系中对审核员有什么要求？

在 BS7799/ISO27001 认证体系中，除了对认证机构有被权威机构认可的要求之外，对具体承担审核任务的审核员也有资质的要求，这就是 IRCA 提出的 ISMS 审核员认证方案。

国际审核员注册协会（International Register for Certified Auditors，IRCA）是世界上管理体系审核员注册的创始机构，也是最大的国际化管理体系审核员注册机构，目前已经在世界 120 多个国家和地区注册了 2 万多名审核员。

IRCA 的服务主要涉及两个领域，一个是管理体系审核员注册。针对 ISMS 审核员，IRCA 设定了四个级别：

- ISMS 实习审核员（ISMS Provisional Auditor）：适用于所有希望成为专职审核员或希望暂时停止审核活动或从审核岗位转向管理岗位的原注册审核员。
- ISMS 审核员（ISMS Auditor）：适用于审核组成员。
- ISMS 主任审核员（ISMS Lead Auditor）：适用于审核组长，特别是那些就职于认证机构或为大型企业实施供方审核的人员。
- ISMS 首席审核员（ISMS Principal Auditor）：适用于（以独立成组的形式）单独实施审核活动的、有经验的审核员。

申请者可以直接申请任何级别的审核员资格，但必须接受 IRCA 的严格审查。IRCA 会考察申请者在 ISMS 审核方面的知识、技能和实际经验，所依据的评估标准直接规定了申请者所需具备的教育、工作经验、审核员培训经历及审核经验。

IRCA 的另一个服务领域是批准培训机构及其审核员培训课程。目前，IRCA 已经批准了 90 多个培训机构，这些机构每年在世界 100 多个国家提供超过 50000 个培训课程。国内人士比较熟知的 BSI、DNV、KPMG 等都是 IRCA 授权的培训机构，他们会不定期地在国内举办各类与 BS7799/ISO27001 相关的审核员课程，包括基础知识、内审员、主任审核员等。当然，接受这些培训机构的培训并取得相应成果，只表明培训人员满足了申请 IRCA 注册审核员的一定条件，要想真正成为 IRCA 认证的审核员，还要按照正式的程序向 IRCA 提出申请。

3.8 ISO27001 认证的实施过程是怎样的？

ISO27001 规定了很多与建立、实施、维护和改进 ISMS 相关的要求，组织是否符合这些要求，要在认证审核过程中予以验证。

组织在建立并实施 ISMS 之后应该运行一段时间，确保体系功能正常、用户得到有效培训、文件和记录系统运转正确，一旦 ISMS 根据设计规范运转达到了令组织满意的状态，就可以联系一家被认可的认证机构，准备相关资料，提出认证申请。

ISO27001 认证审核的过程大致分两个阶段，即文件审核阶段和现场审核阶段，当然，有时候为了稳妥其间，组织可以选择在正式审核之前进行一次预审核。整个审核流程如图 8 所示。

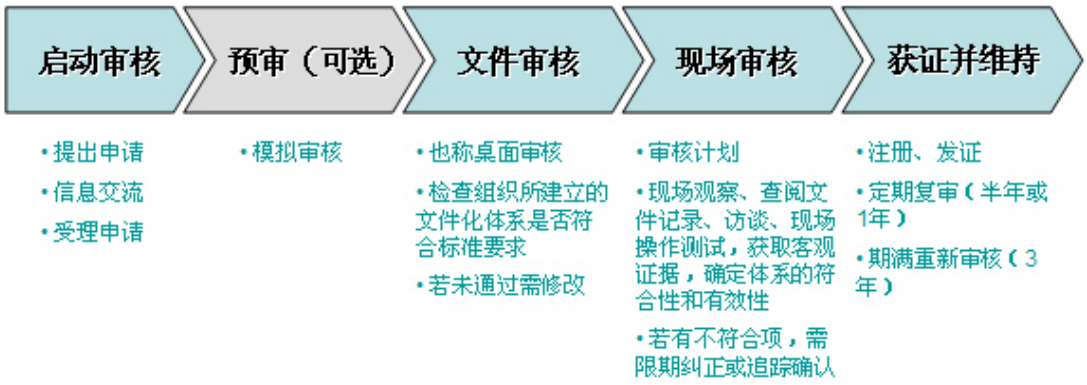

图 8.　ISO27001 认证审核过程

3.9 ISO27001 认证审核费用和周期如何？

除了组织自身投入之外，ISO27001 认证审核费用主要体现在聘请第三方认证机构及审核员方面了。在组织向认证机构提出申请之后，认证机构会初步了解组织现状，确定审核范围，提出审核报价。认证机构的报价通常是根据其投入的时间和人员来确定的，决定因素包括：

- 受审核组织的员工数量；
- 纳入审核范围的信息量；
- 场所数量；
- 组织与外界的关联；
- 组织 IT 的复杂性；
- 组织类型和业务性质等。

就国内目前情况来看，无论是 DNV 还是 BSI，其认证审核的费用一般都会在 10 万人民币左右（中小规模的组织）。

除了费用问题，认证审核的周期通常也是组织比较关心的。一般来说，从组织启动 ISMS 建设项目开始，到最终通过审核，至少要有半年时间（不包括获取证书的时间）。对于很多因为外部驱动力而决心实施 ISO27001 认证项目的组织来说，提早进行规划是必要的。

3.10 为什么应该聘请顾问公司来协助认证？

BS7799 标准从十多年前开始因需而生，到近几年逐渐发展成熟并且被全球范围内广泛接受，直到去年真正成为国际标准，越来越多的组织在依照 BS7799 标准建设信息安全管理体系的进程中都表现出了浓厚的热情。企业要想在经济全球化发展的大环境下赢得信誉和信任，甚至抢得市场先机，势必要在关系到其核心竞争力和业务生存的信息系统保护方面加大力度，按照 BS7799 标准所提供的最佳实践来操作是再合适不过了。

不过，我们也要看到，尽管越来越多的企业在信息安全方面表现出了愈发迫切的需求，但限于自身经验、意识、技能的欠缺，往往在如何合理规划和有效实施方面陷入困境，毕竟信息安全建设是一项技术性很强而且尚处于探索阶段的全新课题，另一方面，BS7799 所要求建立的信息安全管理体系，较之纯粹的信息安全技术又更显得“务虚”和“高端”，是和组织整体的经营管理紧密相关的。面对这样全新而复杂的难题，传统行业内机构通常都会自

叹摸不找头脑，大有“门外汉”的感觉，即便是始终走在信息通信领域前沿的高技术性企业，也不见得在信息安全管理方面有足够的积累。

于是，越来越多的组织选择聘请专业的咨询顾问，协助企业建设信息安全管理体系并且通过 BS7799/ISO27001 认证，这不失为一条“捷径”。

那么，专业的咨询顾问，究竟能给企业带来什么价值呢？

首先，专业的信息安全咨询顾问可以帮助企业消除困惑和疑难，解决信息安全的实际问题，帮助企业建立信息安全管理体系并且成功通过认证。由于专业分工的限制和条件制约，企业不可能在各个方面都能确切知道自己内部和外部面临的信息安全问题，也很难把握自身现状与标准要求之间的差距，加上专业人才的缺乏，就更难在建设全面的信息安全管理体系上获得成功。专业的咨询顾问不但具有丰富的实践经验和知识积累，而且可以以第三方的视角客观、公正、全面地分析企业现存问题。打个比方，如果将企业比作病人，面临信息安全方面的病患，迫切需要诊治，专业的咨询顾问就应该能够承担医生的角色，为企业把脉诊断，开方抓药，取得“事半功倍”的效果。

其次，俗话说，“外来的和尚好念经”，“不识庐山真面目，只缘身在此山中”，由于企业自身条件的限制，其现有资源往往不足以应对企业信息安全问题的分析和解决，或者利用企业现有的人力资源解决问题会成本过高，加上企业内部错综复杂的关系往往通过外部力量更好疏通更好协调，这样一来，借助外部咨询顾问为其分析问题症结，并提出有针对性的解决方案，其获益将会更直接更快捷，也能更让人信服。此外，一个优秀的咨询公司往往在不同地区或者不同领域都有着丰富的经验，接触的企业客户多，接触的先进管理方式也较多，并且建立有完整的知识库和有效的方法论，以此引入企业，往往会带来很多新意识、新思维和新观念，这是企业员工乐意接受的。

再有，在有咨询顾问协助的项目实施过程中，通过不断沟通和交流，企业会逐渐掌握咨询顾问解决特定问题的方法和技术，增强企业解决信息安全问题的能力。信息安全咨询项目是十分系统和专业的，需要足够的经验和知识积累，由具有非常强的专业技能的人员为企业提供咨询服务，同时将所需知识和技能逐渐传递和转移给企业，这是企业寻求咨询顾问支持所看重的。所谓“授人以鱼，不如授人以渔”，在取得项目成功的同时，还能提升自己的能力，企业何乐而不为？

“坐在凳子上的人很难把自己搬起来”，要想公正、客观、全面地分析并解决自身的信息安全问题，要想在信息安全建设方面引入科学的方法、最佳的实践和最新的观念，寻求专业的咨询顾问帮助的确是不错的选择。

3.11 怎样选择顾问公司？

信息安全管理在国内的发展才刚刚起步，即便是有着较长期积累的发达国家和地区，信息安全管理的方法和模式也都因续的是一些最佳实践，还没有形成成熟的理论体系。因此，企业在选择咨询顾问帮助其建立信息安全管理体系并获取相关认证时，更多就应该从实践角度去考虑。

目前国内从事信息安全管理咨询的机构还不多，由于市场起步不久，很多都还处于摸索和积累阶段。能够承担 BS7799 认证咨询业务的公司，大致上有以下几个类型：

- **传统的管理咨询机构**：以四大为代表的传统的审计和咨询机构，在承接 IT 审计和咨询业务的同时，必然也会切入信息安全领域。此类公司优势在于其长期积累下来的管理咨询经验、方法和品牌。不过，由于信息安全建设对专业技能的要求很高，解决专业技术问题并非此类公司的特长。
- **从事体系认证的咨询机构**：典型的，是从事传统的 ISO9000、ISO14000 等体系认

证的咨询机构，这些机构在帮助企业通过体系认证方面有着丰富的经验，熟谙认证之道和审核技巧。当然，同样的问题是，他们在信息安全专业领域涉入不深，往往会影响到具体问题的解决。

- **信息安全专业公司**：随着信息安全这些年的发展，国内也涌现出不少有实力的信息安全专业公司，他们在信息安全技术领域涉入很深，有着扎实的理论和技术功底，在解决企业具体信息安全问题方面的确有着优势。不过，由于往往专注于技术和细节，从更高层次看待企业整体的管理问题并非他们擅长，加上以产品研发和销售为主营的一些公司，咨询服务的能力和经验还是薄弱了一些。
- **专业的信息安全管理咨询机构**：近两年来，随着市场需求的催生，一些专业的信息安全管理咨询机构逐渐脱颖而出，他们往往出身于传统的信息安全专业机构，有着深厚的技术背景和能力，同时，又接受了国际上先进的管理咨询思想和理念，在长期的实践积累过程中，总结出符合信息安全管理特性的咨询方法和模式。此类机构的出现，应该是更能迎合专业细分需求的结果。

当然，无论是什么类型的咨询公司，对企业来说，选择最适合自己的才是关键。一般来说，以下几点是选择咨询公司时应该考虑的。

- **成功案例**：企业在聘请咨询公司帮助自己解决问题时，最看重的是咨询公司能将其丰富的积累和实践经验带进来，而最能说明经验和积累的，就是典型案例。优秀的咨询公司，往往在很多领域都有自己的成功案例，并且留下很好的口碑。对企业来说，做出选择之前，多看看多听听，往往能让自己的判断更加准确。
- **顾问背景**：咨询公司为客户提供服务，说到底是“卖人”，就是专业的咨询顾问。咨询顾问到底能力如何？是否真的有专长？能否与客户愉快地合作和沟通？查看一下顾问的履历，看看其专业和实践背景，是回答这些问题的思路。就信息安全来说，担任咨询顾问的专业人员，除了必须具备咨询工作基本素质和技能之外，还应该在专业领域有深厚的积淀，CISSP（国际上最受认可的信息安全专业资质）、CISA（国际上最受认可的信息系统审计资质）、BS7799 主任审核员等资质，就是对此类人员很好的证明。
- **技术实力**：前面提过，信息安全管理咨询是有着较高专业技术要求的咨询活动，提供咨询服务的机构是否具有很强的技术实力，是否在此领域有长期的实践和积累，将决定着最终信息安全项目的成败。企业在信息安全方面投入，毕竟不仅仅是通过认证获取证书而已，而是应该实实在在发掘自身问题，并且提供切实可行的解决方案，最终获得信息安全长治久安的效果。如果没有坚实的技术实力，咨询公司是很难为企业长期把脉护体的。
- **培训能力**：企业在聘请咨询公司时有一个很重要的考虑，就是从咨询公司那里学习，将咨询公司某方面的专业技能传递并且转移到企业内部。所以，咨询公司能否为企业提供合理有效的知识转移计划，能否真正做好知识转移，这是考察咨询公司实力的很重要的一环。优秀的咨询公司，应该具备很强的培训和知识转移的能力，无论是现场培训还是专门的课程，都应该能够切合企业所需。
- **行业背景**：既然是提供信息安全管理咨询及认证辅导的服务，咨询公司就应该对整个行业有敏锐而准确的把握，应该深谙 BS7799 认证之道，与各认证机构有着良好的沟通关系，掌握行业发展的态势，为客户提供及时的建议和对策。
- **服务价格**：除了以上几个因素之外，价格也是企业选择咨询公司时非常看重的，而且有时候甚至是最为看重的。由于市场才刚刚起步，专业咨询服务很难在价格上有统一的标准，大的咨询公司和小的咨询公司，著名的跨国机构和国内公司，其价格差别往往会较大。这就需要企业自己把握，在综合前面各个因素的同时，对服务价

格有一个合理的期望。

总之，在选择咨询公司时没有唯一的标准，企业结合自己实际情况，综合分析，客观判断，合理选择，找到适合自己的合作伙伴，这才是最好的结果。

4. 实践篇

4.1 什么是信息安全管理体系？

信息安全管理体系（Information Security Management System，ISMS）是组织整体管理体系的一个部分，是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。基于对业务风险的认识，ISMS 包括建立、实施、操作、监视、复查、维护和改进信息安全等一系列的管理活动，并且表现为组织结构、策略方针、计划活动、目标与原则、人员与责任、过程与方法、资源等诸多要素的集合。

ISO27001 是建立和维护信息安全管理体系的标准，它要求应该通过这样的过程来建立 ISMS 框架：确定体系范围，制定信息安全策略，明确管理职责，通过风险评估确定控制目标和控制方式。体系一旦建立，组织应该实施、维护和持续改进 ISMS，保持体系运作的有效性。此外，ISO27001 非常强调信息安全管理过程中文件化的工作，ISMS 的文件体系应该包括安全策略、适用性声明（选择与未选择的控制目标和控制措施）、实施安全控制所需的程序文件、ISMS 管理和操作程序，以及组织围绕 ISMS 开展的所有活动的证明材料。

4.2 怎样建设 ISMS 并最终寻求认证？

组织在确定实施 ISMS 建设及 ISO27001 认证项目之后，通常有两种途径可以去操作，一种是自己做，在组织内部成立专人专项工作组，按照计划自我实施。另一种就是选择有实力的咨询机构，帮助组织完成此项目。两种途径各有所长，关键是看组织自身特点和看问题的角度。如果组织规模不大、业务模式简单、信息系统也不复杂，而且自身对信息安全的认识和运作已经达到了一定高度，有胜任的人员，选择自我实施就是比较经济快捷的途径。不过，如果组织规模较大、组织结构相互关联、对 IT 的依赖广泛，更重要的是，组织本身对信息安全的意识和运作还处于较低水平，或者发展并不均衡，这就需要有外部力量来进行引导，他们以公正独立的姿态，把一些成熟的经验移植过来，以最直接快速的方式发现组织现有问题并对症下药。此外，有经验的咨询机构和顾问通常都能比较好地把握认证机构的“偏好”和习惯，这一点尤其对最终应对审核很重要。一般来说，咨询机构可以在人员培训、全程辅导、后续支持等方面给予组织大力的支持。所谓的“当局者迷，旁观者清”、“外来和尚好念经”，在 ISMS 建设及认证项目上也是这个道理。

当然，无论是选择自我实施，还是请外部的咨询机构和顾问，组织都应该知道，实施 ISMS 认证项目，必须要有一套行之有效的方法，事先要对整个过程做好计划。

在建设信息安全管理体系的方法上，ISO27001 标准为我们提供了指导性建议，即基于 PDCA 的持续改进的管理模式。PDCA 是一种通用的管理模式，适用于任何管理活动，体现了一种持续改进、维持平衡的思想，但具体到 ISMS 建立及认证项目上，就显得不够明确和细致，组织必须还要有一套切实可行的方法论，以符合项目过程实施的要求。在这方面，ISMS 实施及认证项目可以借鉴很多成熟的管理体系实施方法，比如 ISO9001、ISO14001、TS16949 等，大致上说，这些管理体系都遵循所谓的 PROC 过程方法。

PROC 过程模型（Preparation-Realization-Operation-Certification）是对 PDCA 管理模式的一种细化，它更富有针对性和实效性，并且更贴近认证审核自身的特点。

PROC 模型如图 9 所示。

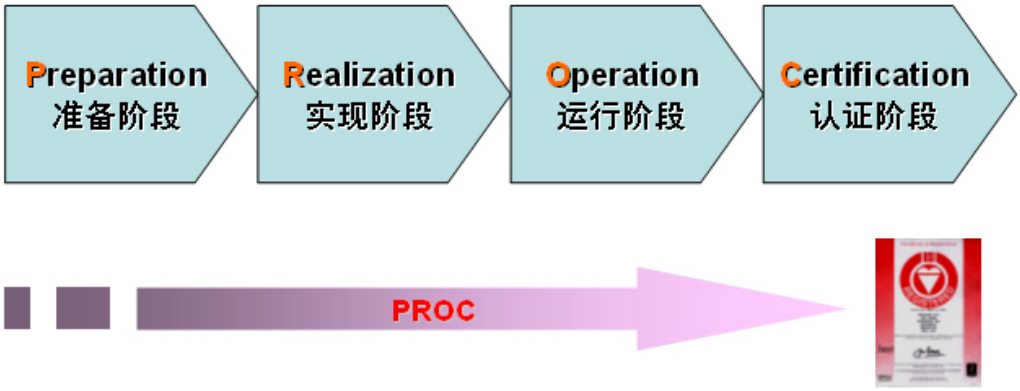

图 9.　PROC 过程方法

PROC 模式将整个信息安全管理体系建设项目划分成四个阶段，共包含 15 项关键的活动，如果每项具有前后关联关系的活动都能很好地完整，最终就能建立起有效的 ISMS，实现信息安全建设整体蓝图，接受 ISO27001 认证并获得认可更是水到渠成的事情。

- **准备阶段（Preparation）**：在准备阶段，项目小组要对 ISMS 实施及认证做好预备工作，明确 ISMS 实施范围，提供相关资源，建立总体的安全管理方针，进行前期培训和预先评估，分析了解业务状况，进行详细的风险评估，发掘安全需求。这一阶段包括以下五项关键活动：
  - **项目启动**：前期沟通，实施计划，项目小组，资源支持，启动会议。
  - **前期培训**：信息安全管理基础，风险评估方法。
  - **预先审核**：初步了解信息安全现状，分析与 ISO27001 标准要求的差距。
  - **业务分析**：访谈调查，核心与支持业务，业务对资源的需求，业务影响分析。
  - **风险评估**：资产、威胁、弱点、风险识别与评估。
- **实现阶段（Realization）**：在实现阶段，项目小组要组织相关资源，依据风险评估结果选择控制措施，为实施有效的风险处理做好计划，同时编写、测试、修订并完善 ISMS 运行和认证所需的文档体系，管理者需要正式发布 ISMS 体系并要求开始实施，通过普遍的培训活动来推广执行。此阶段包括四项关键活动：
  - **风险处理**：针对风险问题，做文件编写规划、BCP 规划和技术方案规划。
  - **文件编写**：编写 ISMS 各级文件，多次 Review 及修订，管理层讨论确认。
  - **发布实施**：ISMS 实施计划，体系文件发布，控制措施实施。
  - **中期培训**：全员安全意识培训，ISMS 实施推广培训，必要的考核。
- **运行阶段（Operation）**：ISMS 建立起来（体系文件正式发布实施）之后，要通过一定时间的试运行来检验其有效性和稳定性。在此阶段，应该培训专门人员，建立起内部审查机制，通过内部审计、管理评审和模拟认证，来检查已建立的 ISMS 是否符合 ISO27001 标准以及企业自己规范的要求。此阶段的关键活动有四项：
  - **认证申请**：与认证机构磋商，准备材料申请认证，制定认证计划，预审核。
  - **后期培训**：审核员等角色的专业技能培训。
  - **内部审核**：审核计划，Checklist，内部审核，不符合项整改。
  - **管理评审**：信息安全管理委员会组织 ISMS 整体评审，纠正预防。
- **认证阶段（Certification）**：经过一定时间运行，ISMS 达到一个稳定的状态，各项

文档和记录已经建立完备，此时，可以提请进行认证。此阶段的关键活动就是为认证做好准备：

- **认证准备：**准备送审文件，安排部署审核事项。
- **协助认证：**内部审核小组陪同协助，应对审核问题。

四个阶段的 15 项关键活动，基本上是顺序开展的，其中各阶段的培训活动，则可以与其他活动并列进行。关键活动流程参见图 10。

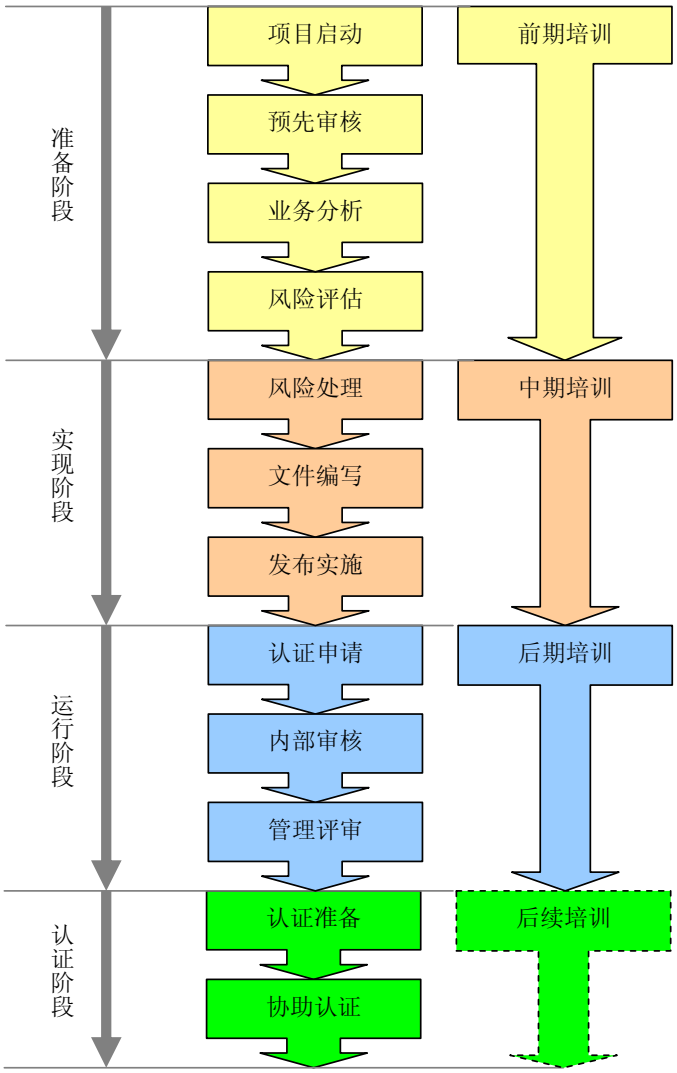

图 10.　PROC 各阶段的关键活动

4.3 怎样组建项目实施队伍？

正式启动 ISO27001 认证项目之前，组织应该为项目实施组建团队，并且明确团队成员各自的职责。项目团队构成通常可以如图 11 所示。

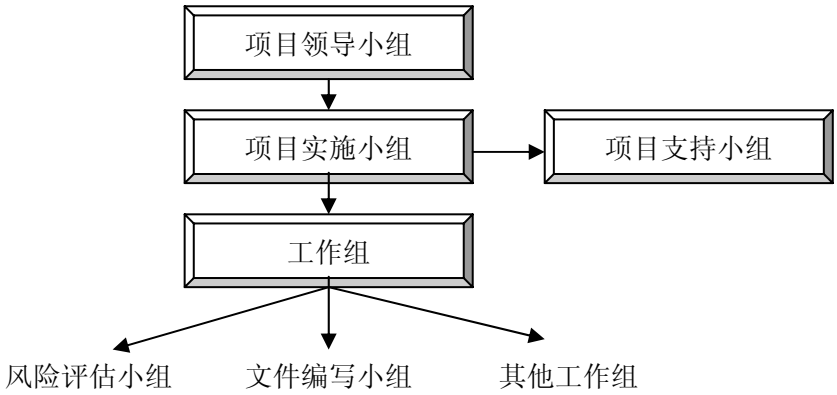

图 11.　ISMS 建设及 ISO27001 认证项目团队构成

这里，项目领导小组应该由公司具有决策权利的人员构成，该小组负责宏观掌控项目进展，对重要阶段成果进行评审，及时指正重大问题，协调沟通各个单位和人员，监督项目执行情况，推动项目顺利实施。项目领导小组应该能够代表组织最高管理者对项目实施的期望和承诺，这种承诺体现在各个层面上，包括运作、技术、预算、时间等。

项目实施小组通常由项目经理担纲，其成员通常来自各个单位或部门。项目经理从整体上负责项目的运作，向各个工作组分配任务，领导项目具体实施。

项目各阶段以及各个不同类型的任务应该由不同的工作组来承担，包括风险评估小组、文件编写小组、风险处理小组等，而整个项目实施过程中需要的一些资源和支持服务，则由项目支持小组来负责，例如必要的人员培训。

4.4 怎样确定 ISMS 实施范围？

确定信息安全管理体系（ISMS）的范围（Scope），是实施 ISO27001 认证项目最关键的前提条件，只有在明确实施范围之后，整个项目各阶段的活动才能有秩序有控制地进行。在后续审核阶段，组织向认证机构提出申请时，是否有确定的范围也是认证机构启动审核的一个必须的条件。

通常范围的确定有两种情况，一种是将整个组织都纳入到认证范围之内，另一种是只针对个别单位和部门。如果是整个组织，好处是界限分明，统一管理，利于长期发展，也利于与其他管理体系（例如 ISO9001、ISO14001 等）有效融合，最终形成企业统一的文化，但有个前提是，管理层必须充分授权，并且有一个权威机构（或人员）来统一协调组织各个部门之间的事务。如果只针对个别部门或单位来认证，范围小，可控性强，易于操作和实施，在实施过程中积累下的经验教训，可以为以后扩大范围到其他部门甚至整个组织而吸取，不过，这种方式要求实施认证的部门独立性很强，与组织其他部门关系不紧密，而且，容易引发组织整体发展的不均衡。

无论怎么考虑，范围的界定总归是要从组织的业务出发的，通过分析业务流程（尤其是核心业务），找到与此相关的人员、部门和职能，然后确定业务流程所依赖的信息系统和场所环境，最终从逻辑上和物理上对 ISMS 的范围予以明确。

需要注意的是，组织确定的 ISMS 范围，必须是适合内外部客户所需的，且包含了与所有对信息安全具有影响的合作伙伴、供货商和客户的接触关系。为此，组织应该通过合同、服务水平协议（SLA）、谅解备忘录等方式来说明其在与合作伙伴、供货商以及客户接触时实施了信息安全管理。

组织在描述 ISMS 范围时应该包括：

- ◆ 为内部或外部客户提供的（也是需要保护的）服务、信息系统、资产等。
- ◆ 实际的物理场所和对象信息（地理位置、部门等）。

表 11 列举了一些通过认证的组织的 ISMS 范围描述（数据来自 ISMS IUG）。

表 11　　ISMS 范围示例

组织名称	ISMS 范围
Supermask Co Ltd	The Information Security Management System for the sales, research, production and storage of photomask. This is in accordance with the Statement of Applicability, Issue A1, dated 23/6/2003.
Doctor A Security Systems (HK) Ltd	The Information Security Management System for provision of Managed Security Services including: Intrusion Detection Monitoring Service; Security Assessment and Audit Service. This is in accordance with the Statement of Applicability Version 1.2 dated 17 Jan 2003
Empower Systems Ltd	The information security management system related to the development, management and operation of secure internal and external systems for the collection, analysis, processing, storage and dissemination of data. The analysis of client businesses to identify an effective, secure and profitable business information management system. This is in accordance with the Statement of Applicability Issue 3.0 dated 12 February 2003.
Daegu Bank	The management of information security system in "Internet Banking Services" provided company's WEB Home-page. The scope specifically includes the management of service development & operation process, client & company information, servers & PCs excluding Host within the internet banking domain from the Daegu HQ. This is in accordance with Statement of Applicability Version 1.0

4.5 如何进行风险评估？

对现代企业来说，信息安全实质上是风险管理的问题，风险管理是围绕信息安全风险而展开的评估、处理和控制活动，其中，风险评估更是建立信息安全管理体系的先决条件，是 PDCA 中 Plan 阶段最关键的一项活动。基于风险评估，组织可以对当前的信息安全状况有一个系统全面的了解，找出潜在问题，分析原因，判断严重性和影响，以此来确定自己在信息安全建设方面的需求。BS7799 标准明确提出，组织所有选择控制目标和控制的举动，都应该根据由风险评估而导出的真实需求而来。

关于风险及相关要素之间的关系，构成了风险管理的理论基础，ISO/IEC TR 13335 标准中那幅经典的关系图则成为这种理论的最佳描述，如图 12 所示。有关风险管理及风险评估的更多介绍，参见 ISMG-001:《信息安全风险管理概要》。

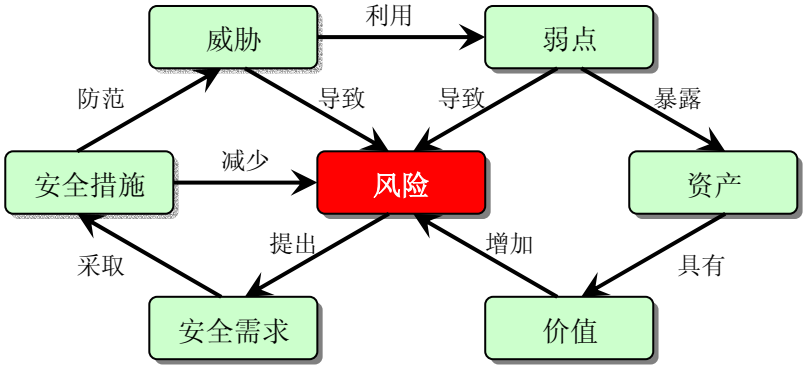

图 12.　风险管理各要素之间的关系

组织在实施风险评估时，应该组建一个风险评估小组，由能够代表各个相关单位和部门的人员组成，各自负责与本部门相关的风险评估事务，并且能共同讨论一些问题。风险评估小组需要指定一个能够担负责任的组长，负责整体协调风险评估事务。在风险评估亦始，评估小组及相关人员应该接受必要的培训，理解信息安全管理基本知识，掌握风险评估的方法和技巧。

完整的风险评估活动，会经历几个节点，通常包括：

- **前期沟通**：前期调研，了解需求，启动风险评估项目；
- **项目计划**：明确目标和范围，对系统环境进行描述，确定各项评估指标，建立评估小组并明确责任，进行必要的培训，提供必须的资源，准备适用的表格、问卷等材料，制定项目计划；
- **资产评估**：识别并评估关键的信息资产；
- **威胁评估**：识别威胁，衡量威胁的可能性；
- **弱点评估**：识别各类弱点（包括现有控制的不足），衡量弱点的严重度；
- **风险评估**：进行风险场景描述，评价风险，划分风险等级，编写风险评估报告；
- **风险处理**：推荐、评估并确定控制目标和控制，编制风险处理计划。

这些节点活动具有紧密的前后关联，前一个节点的输出是下一个节点的输入，这种关系如图 13 所示。

图 13.　风险评估实施流程

对组织来说，事先选择适合的风险评估方法是非常重要的，这也是 ISO27001 标准所要求的（标准本身并没有规定具体的风险评估方法）。传统的风险评估方法主要是定量和定性两种，对 ISO27001 认证项目来说，选择定性方法应该是更简便有效的。实施者因为所处行业的特点，通常会选择一些带有很强行业特色的风险评估方法，比如很多与汽车配件生产相关的半导体制造企业，因为在实施 ISO/TS 16949 以及 QS 9000 质量管理体系时会采用 FMEA（Failure Modes and Effects Analysis，失效模式和后果分析）方法，只需要将一些专业术语映射到信息安全领域，就很容易移植过来使用。

前面我们在介绍 BS7799 相关标准时提到，ISO/IEC TR 13335 对风险评估的过程和方法

有较为详细的描述，风险评估的实施者可以参照执行。另外，OCTAVE（Operationally Critical Threat, Asset and Vulnerability Evaluation）也是目前较为常用的一种风险评估方法。OCTAVE 由 Carnegie Mellon 大学创建，它依赖于组织管理层的授意和指导，需要组织各业务单位和 IT 部门通力协作，适合组织“自主”实施。遵循 OCTAVE 方法，组织可以基于关键信息资产 CIA 所面临的风险来作出信息保护决策。有关 OCTAVE 的相关知识，可以参见 http://www.cert.org/octave/。

4.6 风险评估有什么工具可以利用？

无论选定了何种风险评估方法，组织在实施过程中通常都会借助一些辅助工具来提升工作的效力和效率。有效利用各种工具，可以帮助评估者更准确更全面地采集和分析数据，增强繁琐工作的自动化水平，并且最大程度上减少人为失误。当然，风险评估工具并不局限于完全技术性的产品，事实上很多都是评估者经验积累的成果。

常用的风险评估工具包括：

- **调查问卷**：风险评估者可以根据自己的目标需求来设计调查问卷，比如BS7799符合性调查问卷（Checklist）、控制现状调查问卷、业务流程调查问卷等。定性风险评估过程中，评估者通常都是借助调查问卷来对组织的管理和运营层面进行评估和分析的。
- **扫描工具**：为了发掘信息系统的技术漏洞，评估者可以使用自动化的扫描工具，或者实施授权之下的渗透测试。目前市面上可见的商业化扫描器有很多种，一些免费的扫描工具也值得选择。
- **风险评估软件**：因为风险评估方法本身并没有标准可循，所以目前还没有哪类专门针对风险评估的软件产品得到普遍适用，不过，还是有一些工具可以参考，例如比较早期的Cobra和CRAMM，还有较新的Callio。Cobra是一种定性评估的工具，本质上是一种自动化的调查问卷生成、处理及分析工具，特别适合进行ISO17799标准符合性一类的检查。CRAMM则是一种半定量的风险评估工具，其评估过程本身就体现了一种完整而细致的风险评估方法。而Callio则是直接针对BS7799/ISO27001认证而提供的一款基于Web的工具，除了帮助企业实施定性的风险评估之外，在策略文件建立和ISMS认证方面都有一定的利用价值。

4.7 如何确定风险处理计划？

风险评估得出结果，意味着组织真正掌握了自身的信息安全需求，接下来最关键的就是对症下药，制定并实施有效的风险处理计划。

风险处理计划可以是分阶段分层次的，组织在制定计划时应该优先考虑与关键业务最紧密相关的信息系统环境。至于先做什么后做什么，应该根据风险评估得出风险等级之后，由决策者最终确定。

不过，无论优先顺序如何考虑，组织都有必要有计划地实施以下事务：

- 编写并完善**信息安全策略**文件，这是统领组织信息安全管理各项事务的总体纲领、指导方针和行动指南。务必做到信息安全管理“有法可依”和“有法必依”，并且尽量实现“执法必严”和“违法必究”；
- 在**人员组织**方面应该做到：
  - 组建（或调整）信息安全管理组织架构，设定人员责任（需要与整体的信息安

全文件体系建设一起考虑）；

- 实施层次化和全方位的人员意识培训，使每一个员工能够自觉履行安全责任，使每一个系统管理和维护人员掌握应有的安全技能，使信息安全管理者有能力去行使信息安全管理职权；

- 在**流程建设**方面应该做到：
  - 建立文档安全管理流程，防止关键数据和信息泄漏；
  - 如果有软件开发业务，应该在软件开发过程中考虑安全控制机制，确保过程数据（包括开发代码、测试数据等）、开发成果和知识产权得到保护；
  - 加强内部审核，建立内部审核流程和制度，明确责任人，制定审核计划，定期对公司信息安全管理体系的运行情况进行审核，审核结果和人员考核挂钩，发现问题及时改进，使遵守信息安全策略真正成为每一个员工的意识和习惯；
  - 制定有效的业务持续性计划，建立业务持续性管理机制和框架；
  - 将安全管理流程与 IT 服务管理流程结合，在事件管理、变更管理、配置管理、问题管理等方面进行规范化。
- 在**信息安全技术**运用方面应该考虑：
  - 对 IT 基础设施实施安全加固，从系统一级消减因为配置或者操作不当而造成的安全风险；
  - 加强应用系统的安全性，采取应用审计和分析等手段，对架构于基础设施之上的各种应用系统进行安全加强；
  - 对适合于采用技术措施来予以消减的风险，应该制定可行的解决方案，或者委托专业技术公司来提供并实施解决方案，方案的实施应该在相应的策略或程序指导下进行。

有了安全计划，为了落实既定的目标，必须有针对性地设计解决方案，其中技术或产品解决方案就是很典型的例子。

4.8 应该怎样去构建 ISMS 文件体系？

ISO27001 标准所要求建立的 ISMS 是一个文件化的体系，ISO27001 认证第一阶段就是进行文件审核，文件是否完整、足够、有效，都关乎审核的成败，所以，在整个 ISO27001 认证项目实施过程中，逐步建立并完善文件体系非常重要。

组织应该建立专门的文件编写小组，负责构建 ISMS 文件体系。除了应满足标准要求和要有统一的格式之外，体系文件的编写还应该遵循以下原则：

- 文件应该符合业务运作和安全控制的实际情况，应该具有可操作性；
- 不同层次的文件之间应该保持紧密关系并且协调一致，不能存在相互矛盾的地方；
- 文件应该有一个编写、审核、修订、批准和实施的周期过程，确保最终定稿的文件是适宜和切实可行的。

编写 ISMS 文件时，除了依据标准和相关法律法规之外，组织还应该充分考虑现行的策略、程序、制度和规范，有所继承有所修正。如果组织之前已经实施过其他管理体系，例如 ISO 9001、ISO 14001 等，这些管理体系的文件也是很重要的参考依据。

ISO27001 标准要求的 ISMS 文件体系应该是一个层次化的体系，按照一般管理体系的惯例，通常是由四个层次构成的：

- **信息安全手册**：该手册由信息安全委员会负责制定和修改，是对信息安全管理体系框架的整体描述，以此表明确定范围内 ISMS 是按照 ISO27001 标准要求建立并运行的。信息安全手册包含各个一级文件。

- **一级文件**：全组织范围内的信息安全方针，以及下属各个方面的策略方针等。这需要从组织整体考虑来制定，应该能够反映组织最高管理者对信息安全工作下达的旨意，应该能为所有下级文件的编写指引方向。一级文件至少包括（可能不限于此）：
  - 信息安全方针
  - 风险评估报告
  - 适用性声明（SoA）
- **二级文件**：各类程序文件。这些程序文件应该是针对信息安全某方面工作的，是对信息安全方针内容的进一步落实，应该是不同部门都能适用的，至少包括（可能不限于此）：
  - 风险评估流程
  - 风险管理流程
  - 风险处理计划
  - 管理评审程序
  - 信息设备管理程序
  - 信息安全组织建设规定
  - 新设施管理程序
  - 内部审核程序
  - 第三方和外包管理规定
  - 信息资产管理规定
  - 工作环境安全管理规定
  - 介质处理与安全规定
  - 系统开发与维护程序
  - 业务连续性管理程序
  - 法律符合性管理规定
  - 信息系统安全审计规定
  - 文件及材料控制程序
  - 安全事件处理流程
- **三级文件**：具体的作业指导书。描述了某项任务具体的操作步骤和方法，是对各个程序文件所规定的领域内工作的细化。
- **四级文件**：各种记录文件，包括实施各项流程的记录成果。这些文件通常表现为记录表格，应该成为 ISMS 得以持续运行的有力证据，由各个相关部门自行维护。

4.9 如何设立信息安全管理组织？

为了有效运行、维护和改进 ISMS，组织应该着手完善自己的信息安全管理组织架构，通常应该考虑以下几点：

- **信息安全委员会**：组织应该建立全公司统一的信息安全委员会，评审信息安全方针，确保对安全措施的选择有一个明确的指导方向并且得到高管的实际支持，同时负责协调信息安全控制措施的实施情况，对重大变更进行决策，审查信息安全事故。信息安全委员会的成员应该包括：组织高管代表（通常是总经理）、信息安全主管、各单位代表（包括业务部门和 IT 部门）。
- **信息安全主管**：通常由组织的最高管理者委任，是组织高管在信息安全管理方面的代表。信息安全主管负责组织的信息安全方针的贯彻与落实，发生安全事故时，还需要做现场的指导和统筹。

- **信息安全委员**：组织各个部门应该有代表作为信息安全委员会的成员，除了承担信息安全委员会共同职责外，还应该负责各自部门内部的安全控制活动。
- **内审员**：信息安全主管应该委派 ISMS 内审人员，组建内审小组，按照既定的内审流程，对已实施的 ISMS 进行 ISO27001 符合性审查，以便及时发现问题，予以纠正。内审员必须由经过 ISMS 审核培训的、且有一定经验和技能的员工担任，内审工作应该保持独立性，最好是专人负责内审事务。

4.10 怎样加强人员安全意识并推动体系实施？

为了让所有承担 ISMS 相关任务的人员能够恪尽职守，组织必须确保：

- 确定承担信息安全工作的人员需要何种技能；
- 给予相关人员适当的培训，必要时，需要为特定任务招聘有经验的人；
- 评估培训效果；
- 维护一个教育和培训程序，对每个职员的能力、经验和资历进行登记。

组织必须确保相关人员能够意识到其所进行的信息安全活动的重要性，并且清楚各自在符合 ISMS 目标过程中参与的方式。为此，开发一个培训和意识程序是非常重要的。通过有计划有步骤地实施意识培训，让每一个职员都能理解并遵守信息安全最佳实践，这比购买最高端产品采用最精尖技术来得更有效更经济，说到底，信息安全问题，最关键是人的问题。通常最先受到安全事件影响的就是人，如果每个人都能意识到安全问题可能造成的危害，就能够在事件发生时及时报告和处理，避免或降低负面影响。

组织在实施一个信息安全意识程序时，有几个关键因素需要考虑：

- 努力使这种意识能够融入到组织整体的环境和文化当中；
- 确保高级管理者承诺并支持；
- 理解职员对于安全的重要性；
- 找到内部沟通渠道；
- 充分利用现有资源；
- 建立策略、程序、表格和相关的检查表单；
- 识别程序的最终结果；
- 确保能够交付到人。

就 ISMS 实施及 ISO27001 认证项目来说，每个阶段的工作，相关人员都需要接受必要的培训和意识的宣贯，在这方面，组织可以邀请有实力有经验的专业机构，拟定意识和培训计划，实施意识和培训活动，考核最终效果。

ISMS 培训工作应该分层次、分阶段、循序渐进地进行。借助培训，组织一方面可以向一般员工宣贯安全策略、提升安全意识；另一方面，也可以向特定人员传递专业技能（例如风险评估方法、策略制定方法、安全操作技术等）；此外，面向管理人员的培训，能够提升组织整体的信息安全管理水平；当然，还有针对内审人员的 ISO27001 审核员培训。所有这些培训，如果成功实施，定能极大促进 ISO27001 认证项目的顺利进行。

通常来讲，组织应该考虑实施的培训内容包括：

- **信息安全意识培训**：在 ISMS 实施亦始或最终运行阶段，组织可以为所有人员提供信息安全意识培训，目的在于让所有与 ISMS 相关的人员都了解信息安全管理基本要领，理解信息安全策略，知道信息安全问题所在，掌握应对和解决问题的方法和途径。
- **信息安全管理基础培训**：在 ISMS 准备阶段，组织可以向 ISMS 项目实施相关人员（例如风险评估小组人员、各部门代表等）提供 BS7799 基础培训，通过短期学习，

帮助大家掌握 BS7799 标准的精髓，理解自身角色和责任，从而在 ISMS 项目实施过程中起到应有的作用。

- **ISMS 实施培训**：组织可以向 ISMS 项目的核心人员提供 ISMS 实施方法的培训，包括风险评估方法、策略制定方法等，目的在于协作配合，共同推动 ISMS 项目有序且顺利地得以进展。
- **信息安全综合技能培训**：为了让 ISMS 能够长期稳定地运行下去，组织可以向相关人员提供信息安全操作技能的培训，目的在于提高其运营 ISMS 的技术能力，掌握处理问题的思路和方法。
- **BS7799 内审员培训**：组织可以为内审人员提供系统的学习课程，帮助其掌握 BS7799 内部审计所需知识和技能，从而增强企业 ISMS 的长期稳定性。

4.11 如何对 ISMS 进行内部审核？

ISO27001 明确指出，在 PDCA 的 Check 阶段，组织应该借助安全审计等途径，对 ISMS 的效力进行定期评审，以确定其是否符合既定的安全方针和目标，确定安全控制是否依然有效。安全审计可以由组织内部来完成（内部审核），也可以由第三方机构来实施（外部审核），一般来说，建立 ISMS 之后，在后续长期的运行过程当中，组织最应该诉求的，是做好内部审核工作。

内部审核的实质，是验证组织信息安全管理体系的有效性，看其是否符合标准规范的要求，是否符合组织既定的安全需求。

内部审核通常包括管理和技术两个方面，一方面，组织可以依据 ISO27001 标准、自身的方针和程序等管理文件，对组织当前 ISMS 所有相关活动和内容进行符合性检查；另一方面，组织可以借助一些技术手段，对信息系统进行检查以确保其符合安全实施标准。内部审核可以作为提请真正认证审核的一项模拟活动来进行。

具体的内部审核流程和方法，参见 ISMG-006:《信息安全管理内审指南》。

4.12 建设 ISMS 得以成功的关键因素有哪些？

组织要让信息安全管理体系实施过程顺利进行，并且最终取得期望的结果，必须具备一些通往成功的要素：

- 安全策略、目标和活动应该反映业务目标；
- 实施信息安全的方法应该与组织的文化保持一致；
- 来自高级管理层的明确的支持和承诺；
- 深刻理解安全需求、风险评估和风险管理；
- 向所有管理者和员工有效地推广安全意识；
- 分发信息安全策略、指南和标准给所有员工及签约人；
- 提供适当的培训和教育；
- 建立完整而平衡的测量体系，用来评估信息安全管理体系的表现，提供改进的反馈建议。

这里再次强调，信息安全管理体系的实施，是一项自顶向下的企业管理活动，必须得到最高管理者的确定承诺和有效的支持，只有这样，组织的信息安全方针才能上传下达，组织的信息安全管理活动才能有序进行，组织的信息安全目标才能最终实现。