第6章 信息安全管理基础

信息安全工程与实践

- 本章学习目标
  - 了解信息安全管理的概念，理解信息安全管理的意义。
  - 明确信息安全管理的内容及原则，熟悉信息安全管理的模型。
  - 熟悉信息安全管理标准，了解 BS7799 系列标准的主要内容。
  - 掌握信息安全管理体系 PDCA 循环模型。
  - 理解信息安全管理体系过程。

6.1 概述

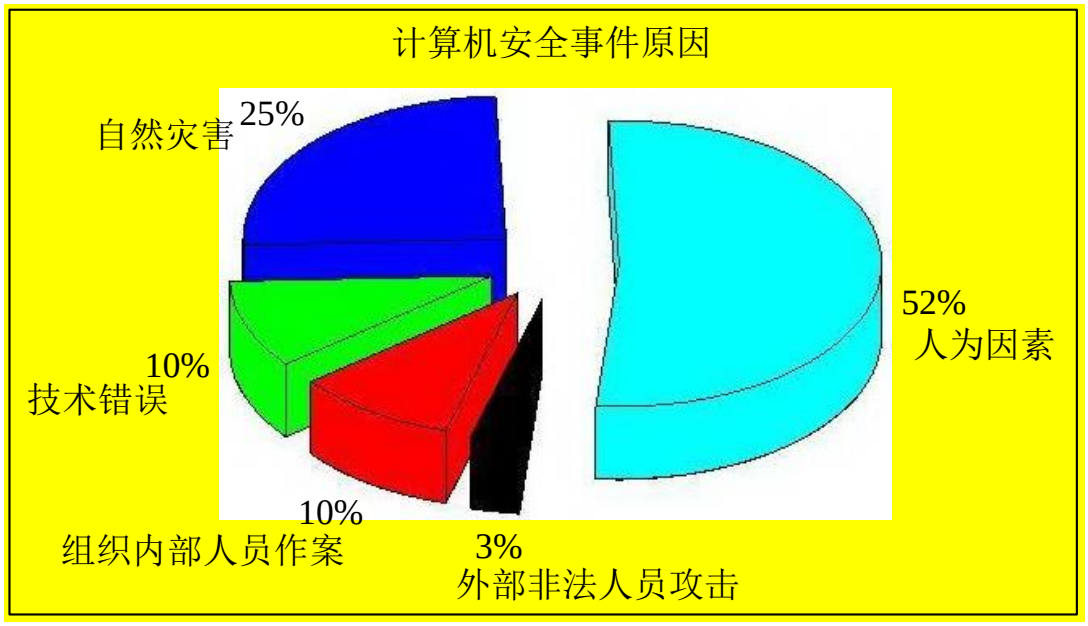
- 传统的信息系统安全建设一般是事后的、被动的和单一的，应对措施简单，针对出现的问题，主要采用一些技术上的安全防护措施，并以某个问题的暂时解决为结束的标志。

- 信息安全管理需要站在系统工程的角度，从管理和技术两方面对它进行全面的分析

6.1 概述

信息安全管理的概念

- 什么是信息安全管理
  - 仅依靠产品和技术，即使采购和使用了足够先进、数量够多的信息安全产品，仍无法避免一些安全事件。
  - 计算机安全事件原因分析:



6.1 概述

信息安全管理的概念

- ✦什么是信息安全管理
- **信息安全管理**是组织中用于指导和管理各种控制信息安全风险、一组相互协调的活动，有效的信息安全管理应该是在有限的成本下，尽量做到安全“滴水不漏”。
- 计算机犯罪具有**瞬时性、广域性、专业性**.
  - 信息系统管理规范化
  - 流程的规范化
  - 组织结构的规范化
  - 规章制度的规范化

6.1 概述

国内外信息安全管理现状

- 国外
  - 目前在信息安全技术处于领先的国家主要是美国、法国、以色列、英国、丹麦、瑞士等，一方面这些国家在技术上，特别是在芯片技术上有着一定的历史沉积，另一方面这些国家在信息安全技术的应用上。
  - 优势主要集中在防火墙、入侵检测、漏洞扫描、病毒查杀、身份认证等传统的安全产品上。

6.1 概述

国内外信息安全管理现状

✦国内

➢ 我国信息安全管理当前的成绩：

- ✓ 初步建成了国家信息安全组织保障体系。
- ✓ 制定了一系列必须的信息安全管理法律法规。
- ✓ 制定和引进了一批重要的信息安全管理标准。
- ✓ 信息安全风险评估工作已经得到重视和开展。

6.1 概述

信息安全管理的意义

- 信息已经成为维持社会经济活动和生产活动的重要基础资源，成为政治、经济、文化、军事乃至社会任何领域的基础。
- 信息安全管理是保护国家、组织和个人等各个层面上信息安全的重要基础。在一个有效的信息安全管理体系上，通过完善信息安全管理结构，综合应用信息安全管理策略和信息安全技术产品，才有可能建立起一个真正意义上的信息安全保障体系。

6.1 概述

信息安全管理内容与原则

✦ 信息安全管理内容

- 落实安全管理机构及安全管理人员，明确职责，制定安全规划。
- 开发安全策略。
- 实施风险管理。
- 制定业务持续性计划和灾难恢复计划。
- 选择与实施安全措施。
- 保证配置、变更的正确与安全。
- 进行安全审计。
- 保证维护支持。
- 进行监控、检查，处理安全事件。
- 安全意识与安全教育。
- 人员安全管理等。

6.1 概述

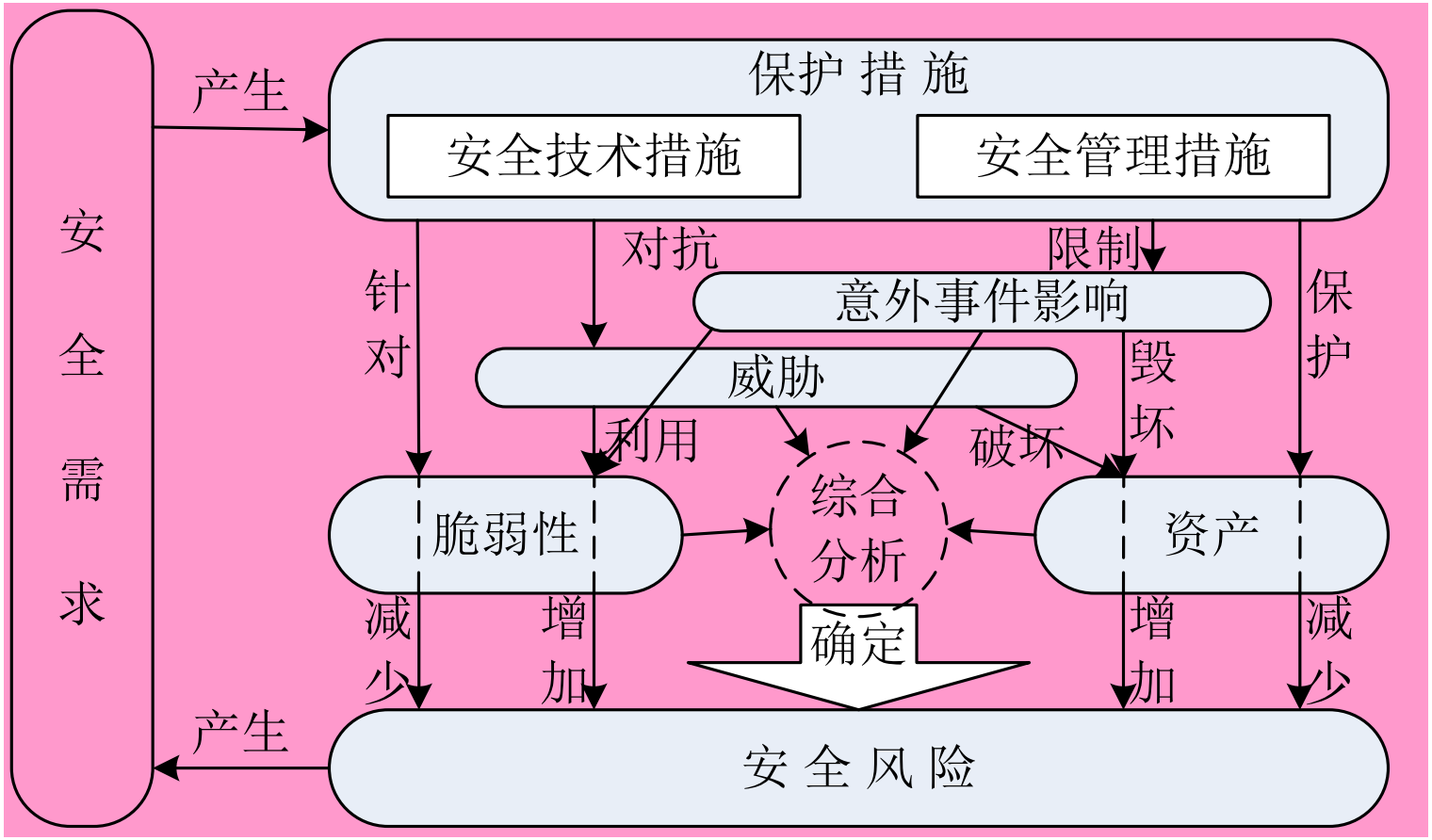
信息安全管理内容与原则

✦ 信息安全管理原则

- 基于安全需求原则。
- 主要领导负责原则。
- 全员参与原则。
- 系统方法原则。
- 持续改进原则。
- 依法管理原则。
- 分权和授权原则。
- 选用成熟技术原则。
- 分级保护原则。
- 管理与技术并重原则。
- 自保护和国家监管结合原则。

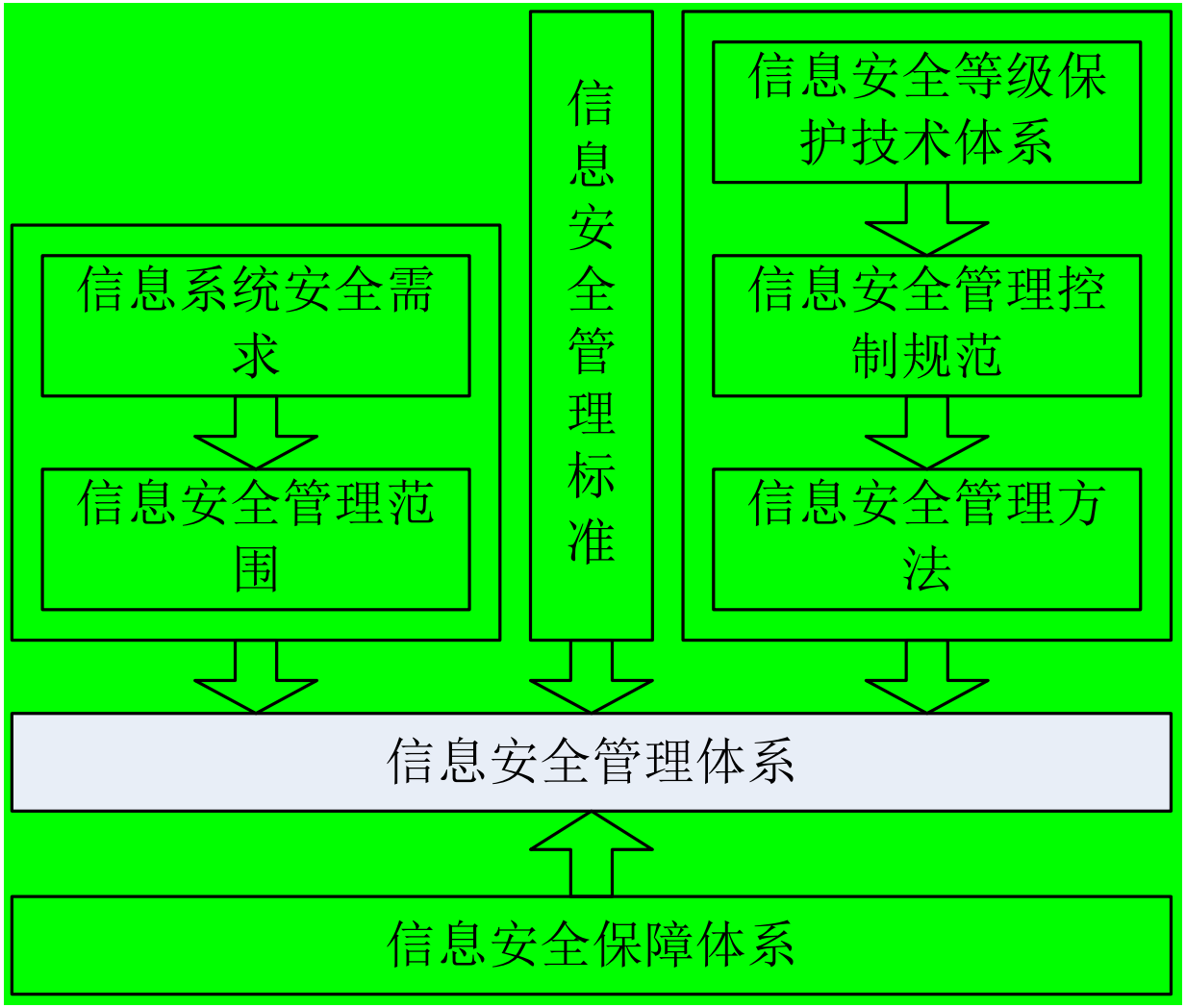
6.1 概述

信息系统的安全因素



6.1 概述

信息安全管理模型



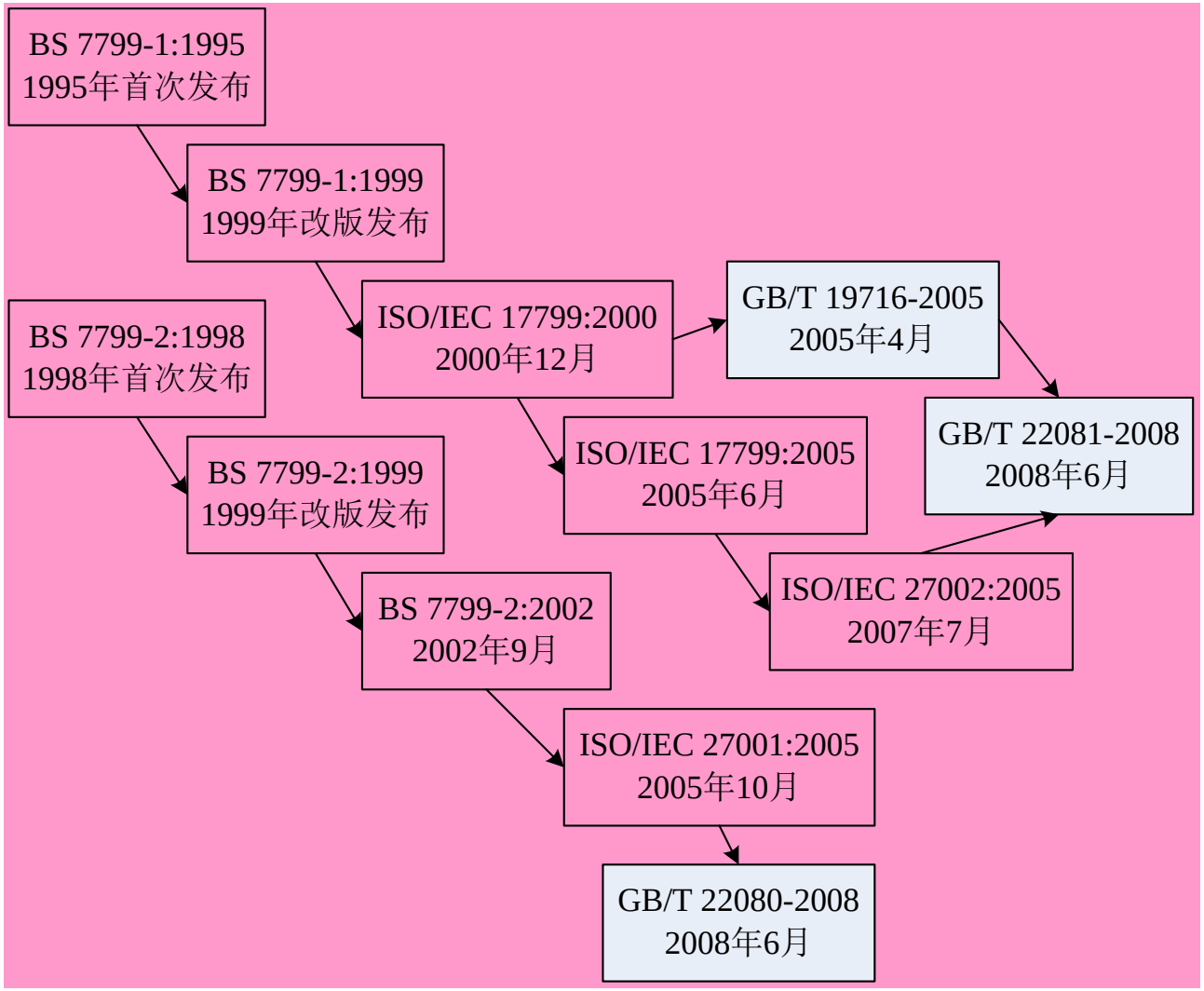
6.1 概述

信息安全管理实施要点

- 信息安全管理的方法包括法律方法、行政方法、经济方法和宣传教育方法，四者相互结合，形成完整的管理方法体系
  - 法律方法是指通过国家制定和实施的各种法规进行管理的方法。
  - 行政方法。
  - 经济方法。
  - 宣传教育方法是指通过多种形式的教育，全面提高全社会的安全素质。

6.2 信息安全管理标准

信息安全管理标准的发展



6.2 信息安全管理标准

BS 7799

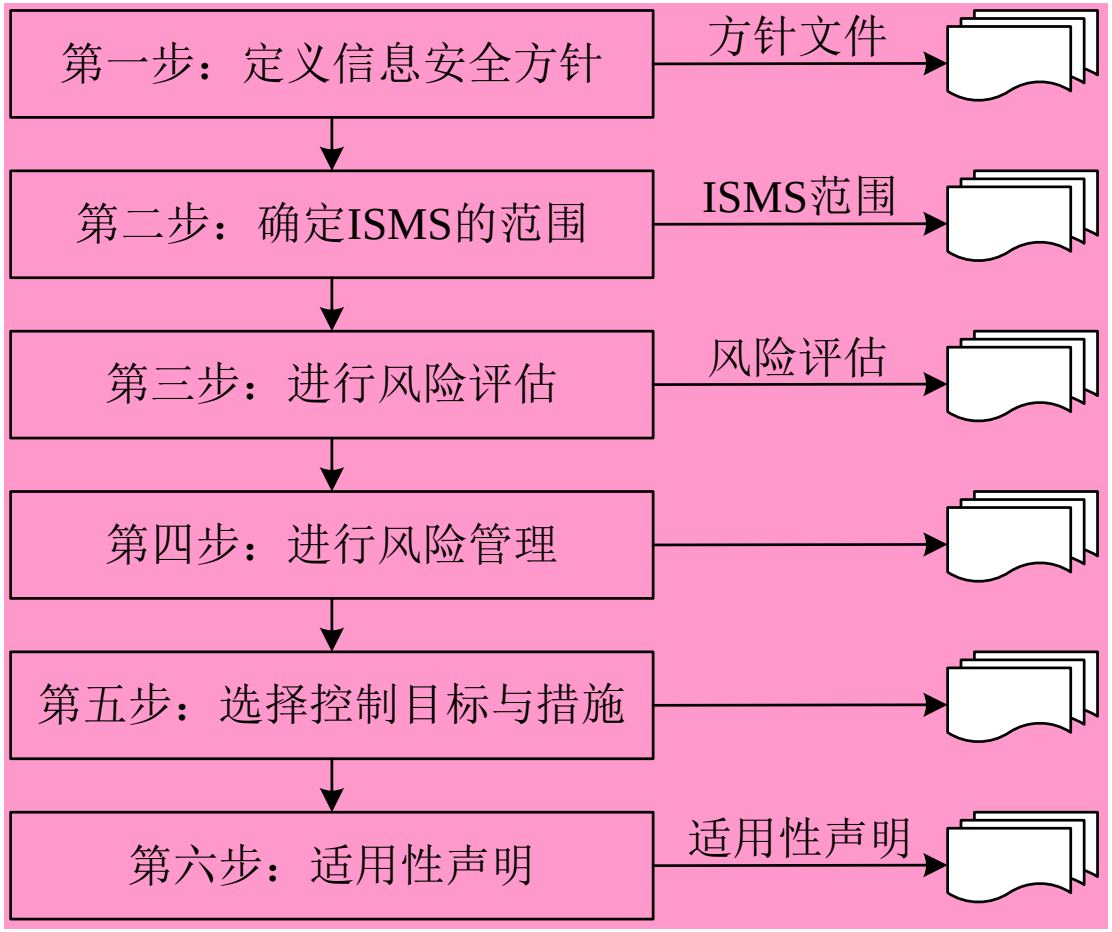
✦BS7799-1：信息安全管理实施细则

控制方面	控制目标	控制措施
安全方针（1，2）	为信息安全提供管理方向和支持	建立安全方针文档，并评审与评价方针
安全组织（3，10）	建立组织内的管理体系，以便安全管理	完善组织结构，控制组织内部信息安全，保证被第三方访问的设施和信息资产安全，进行外部信息安全评审，确保外包合同安全
资产分类与控制（2，3）	维护组织资产的适当保护系统	制定资产清单，进行信息标签分类，确保信息资产受到适当保护
人员安全（3，10）	减少人为造成的风险	减少错误、盗窃、滥用等造成的风险，进行教育培训，完善事故反应机制，总结教训，奖罚并用
物理与环境安全（3，13）	防止未许可的介入、损伤和干扰服务	阻止对工作区和物理设备的非法进入，防止资产的丢失、损坏或泄露造成业务活动的中断，桌面与屏幕管理阻止信息的泄露
通信和运营管理（7，24）	保证通信和操作设备的正确和安全	确保信息处理设备的正确与安全操作，减少系统失效风险，保持软件和信息的完整性，保持信息处理和通信的完整性和有效性，确保网络中信息及其支持系统的安全，防止资产损坏和业务活动中断，防止组织间在交换信息时发生信息丢失、更改和误用
访问控制（8，31）	控制对业务信息的访问	控制信息访问，防止非授权访问设备、计算机、系统及信息，保护网络服务，检测非法行为，确保使用移动式计算和远程工作设施时的信息安全
系统开发与维护（5，18）	保证系统开发与维护的安全	确保安全性深入到操作系统中，防止应用系统用户数据的丢失、修改或误用，保护信息的保密性、完整性和可靠性，保证IT方案及其支持活动以安全的方式进行，维护应用系统软件和信息的安全
业务持续性管理（1，5）	防止商业活动中断和事故的影响	防止业务活动的中断，并保护关键业务过程不受重大事故或灾难影响
法律符合性（3，11）	避免任何违反法律法规、合同等行为	避免与有关法律法规或合同约定事项相抵触，确保安全体系按安全方针及标准执行，将系统的审核效果最大化，并使其影响最小化

6.2 信息安全管理标准

BS 7799

- BS7799-2：信息安全管理体系规范



6.2 信息安全管理标准

BS 7799

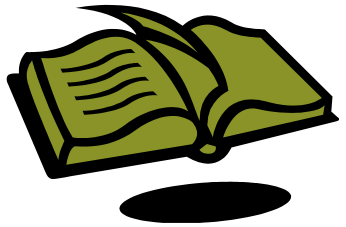
✦引入BS7799的好处：

- 通过认证能向客户、竞争对手、投资商、供应商等展示在其行业中的领导地位。
- 定期监督审核能加强系统的安全性，减少系统故障和潜在的风险隐患，节约资源。
- 通过认证相当于是一种承诺，能提高企业的信誉度，增强客户购买或投资的信心。
- 能够向政府及行业主管部门证明企业对相关法律法规的符合性。
- 可以改善企业的业绩，消除不信任感，有利于拓展市场与业务。
- 获得国际认可的认证证书，能得到国际上的承认。

6.3 信息安全管理体系简介

信息安全管理体系

- 信息安全管理体系（ISMS），是组织在一定范围内建立的信息安全方针和目标，以及为实现这些方针和目标所采用的方法和文件体系。
- ISMS的实施依据:

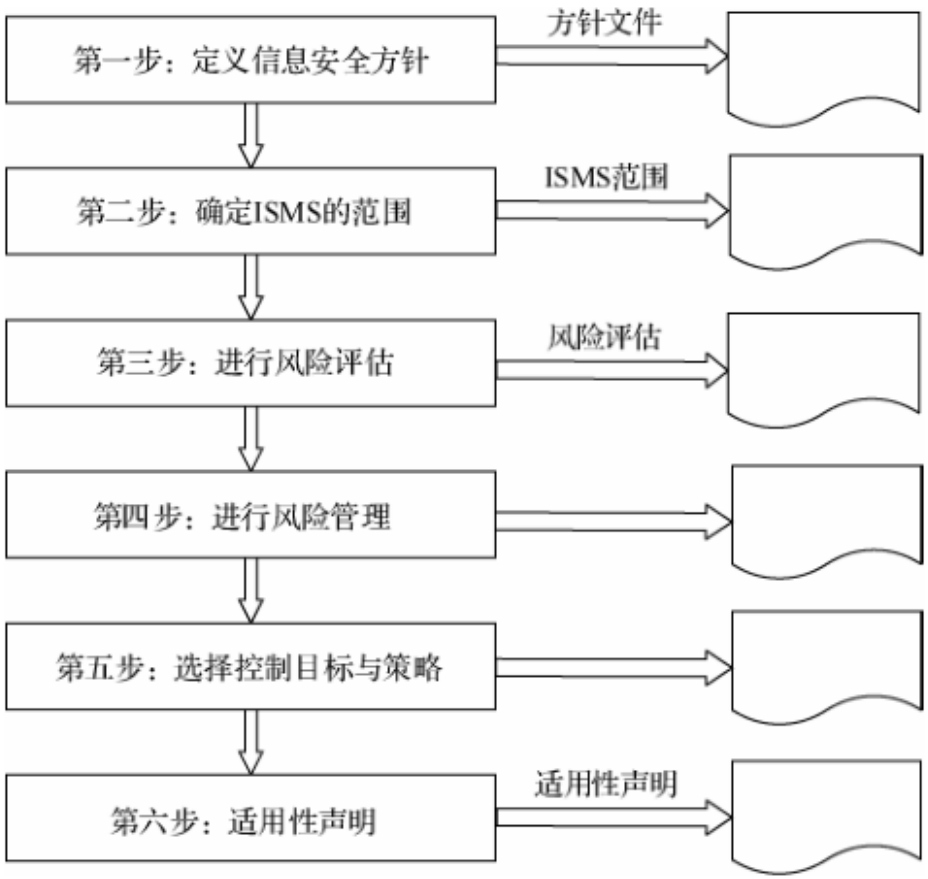


  - BS 7799-2(ISO/IEC 17799)
  - ISO/IEC 27001：2005《信息技术-安全技术-信息安全管理体系要求》
  - GB/T 22080《信息技术-安全技术-信息安全管理体系要求》

6.3 信息安全管理体系简介

信息安全管理体系

✦信息安全管理体系规范



6.3 信息安全管理体系简介

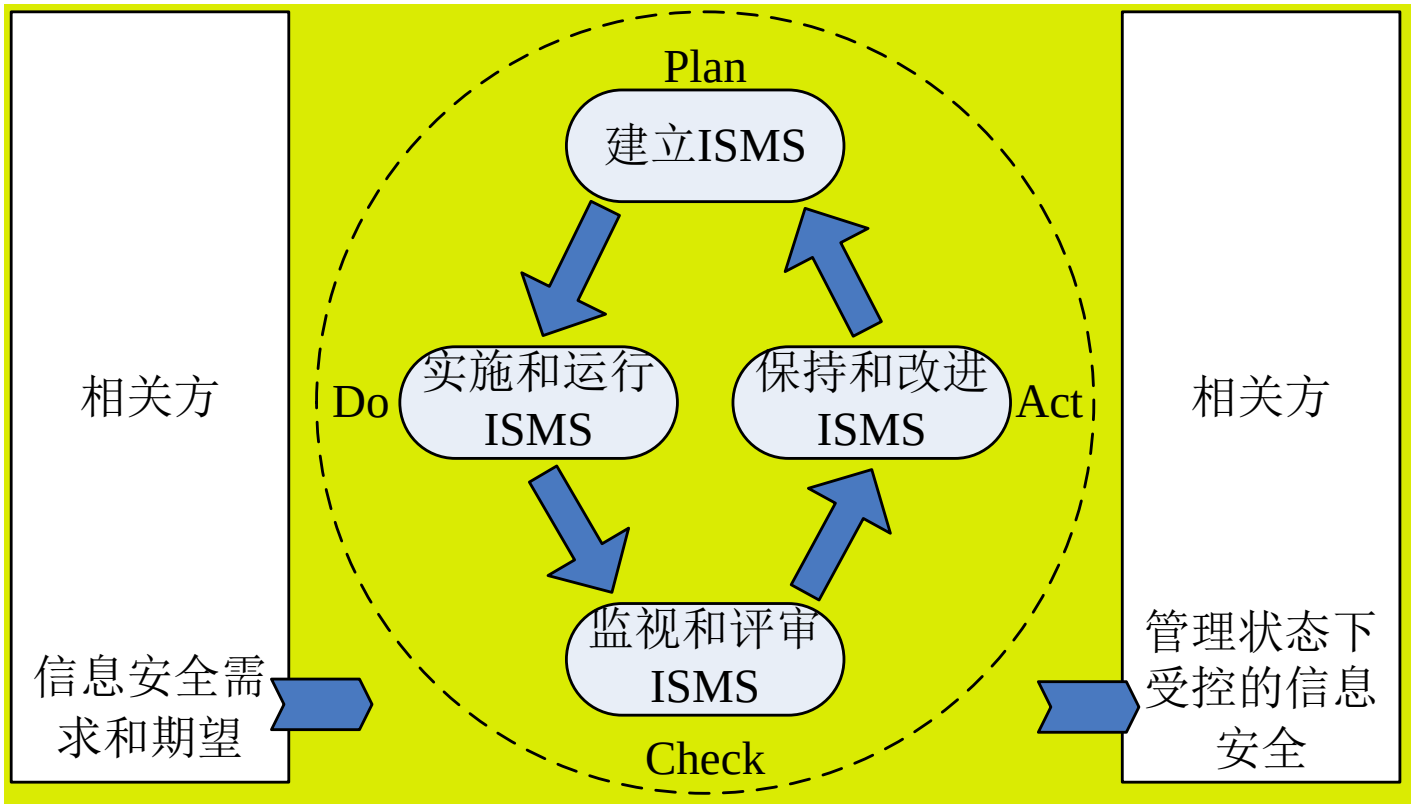
ISO与IEC

- ISO：International Organization for Standardization（国际标准化组织）
- IEC：International Electrotechnical Commission（国际电工委员会）
- 共同点：使用共同的技术工作导则，遵循共同的工作程序。
- 区别：工作模式的不同。

6.3 信息安全管理体系简介

PDCA（戴明环）循环模型：

- “规划（Plan）-实施（Do）-检查（Check）-处置（Act）”



6.3 信息安全管理体系简介

信息安全管理体系的特点

- 强调基于系统、全面和科学的风险评估，体现以预防控制为主的思想。
- 强调全过程的动态控制，达到控制成本与风险的平衡。
- 强调关键资产的信息安全保护，保持组织的竞争优势和运作持续性。

6.4 信息安全管理体系过程

- 信息安全管理体系的准备
- 信息安全管理体系的建立
- 信息安全管理体系的实施和运行
- 信息安全管理体系的监视和评审。
- 信息安全管理体系的保持和改进。
- 信息安全管理体系的认证。

6.4 信息安全管理体系过程

信息安全管理体系的准备

- 组织与人员建设。
- 工作计划制定。
- 能力要求与教育培训。
- 信息安全管理体系文件。

6.4 信息安全管理体系过程

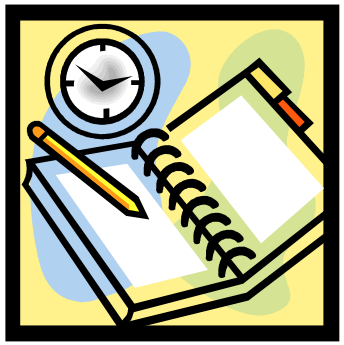
信息安全管理体系的准备

- ✦组织与人员建设。
- ➢ 首先需要建设有效的信息安全组织机构，对相关的各类人员进行角色分配、明确权限并落实责任。
  - ✓ 成立信息安全委员会。
  - ✓ 组建信息安全管理推进小组。
  - ✓ 保证有关人员的职责和权限得到有效地明确。

6.4 信息安全管理体系过程

信息安全管理体系的准备

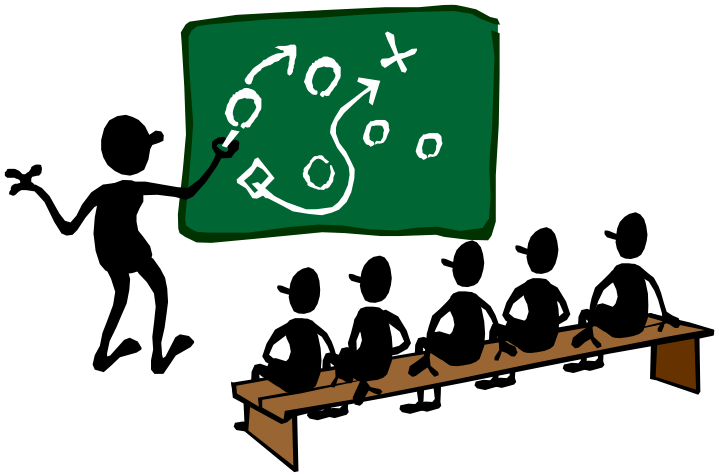
- ✦ 工作计划制定。
- ➢ 制定一个切实可行的工作计划，明确准备、初审、体系设计、实施运行和审核认证等不同阶段的工作任务和目标，以及责任分工，用以控制工作进度，并突出工作重点。
- ➢ 制定计划时,要求：
- ✓ 要充分考虑资源需求。
- ✓ 考虑认证的费用。



6.4 信息安全管理体系过程

信息安全管理体系的准备

- ✦能力要求与教育培训
  - ➢ 人员能力的要求：
    - ✓ 适当的教育。
    - ✓ 适当的培训。
    - ✓ 适当的经历。
  - ➢ 教育培训的要求：
    - ✓ 确定教育与培训的需求。
    - ✓ 编制教育与培训的计划。
    - ✓ 确定教育与培训的内容和方式。



6.4 信息安全管理体系过程

信息安全管理体系的准备

- ✦信息安全管理体系文件。
  - ➢ 信息安全管理体系文件，是按照信息安全管理标准的要求建立管理模型的依据，也是伴随ISMS建设过程产生的一系列的体系文件，即作为管理的依据。
  - ➢ 各种层次的ISMS文件，是建立信息安全管理体系的重要基础性工作，也是ISO/IEC 27001等标准的明确要求。
  - ➢ ISMS文件的作用：
    - ✓ 阐述声明的作用。
    - ✓ 规定和指导的作用。
    - ✓ 记录和证实的作用。

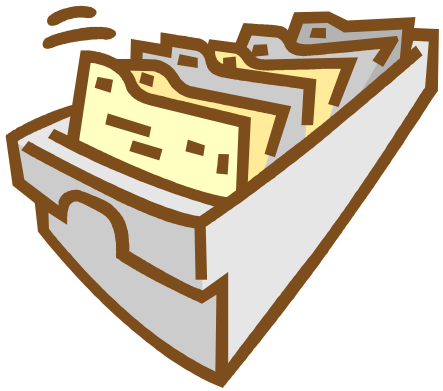
6.4 信息安全管理体系过程

信息安全管理体系的准备

- ✦信息安全管理体系文件。
- ➢ 信息安全管理体系文件，无刻意的描述形式，在具体实施中，为便于运作并具有操作性。

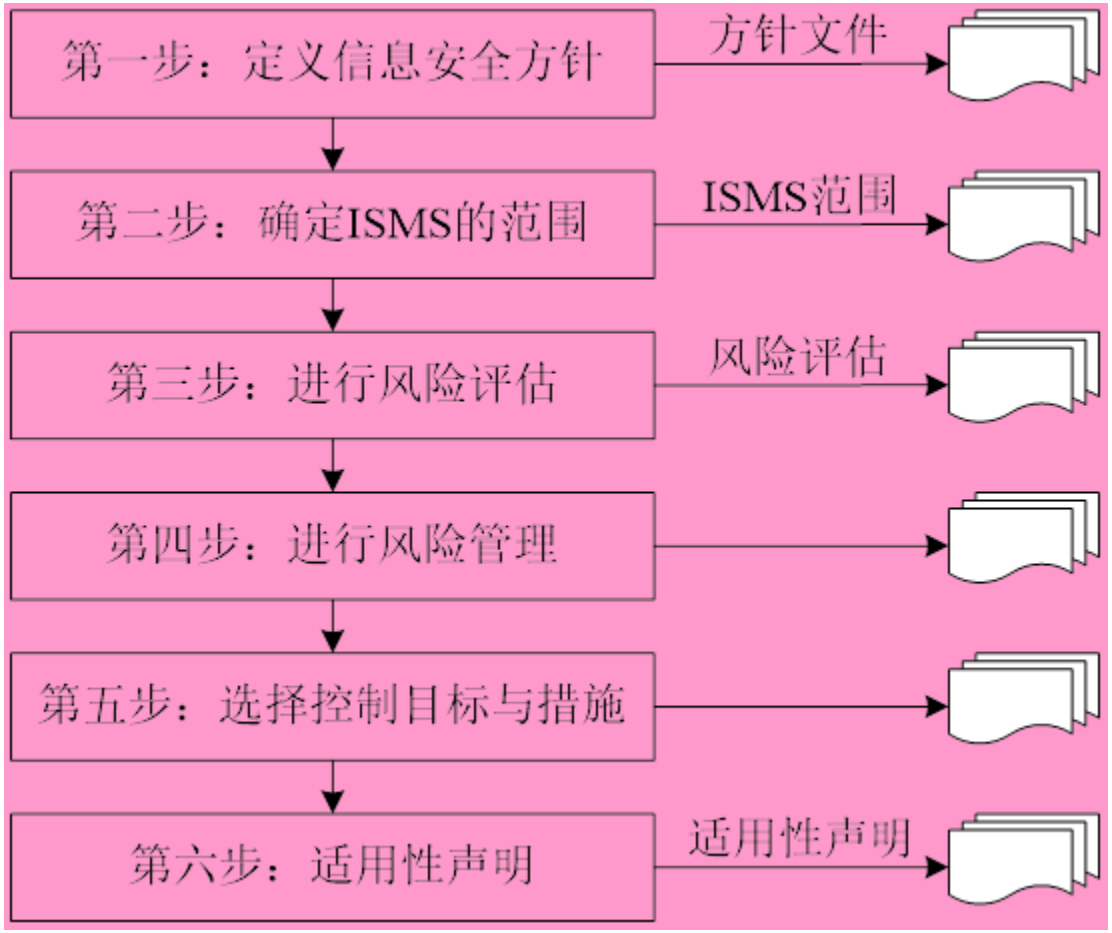
  可把ISMS文件分成以下层次（类型）：

- ✓ 适用性声明(SoA)。
- ✓ ISMS管理手册。
- ✓ 程序文件。
- ✓ 作业指导书。
- ✓ 记录。



6.4 信息安全管理体系过程

信息安全管理体系的建立



6.4 信息安全管理体系过程

信息安全管理体系的建立

- 信息安全管理体系
  - 确定ISMS信息安全方针。
  - 确定ISMS范围和边界。
  - 实施ISMS风险评估。
  - 进行ISMS风险管理。
  - 为处理风险选择控制目标与措施。
  - 准备适用性声明。

6.4 信息安全管理体系过程

信息安全管理体系的建立

- ✦确定ISMS信息安全方针
- ➢ ISMS信息安全方针，是统领整个体系的目的、意图和方向。应语言精炼、简明扼要、易理解和记忆。要求：
- ✓ 包括目标框架和工作的总方向与原则。
- ✓ 考虑法律法规、业务和合同中的安全要求。
- ✓ 在战略性风险管理环境下，建立和保持ISMS。
- ✓ 建立风险评价的准则，定义风险评估的结构。
- ✓ 得到管理层的批准。

6.4 信息安全管理体系过程

信息安全管理体系的建立

✦电子科技大学网络系统ISMS安全方针。

文件名称	电子科技大学网络系统信息安全方针	
编号	电子科技大学网络系统-001	
版本	版本 Version 1.0	
密级	绝密	
文件审定	姓名	部门
	昝浩	网安部
	李泽华	网安部
复核计划	复核时间	复核结果
	2016.12.1	合格
	2016.12.5	合格
目标	提高电子科技大学全体员工的安全意识，积极做好预防工作，贯彻落实安全方针和各项安全措施，保护学校网络安全运行	
适用范围	本信息安全管理方针适用于电子科技大学所有网络相关的业务，以及所有用于保护电子科技大学的信息资产	
相关内容	电子科技大学成立信息安全委员会来领导信息安全工作电子科技大学所有员工都必须接受信息安全的教育培训，提高信息安全意义建立完整的事故处理程序对网络访问进行严格控制定期对本方针进行回顾和评审	
实施时间	本方针自签发之日起，正式实施	

6.4 信息安全管理体系过程

信息安全管理体系的建立

- ✦确定ISMS范围和边界。
- ➢ 根据业务、组织、位置、资产和技术等方面的特性，确定ISMS的范围和边界。
- ➢ 范围确定的标准主要看组织的业务需求，而不是组织的范围有多大，ISMS范围就有多大。考虑：
- ✓ 组织现有部门。
- ✓ 办公场所。
- ✓ 资产状况。
- ✓ 所采用的技术。

6.4 信息安全管理体系过程

信息安全管理体系的建立

- ✦实施ISMS风险评估。
- ➢ 风险评估为控制目标与控制措施的选择提供依据，也是对安全控制的效果进行测量和评价的主要方法。
- ➢ 风险评估是对信息和信息处理设施的威胁、影响和脆弱点及三者发生的可能性评估，即利用适当的风险评估工具，包括定性和定量的方法，确定资产风险等级和优先控制顺序等。
- ➢ 风险评估的过程：
- ✓ 风险识别。
- ✓ 风险评估。

6.4 信息安全管理体系过程

信息安全管理体系的建立

- ✦实施ISMS风险评估——风险识别。
  - ➢ 风险识别是风险管理的第一步，也是风险管理的**基础**。
  - ➢ 风险识别是指在风险事故发生之前，人们运用各种方法系统的、连续的认识所面临的各种风险以及分析风险事故发生的**潜在原因**。
  - ➢ 风险识别的范围：
    - ✓ ISMS范围内的信息资产及其估价，以及资产负责人。
    - ✓ 信息资产面临的威胁，以及威胁发生的可能性与潜在影响。
    - ✓ 可被威胁利用的脆弱性，以及被利用的难易程度。

6.4 信息安全管理体系过程

信息安全管理体系的建立

- 实施ISMS风险评估——风险评估。
  - 评估因安全故障或失效而可能导致的业务损害，考虑因资产的机密性、完整性、可用性等的损失而导致的潜在后果。
  - 评估与这些资产相关的主要威胁、脆弱性和影响造成此类事故发生的现实可能性，以及已经实施的安全控制措施。
  - 测量风险的大小，并确定优先控制等级。
  - 根据风险接受准则，对风险评估结果进行评审，判断风险是否可接受或需要处理。

6.4 信息安全管理体系过程

信息安全管理体系的建立

- 进行ISMS风险管理。
  - **接受**风险。
  - **避免**风险。
  - **降低**风险。
  - **转移**风险。

6.4 信息安全管理体系过程

信息安全管理体系的建立

- 为处理风险选择控制目标与措施。
- 组织应根据信息安全风险评估的结果，针对具体风险，制定相应的控制目标，并实施相应的控制措施。
- 选择应当由安全需求来驱动，并基于最好的满足安全需求，同时要考虑风险平衡与成本效益的原则，并具有可实施性，对所选择的控制目标和控制措施要及时加以校验和调整，以适应不断变化的情况，使信息资产得到有效的、经济的、合理的保护。

6.4 信息安全管理体系过程

信息安全管理体系的建立

- ✦准备适用性声明(SoA文件)。
- ➢ SoA文件记录了风险控制目标和针对各风险所采取的控制措施，并包括这些控制措施是否被选择的原因。
- ➢ SoA文件向内部员工和外界均声明了对风险的态度。

控制（ISO/IEC 27001附录A）	是否选择	说明
A.5.1.1 信息安全方针文件	是	参见《XXX公司信息安全方针》，编号：XXX-001
A.10.10.3 日志信息的保护	是	在系统出现异常或故障时，利用日志信息追溯原因时非常重要。使用适当的方法保护记录日志的设施和日志信息，是实施的基本控制手段之一
A.11.4.2 外部连接的用户鉴别	是	外部用户通过Internet访问公司内部网自主办理业务，具有高风险性。使用适当的鉴别方法控制远程用户的访问，这是实施的基本控制手段之一
……	……	……
A.15.3.2 信息系统审计工具的保护	否	公司没有这类保护要求，这项控制不适用

6.4 信息安全管理体系过程

信息安全管理体系的实施和运行

- ISMS的规范建立和有效运行时实现信息安全保障的有效手段。
- 经过审核与批准并发布实施后进入运行阶段。
- 运行ISMS，要在实践中体验其充分性、适用性和有效性，并不断完善ISMS。
- 实施ISMS，必须充分考虑各种因素，如宣传贯彻、实施监督、考核评审、信息反馈与及时改进等，还要考虑实施的培训费、报告费等各项费用，以及解决员工工作习惯的冲突、不同机构/部门之间的协调等问题。

6.4 信息安全管理体系过程

信息安全管理体系的实施和运行

- 具体实施和运行ISMS过程中，应做好以下工作：
- 做好动员与宣传。（全体员工会议）
- 实施培训和意识教育计划。（目标、方式、记录、归档）
- 制定与实施风险处置计划。（制定风险处置计划，达到控制目标）
- 实施所选择的控制措施，并评价其有效性。
- 管理ISMS的运行。（管理资源、运行的信息）
- 保持ISMS的持续有效。（监视和审核）

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- 监视和评审过程。
  - 执行监视、评审规程和其他控制措施。
  - 定期评审ISMS的有效性。
  - 测量控制措施的有效性，验证安全要求是否被满足。
  - 定期进行风险评估的评审，以及对残余风险和已确定的可接受的风险级别进行评审。
  - 定期进行ISMS内部审核和管理评审。

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 内部审核。
- 内部审核要确定ISMS的控制目标、控制措施、过程和程序是否达到如下要求：
  - ✓ 符合标准，以及相关法律法规的要求。
  - ✓ 符合已识别的信息安全要求，例如安全目标、安全漏洞、风险控制等。
  - ✓ 得到有效地实施和保持。
  - ✓ 按期望运行。

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 内部审核。
  - 最终的内部审核报告，应是正式的，内容包括审核的目的及范围、审核准则、审核部门及负责人、审核组成员、审核时间、审核情况、审核结论、分发范围等。

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 内部审核——示例

XXX 公司信息安全管理体系审核报告

一、审核目的

对 XXX 公司现有的信息安全管理体系作全面审核，了解其信息安全管理体系运行的有效性和符合性，评价其是否具备申请 ISO/IEC 27001 认证的条件。

二、审核范围

ISO/IEC 27001 所要求的相关活动及所有相关职能部门。

三、审核准则

1、ISO/IEC 27001 标准。

2、ISMS 信息安全手册、程序文件及其他相关文件。

3、组织适用的 ISMS 法律法规及其他要求。

四、审核组成员

审核组长：马 XX

审核员：刘 XX、李 XX、谢 XX、林 XX、张 XX

五、审核时间

2012 年 2 月 13-2012 年 2 月 15 日

6.4 信息安全管理体系过程

✦ISMS 内部审核——示例

六、审核概况

按公司计划，审核组 6 人于 2012 年 2 月 13 日开始进行了为期 3 天的现场审核。

审核组检查了公司信息安全管理体系有关的各个部门，包括信息中心、研发部、技术服务总、市场部、行政人事部、财务部等，查看了公司的各生产现场和设施，并同总经理、信息安全管理经理、部门主管和普通员工等 20 余人进行了交谈，对所有 ISO/IEC 27001 的要求进行了抽样取证。

通过检查，审核组发现，XXX 公司的信息安全管理体系在文件规定和实际行动方面已按照 ISO/IEC 27001 标准的要求建立起来了，但各部门对 ISO/IEC 27001 标准、程序文件的熟悉方面尚存在一定的差距，需要进一步完善和提高，例如：……，这些不符合已得到责任部门的确认，详细见附件 1。

需要指出的是，审核是抽样的，可能有些实际存在的问题未被发现，……。各部门要按 ISO/IEC 27001 标准和公司信息安全管理体系要求进行自查和措施改进。

七、审核结论

1、XXX 公司的信息安全管理体系运行有效，具体表现在：……。

2、XXX 公司的信息安全管理体系基本符合 ISO/IEC 27001 的标准要求。

4、审核组建议：XXX 公司在 30 天内对本次审核提出的不符合项目完成纠正后，可以申请 ISO/IEC 27001 的正式认证。

八、本报告分发范围

1、正、副总经理、信息安全管理经理、信息中心

2、受审核部门成员

3、审核组成员

九、附件

1、XXX 公司信息安全管理体系审核不符合报告。

2、审核会议纪录。

审核组长：马 XX

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 管理评审。
  - 组织的最高管理者应该按照计划的时间间隔（至少每年一次）评审信息安全管理体系，以确保其持续的适宜性、充分性和有效性。
  - 管理评审过程，应确保收集到必要的信息，以供管理者对包括ISMS改进的机会和变更的需要，以及安全方针和安全目标等在内进行评价，评审结果应清楚地写入文件，并保持记录。

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 管理评审。
- 管理评审的时机：
- 一般每年做一次管理评审，有的认证机构每半年有一次监督审核，因此企业每六个月做一次管理评审。但若发生以下情况，应适时进行管理评审：
- ✓ 在进行第三方认证之前。
- ✓ 企业内、外部环境发生较大变化时。
- ✓ 新的ISMS进行正式运行时。
- ✓ 其他必要的时候，如发生重大信息安全事故时。

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 管理评审。
- 管理评审的输入：
  - ✓ ISMS审核和评审的结果。
  - ✓ ISM方针、风险控制目标和控制措施的实施情况。
  - ✓ 事故、事件的调查处理情况。
  - ✓ 纠正和预防措施的实施情况。
  - ✓ 相关方的投诉、建议等反馈。

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 管理评审。
- 管理评审的输入：
  - ✓ 用于改进ISMS业绩和有效性的技术、产品或程序。
  - ✓ 对于法律法规及其他要求的符合性报告。
  - ✓ 关于ISMS运行的有效性测量报告。
  - ✓ 风险评估报告，以及已采取措施的跟踪报告。
  - ✓ 任何可能影响ISMS变更的因素。
  - ✓ 改进的建议。

6.4 信息安全管理体系过程

信息安全管理体系的监视和评审

- ISMS 管理评审。
- 管理评审的输出：
  - ✓ ISMS的适宜性、充分性和有效性的测量结论。
  - ✓ 组织机构是否需要调整。
  - ✓ 信息安全方针、控制目标、控制措施、风险等级和风险接受准则是否需要修改。
  - ✓ 更新风险评估和风险处置计划。
  - ✓ 资源配置是否充足，是否需要调整。
  - ✓ 改进测量控制措施有效性的方式。

6.4 信息安全管理体系过程

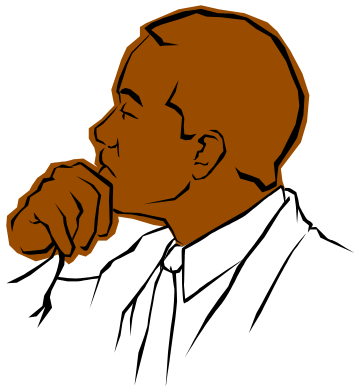
信息安全管理体系的监视和评审

	ISMS内部审核	ISMS管理评审
目的	确保ISMS运行的符合性、有效性	确保ISMS持续的适宜性、充分性、有效性
依据	ISO/IEC 27001标准、体系文件、法律法规	法律法规、期望值、内部审核的结论
结果	提出纠正措施并跟踪实现	改进ISMS，提高管理水平
执行者	与审核领域无直接关系的审核员	最高管理者

6.4 信息安全管理体系过程

信息安全管理体系的保持和改进

- 针对与ISMS要求不符合应实施纠正措施、改进措施和预防措施等。
- 保持和改进就是要实施这些措施。其中改进措施主要通过纠正与预防性控制措施来实现，同时对潜在的不符合采取预防性控制措施。



6.4 信息安全管理体系过程

信息安全管理体系的保持和改进

- ✦纠正措施
- ➢ 纠正措施应形成文件，并规定以下方面的要求：
- ✓ 识别在实施和运行ISMS过程中的不符合因素。
- ✓ 确定这些不符合因素的原因。
- ✓ 对确保这些不符合不再发生所需的措施进行评价。
- ✓ 确定和实施所需要的纠正措施，并记录结果。
- ✓ 评审所采取的纠正措施。

6.4 信息安全管理体系过程

信息安全管理体系的保持和改进

- ✦预防措施
- ➢ 预防措施应形成文件，并规定以下方面的要求：
- ✓ 识别潜在的不符合因素的原因。
- ✓ 对预防这些不符合因素发生所需的措施进行评价。
- ✓ 确定和实施所需要的预防措施，并记录结果。
- ✓ 评审所采取的预防措施。
- ✓ 识别发生变化的风险，并通过关注变化显著的风险来识别预防措施的要求。
- ✓ 根据风险评估的结果来确定预防措施的优先级。

6.4 信息安全管理体系过程

信息安全管理体系的保持和改进

- 修正不符合项
  - 对于轻微的不符合，可采取口头纠正和辅导，不必采取更进一步的纠正与预防措施。
  - 对于严重的不符合，应积极采取补救措施，下达纠正与预防措施任务给相关责任部门，并要求在规定的时间内完成相关原因分析和确定纠正与预防措施后回传，以减少或消除其不利影响。

6.4 信息安全管理体系过程

信息安全管理体系的保持和改进

✦修正不符合项——纠正与预防不符合的措施表

下达纠正与预防措施：
（1）不符合项的来源：
（2）不符合项事实的陈述：
（3）不符合项信息严重性评价：
（4）纠正与预防措施任务的下达：
责任部门：
时间要求：
建议的纠正与预防措施：
填写人/日期：　　审核人/日期：　　信息安全管理经理/日期：

制定纠正与预防措施：
（1）不符合项的原因：
（2）纠正与预防措施任务的制定：
责任人：
预定完成日期：__年__月__日
制定的纠正与预防措施：
编制人/日期：　　审核人/日期：　　信息安全管理经理/日期：

验证纠正与预防措施：
☐ 已按期在__年__月__日完成，效果简述：
☐ 未按期完成，推迟至__年__月__日完成，推迟原因：
☐ 其他：
验证人/日期：　　核实人/日期：

6.4 信息安全管理体系过程

信息安全管理系统的认证

- 按照ISO和IEC的定义，认证（Certification）是由国家认可的认证机构证明一个组织的产品、服务、管理体系等符合相关标准、技术规范（TS）或其强制性要求的合格评定活动。
- 认证的基础是标准。
- 认证的方法包括对产品的特性抽样检验和对组织体系的审核与评定。
- 认证的证明方式是认证证书与认证标志。

6.4 信息安全管理体系过程

信息安全管理系统的认证

- 认证标准：ISO/IEC 27001：2005《信息技术-安全技术-信息安全管理体系要求》。该标准适用于所有类型的组织（例如商业企业、政府机构、非赢利组织）。
- 实施认证：根据ISO/IEC 27001标准，建立完整的信息安全管理体系，达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式，用最低的成本，达到可接受的信息安全水平，并从根本上保证业务的持续性。

6.4 信息安全管理体系过程

信息安全管理系统的认证

- ISMS认证的目的
  - 节约信息安全成本，增强客户、合作伙伴等相关方的信心和信任，提高组织的公众形象和竞争力。
  - ✓ 使组织获得最佳的信息安全运行方式。
  - ✓ 保证组织业务的安全。
  - ✓ 降低组织业务风险、避免组织损失。
  - ✓ 保持组织核心竞争优势。

6.4 信息安全管理体系过程

信息安全管理系统的认证

- ISMS认证的目的
  - ✓ 提供组织业务活动中的信誉。
  - ✓ 增强组织竞争力。
  - ✓ 满足客户要求。
  - ✓ 保证组织业务的可持续发展。
  - ✓ 使组织更加符合法律法规的要求。

6.4 信息安全管理体系过程

信息安全管理系统的认证

- ✦认证的前期工作
  - ➢ 确定认证范围：信息安全管理体系涉及的范围。
  - ➢ 检查基本条件。
    - ✓ 遵循相关法律法规的努力已得到相关机构的认可。
    - ✓ 当前的ISMS已被有效实施运行3个月以上。
    - ✓ ISMS运行期间及建立体系前的一年内未受到主管部门行政处罚。
  - ➢ 寻求信息安全管理体系认证机构。

6.4 信息安全管理体系过程

信息安全管理系统的认证

- 认证的前期工作——认证机构

6.4 信息安全管理体系过程

信息安全管理系统的认证

- 认证的前期工作——认证机构
- IAF:多边合作组织，协调各国认证认可制定，通过统一规范各成员单位的审核员资格要求、认证标准及管理体系认证机构的评定和认证程序，在技术运作上保持一致，确保有效的国际互认。
- 中国合格评定国家认可委员会（CNAS）:China National Accreditation Service for Conformity Assessment检查基本条件。
- 中国信息安全认证中心（ISCCC）:China Information Security Certification Center 。

6.4 信息安全管理体系过程

信息安全管理系统的认证

✦认证的前期工作——中国国家认证认可监督管理委员会

查询结果

序号	机构类别	批准号	机构名称	联系电话	邮编	证书有效期
1	认证	CNCA-R-2002-001	中国质量认证中心	010-83886666	100070	2014-12-10
2	认证	CNCA-R-2002-003	上海质量体系审核中心	021-52387700（总机），52389950	200050	2014-12-10
3	认证	CNCA-R-2002-005	中国船级社质量认证公司	010-65239001	100006	2014-12-10
4	认证	CNCA-R-2002-008	中国新时代认证中心	010-64642970	100028	2014-12-10
5	认证	CNCA-R-2002-011	北京赛西认证有限责任公司	010-64007810	100007	2014-12-10
6	认证	CNCA-R-2002-012	广州赛宝认证中心服务有限公司	020-87236606	510610	2014-12-10
7	认证	CNCA-R-2002-016	北京新世纪认证有限公司	010-58561802	100035	2014-12-10

共11 条 当前 1/2页 首 页 上一页 下一页 尾页 跳转到第 页 跳转

查询结果

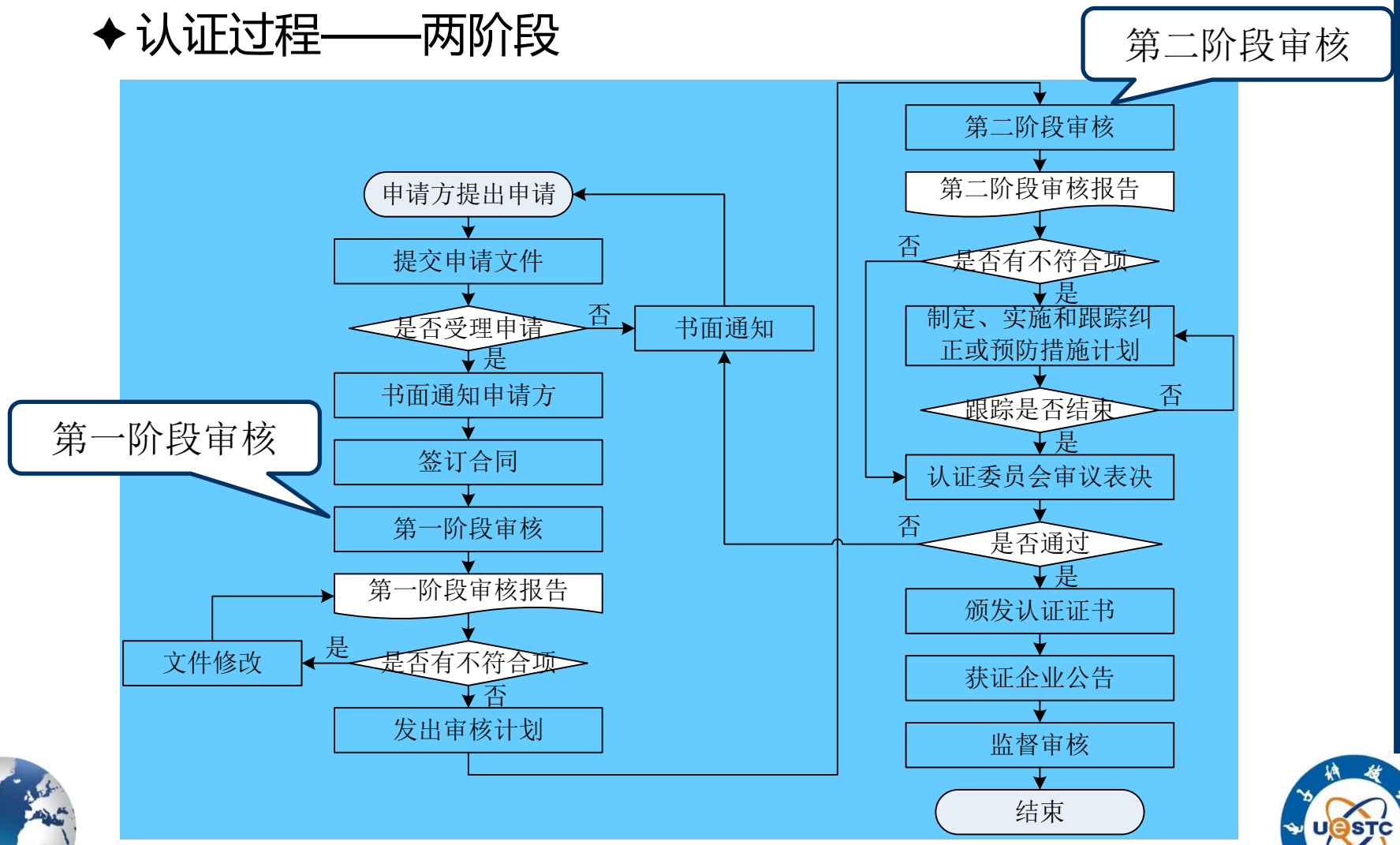
序号	机构类别	批准号	机构名称	联系电话	邮编	证书有效期
8	认证	CNCA-R-2002-021	华夏认证中心有限公司	010-62335102	100083	2014-12-10
9	认证	CNCA-R-2007-138	中国信息安全认证中心	010-65994357	100088	2015-01-28
10	认证	CNCA-RF-2003-27	上海挪华威认证有限公司（挪威DNV设立认证机构）	021-32084518；021-58818903；010-65627888	200336	2013-05-29
11	认证	CNCA-RF-2008-17	英标管理体系认证（北京）有限公司（英国BSI设立认证机构）	010-65157060	100004	2012-12-17

共11 条 当前 2/2页 首 页 上一页 下一页 尾页 跳转到第 页 跳转

6.4 信息安全管理体系过程

信息安全管理系统的认证

✦认证过程——两阶段



6.4 信息安全管理体系过程

信息安全管理系统的认证

- ✦认证过程——两阶段
- ➢第二个阶段审核结论情况
- ✓信息安全管理体系已建立、运行有效，无严重不符合项和轻微不符合项，同意推荐认证通过。
- ✓信息安全管理体系已建立并正常运行，审核过程中发现少量轻微不符合项或个别严重不符合项，要求组织在规定的时间内实施纠正措施，同意在验证纠正措施的实施后推荐认证通过。
- ✓信息安全管理体系存在缺陷，发现较多不符合项，需要在实施纠正措施后安排复审，本次不予推荐认证通过。

6.4 信息安全管理体系过程

信息安全管理系统的认证

- 认证过程——认证的维持
  - 在组织通过审核并获得认证证书后，认证并非结束。认证机构将通过执行每年至少一次的监督审核，继续监控ISMS符合标准的情况。这期间如果组织未能持续满足认证要求，认证机构将公告撤销其认证证书。
  - 认证证书的有效期一般为3年。
  - 被审核方有义务通知认证机构所发生的可能影响到系统或证书的变更。

6.4 信息安全管理体系过程

✦ISMS认证案例

信息安全管理体系认证证书名称

证书注册号

获得证书的组织名称

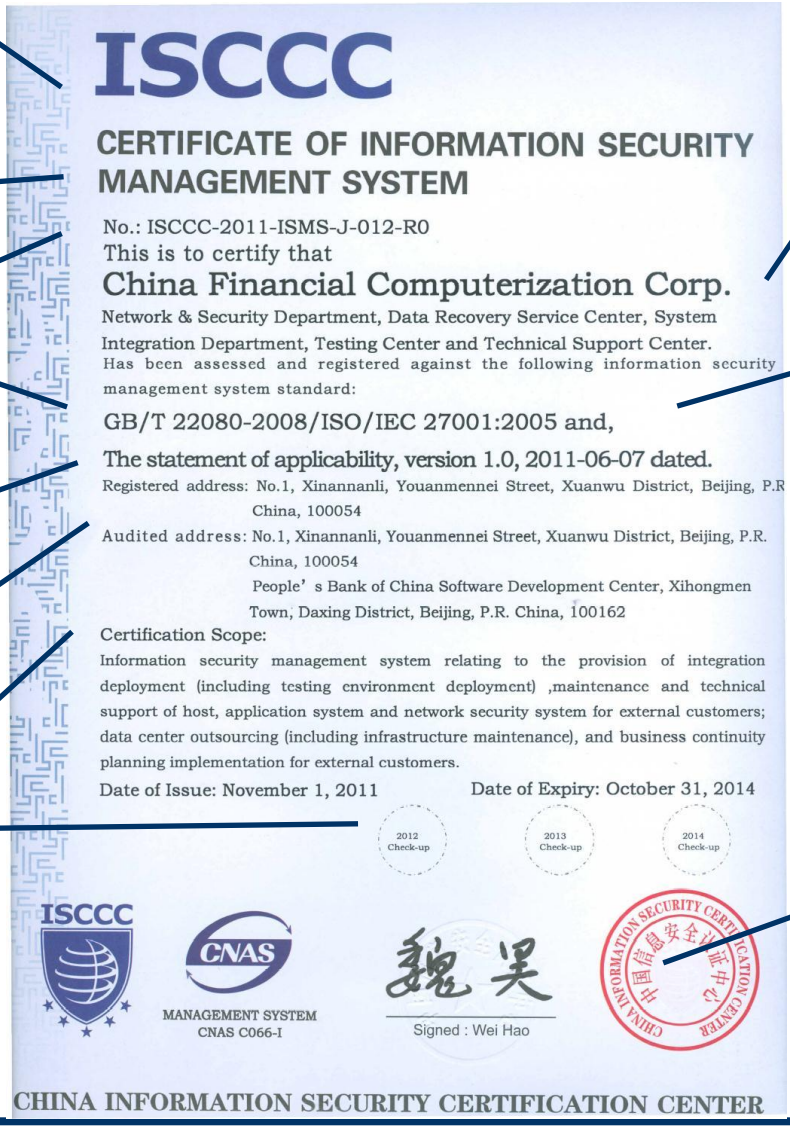
适用性声明和版本描述

注册地址

审计地址

证书覆盖的认证范围

年度审核



ISCCC

CERTIFICATE OF INFORMATION SECURITY MANAGEMENT SYSTEM

No.: ISCCC-2011-ISMS-J-012-R0

This is to certify that

China Financial Computerization Corp.

Network & Security Department, Data Recovery Service Center, System Integration Department, Testing Center and Technical Support Center.

Has been assessed and registered against the following information security management system standard:

GB/T 22080-2008/ISO/IEC 27001:2005 and,

The statement of applicability, version 1.0, 2011-06-07 dated.

Registered address: No.1, Xinannanli, Youanmennei Street, Xuanwu District, Beijing, P.R China, 100054

Audited address: No.1, Xinannanli, Youanmennei Street, Xuanwu District, Beijing, P.R. China, 100054

People's Bank of China Software Development Center, Xihongmen Town, Daxing District, Beijing, P.R. China, 100162

Certification Scope:

Information security management system relating to the provision of integration deployment (including testing environment deployment) ,maintenance and technical support of host, application system and network security system for external customers; data center outsourcing (including infrastructure maintenance), and business continuity planning implementation for external customers.

Date of Issue: November 1, 2011

Date of Expiry: October 31, 2014

2012 Check-up

2013 Check-up

2014 Check-up

ISCCC

CNAS

MANAGEMENT SYSTEM CNAS C066-I

Signed : Wei Hao

CHINA INFORMATION SECURITY CERTIFICATION CENTER

相关的业务功能、流程与活动

关于信息安全系统满足相关认证标准的声明

证书的有效期

认证机构的标志、印章、签名

小 结

1. ISMS实施过程采用了PDCA模型，实施依据是BS 7799-2、ISO/IEC 27001或GB/T 22080等标准。
2. 在建设ISMS之前，要做好相关的组织与人员建设、制定好工作和教育培训计划等工作。
3. 建立ISMS要建立ISM框架，确定方针和系统范围，进行风险分析，选择控制目标与措施，进行适用性声明等步骤。
4. 在实施和运行ISMS时，要注意宣传、协调和反馈。
5. 在监视和评审ISMS时，强调内部审核和管理评审。
6. 在保持和改进ISMS时，实施纠正与预防等控制。
7. ISMS的认证。

作 业

1. 什么是信息安全管理，为什么要实行信息安全管理?
2. 信息安全管理应遵循的原则有哪些?
3. 简要介绍信息安全管理模型的内容。
4. BS7799 准则的主要内容是什么?
5. 信息安全管理体系的过程包含哪些内容?

作 业

6．简要概述 PDCA 的过程内容。

7．如何确定 ISMS 的安全方针?

8．如何修正 ISMS 内容中的不符合项?

9．如何进行 ISMS 的内部审核与管理评审?

10．为什么要进行信息安全管理体系的认证?

实 验

实验三　信息安全方针的建立

实验四　ISMS 管理评审