第2章 信息安全管理体系

信息安全管理

主讲 李章兵

教学内容

- 2.1 ISMS概述
- 2.2 信息安全管理标准的发展史
- 2.3 信息安全管理标准介绍
- 2.4 BS7799体系
- 2.5 基于SSE-CMM的ISMS
- 2.6 ISO/IEC 27001:2005标准

教学目标

- 本章的重点
  - ISMS概念与建立步骤
  - PDCA模型
  - 我国信息安全管理标准
  - ISMS体系与作用范围
    - BS7799与管理框架
    - SSE-CMM与安全过程
    - ISMS 27000与核心内容、十大管理要项、建立过程

2.1信息安全管理体系概述

- **1. ISMS定义**
  - 信息安全管理体系（**Information Security Management System，ISMS**）是组织在整体或特定范围内建立的信息安全方针和目标，以及完成这些目标所用的方法和手段所构成的体系。
  - **ISMS的范围包括：**
    - 组织的所有信息系统；
    - 组织的部分信息系统；
    - 特定的信息系统。

2.1信息安全管理体系概述

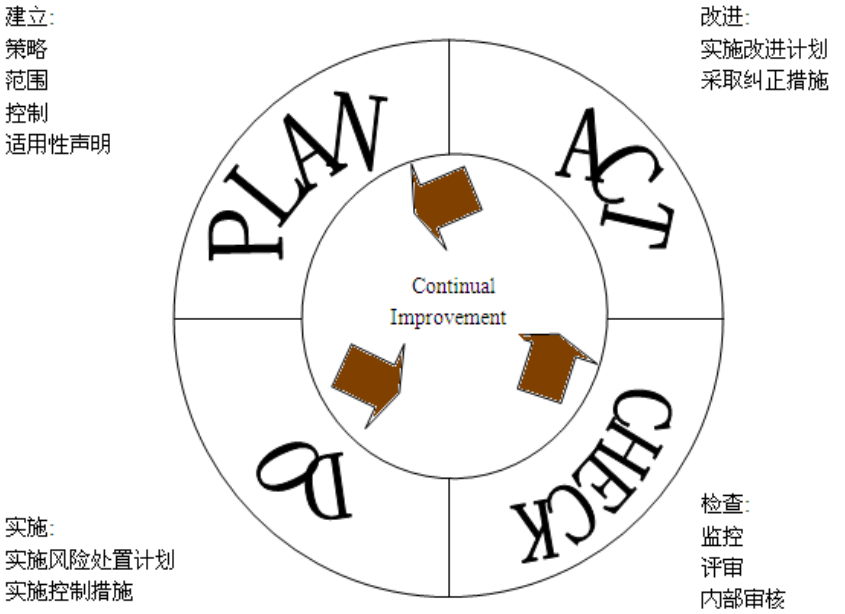
- **2. ISMS作用与特点**
  - **ISMS作用**
    - 强化员工的信息安全意识，规范组织信息安全行为；
    - 促使管理层贯彻信息安全保障体系；
    - 对关键信息资产进行全面系统的保护，维持竞争优势；
    - 确保业务持续开展并将损失降到最低程度；
    - 使组织的生意伙伴和客户对组织充满信心；
    - 如果通过体系认证，可以提高组织的知名度与信任度。
  - **ISMS特点**
    - 以预防控制为主的思想；
    - 强调合规性；
    - 强调全过程和动态控制；
    - 关注关键性信息资产。

2.1信息安全管理体系概述

- **3.建立ISMS的步骤：**
  - 信息安全管理体系的策划与准备
  - 信息安全管理体系的文件编制
  - 建立信息安全管理框架
  - 信息安全管理体系的运行
  - 信息安全管理体系的审核与评审

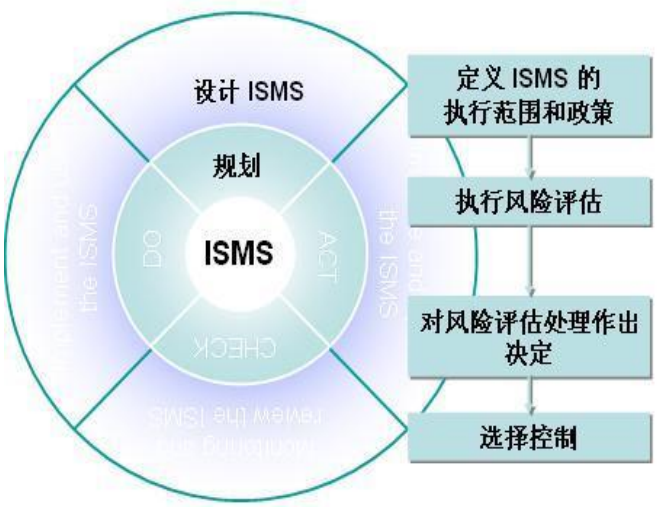
2.1信息安全管理体系概述

- **4. PDCA模型（戴明环）**
  - **P（Plan）——计划，确定方针、目标和活动计划；**
  - **D（Do）——实施，实现计划中的内容；**
  - **C（Check）——检查，检查并总结执行计划的结果；**
  - **A（Action）——处置，对检查总结的结果进行处理。**
  -



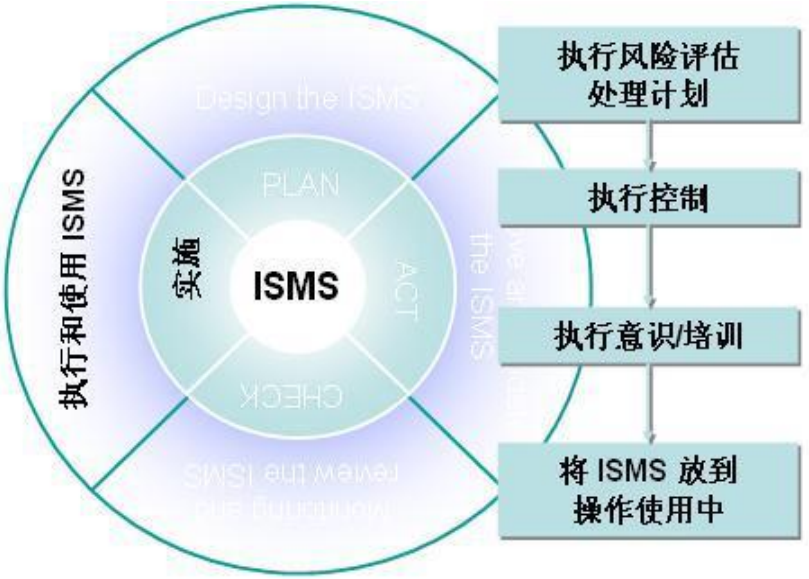
2.1信息安全管理体系概述

- **4. PDCA模型（戴明环）**
  - **P（Plan）---计划阶段**
    - 确定信息安全方针
    - 确定信息安全管理体系的范围
    - 制定风险识别和评估计划
    - 制定风险控制计划
      - 分析目前现状，找出存在的问题；
      - 分析产生问题的各种原因以及影响因素；
      - 分析并找出管理中的主要问题；
      - 制定管理计划，确定管理要点。



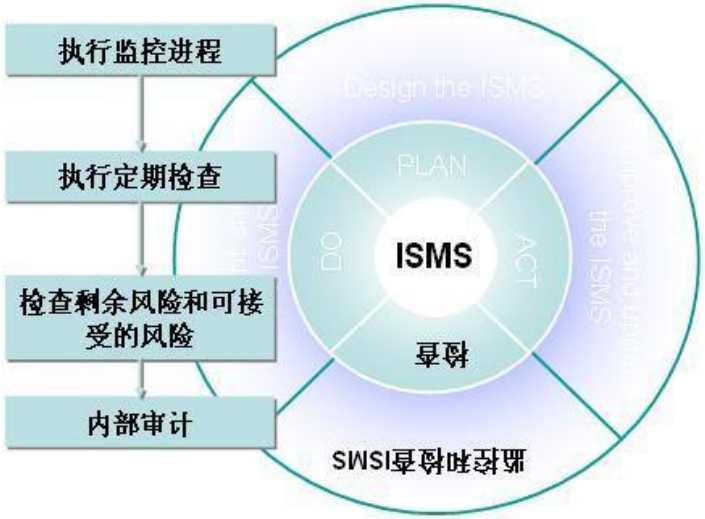
2.1信息安全管理体系概述

- **4. PDCA模型（戴明环）**
  - **D（Do）---实施阶段**
    - 保证资源、提供培训、提高安全意识
    - 风险治理
  - **本阶段的任务是在管理工作中全面执行制定的方案。**



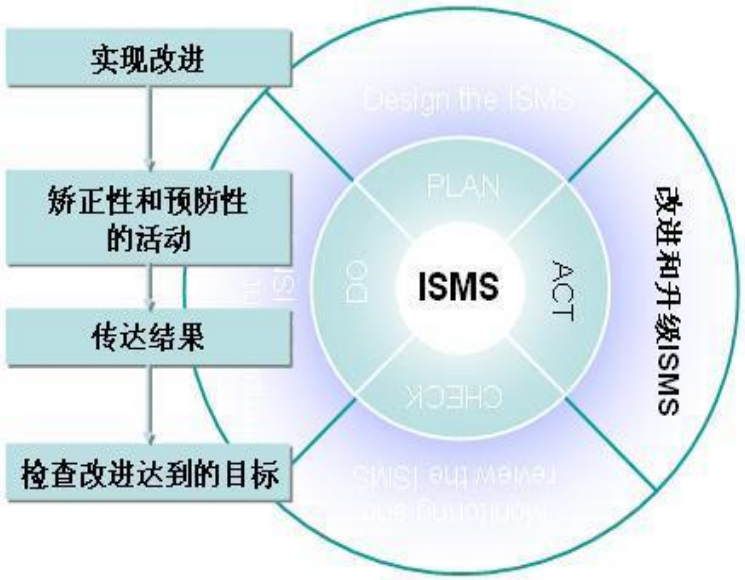
2.1信息安全管理体系概述

- **4. PDCA模型（戴明环）**
  - **C（Check）---检查阶段**
    - 日常检查
    - 内部信息安全管理体系审核
    - 自治程序
    - 管理评审
    - 从其他处学习
    - 趋势分析
  - 它是对实施方案是否合理、是否可行以及有何不妥的检查。



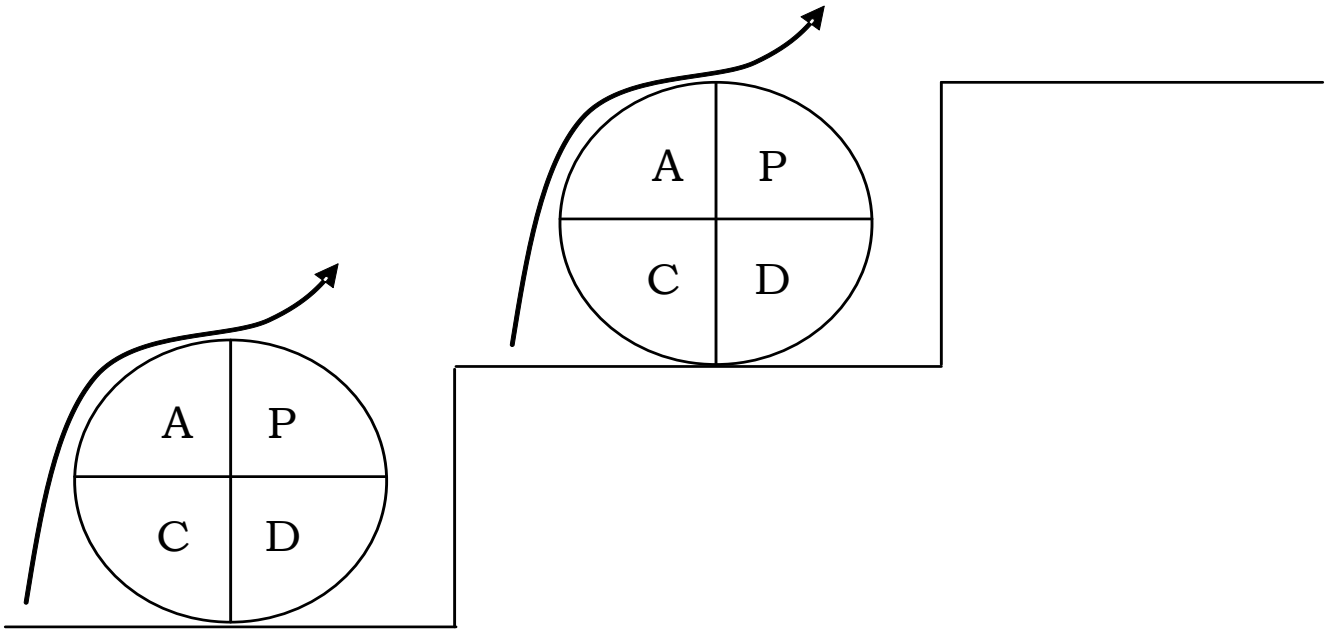
2.1信息安全管理体系概述

- **4. PDCA模型（戴明环）**
  - **A（Action）---处置阶段**
    - 不符合项
    - 纠正和预防措施
  - **对已解决的问题，加以标准化**
  - **找出尚未解决的问题**



2.1信息安全管理体系概述

- PDCA循环是螺旋式上升和发展的。



持续改进的PDCA过程

2.2 信息安全管理标准的发展史

- 信息安全与管理标准的发展历程关系
  - 信息安全发展历程
    - 通信保密（ComSEC)
    - 计算机安全(CompSEC)
    - IT安全(ITSEC)
    - 信息安全保障（IA)
  - 管理标准的发展

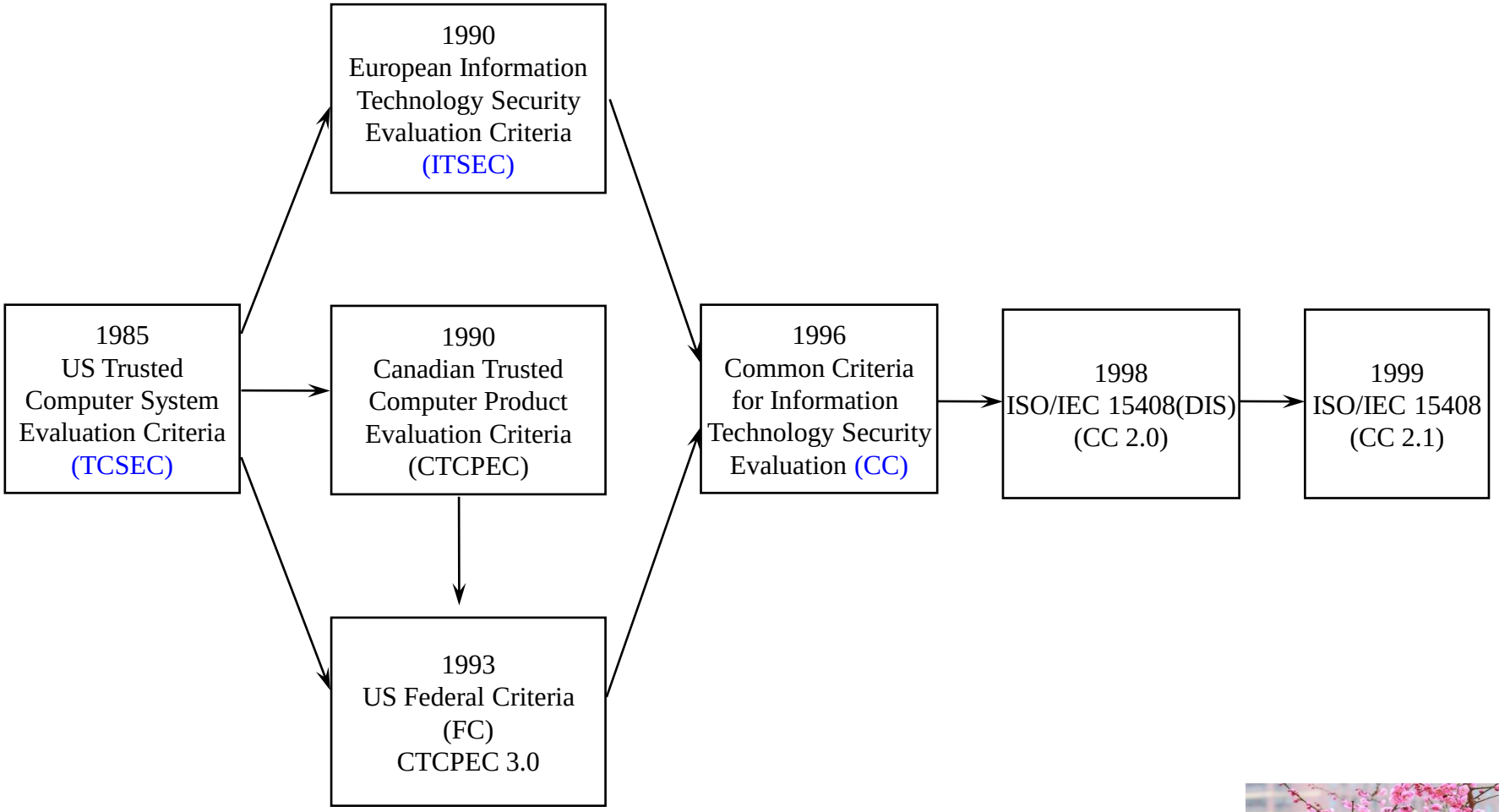
2.2 信息安全管理标准的发展史

• 1. CC标准的发展历程

- **1. 1997年10月7日，美国公告了针对 ISO/IEC 15408(以下简称CC)通过后认证机制所需TTAP (Trust Technology Assessment Program) Laboratories,接受CC测试与评估工作，作为NIAP (National Information Assurance Partnership) CCEVS (Common Criteria Evaluation and Validation Scheme)认证建立起来的过渡方案。**
- **2. 1997年11月8日，TTAP提出基于CC认证、检测的工作建议。**
- **3. 1999年4月，美国、加拿大、德国、英国、法国共同簽署CCMRA (Mutual Recognition Agreement)，預期欧洲、亞太其他国家将陆续加入。**
- **4. 1999年5月14日，美國公告了CC认证计划，同時宣布密码組认证计划將并入此计划。**
- **5. 1999年6月8日，美国宣布CC 2.1版正式成为ISO/IEC 15408。**
- **6. 2000年5月23~25日，在美国Baltimore International Convention Center举办第1次CC国际研讨会。**
- **7. 2000年8月30日，美国公告Computer Science Corporation (CSC)，Cygna Com Solutions, Science Applications International Corporation (SAIC)與 TUV:T Incoporated 4家民間实验室已經通過NIAP的認可 CCTL (Common Criteria Testing Laboratories)。**

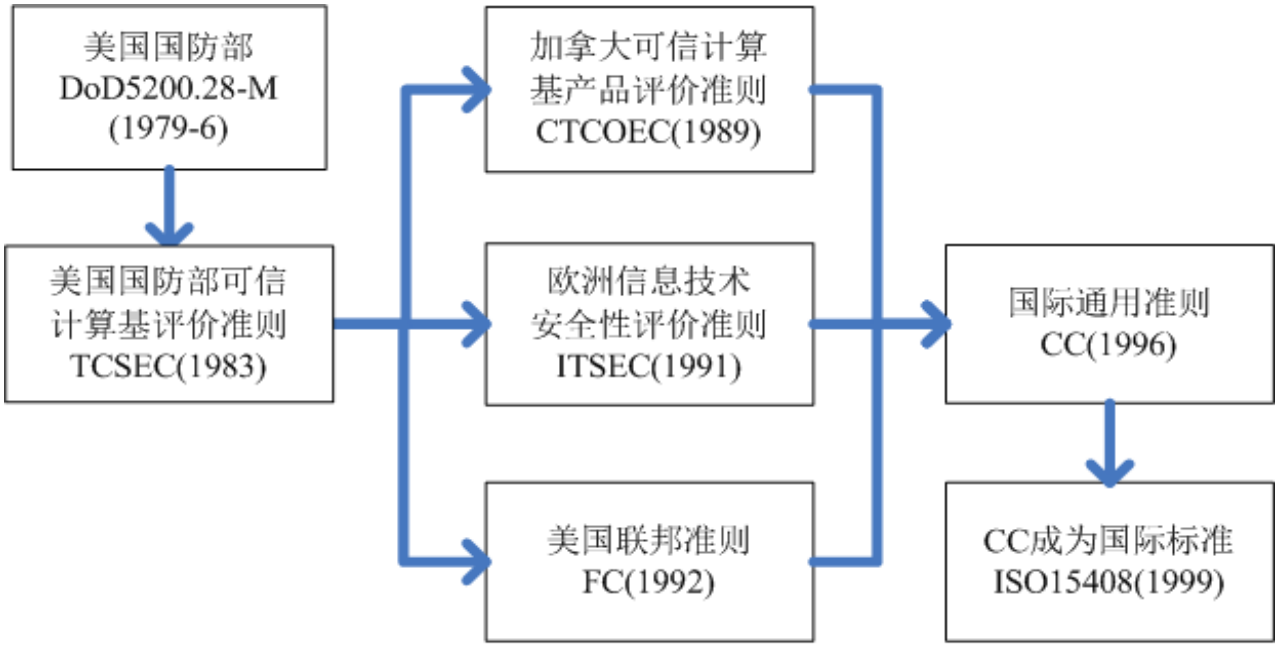
2.2 信息安全管理标准的发展史

- 1. CC标准的发展历程



2.2 信息安全管理标准的发展史

- **1. CC标准的发展历程**



CC标准的演进历程

2.2 信息安全管理标准的发展史

- 分级对应

ITSEC保证	TCSEC分级	CC
E0	D	
		EAL1
E1	C1	EAL2
E2	C2	EAL3
E3	B1	EAL4
E4	B2	EAL5
E5	B3	EAL6
E6	A	EAL7

问题:CC中的评估保证级4级（EAL4）对应TCSEC和ITSEC的哪个级别？

2.2 信息安全管理标准的发展史

- **2. BS 7799系列标准的发展历程**
  - 参照质量管理体系BSI提出了信息安全管理标准BS 7799系列
  - Information security management
    - Part 1: Code of practice for information security management
    - Part 2: Specification for information security management systems.
  - BS7799英国标准协会针对信息安全管理制定的，发布于1995年，后几经修改，成为目前被广泛接受的标准。分为两个部分：
    - BS7799－1，是信息安全管理实施细则，供负责信息安全系统开发的人员参考使用；
    - BS7799－2，是建立信息安全管理体系的规范，最终目的是建立适合企业的信息安全管理体系。
  - BS 7799中提出了若干重要概念
    - 风险评估:评估信息安全漏洞对信息处理设备带来的威胁和影响及其发生的可能性。
    - 风险管理 :以可以接受的成为、确认、控制、排除 可能影响信息系统的安全风险或将其带来的危害最 小化的过程。

2.2 信息安全管理标准的发展史

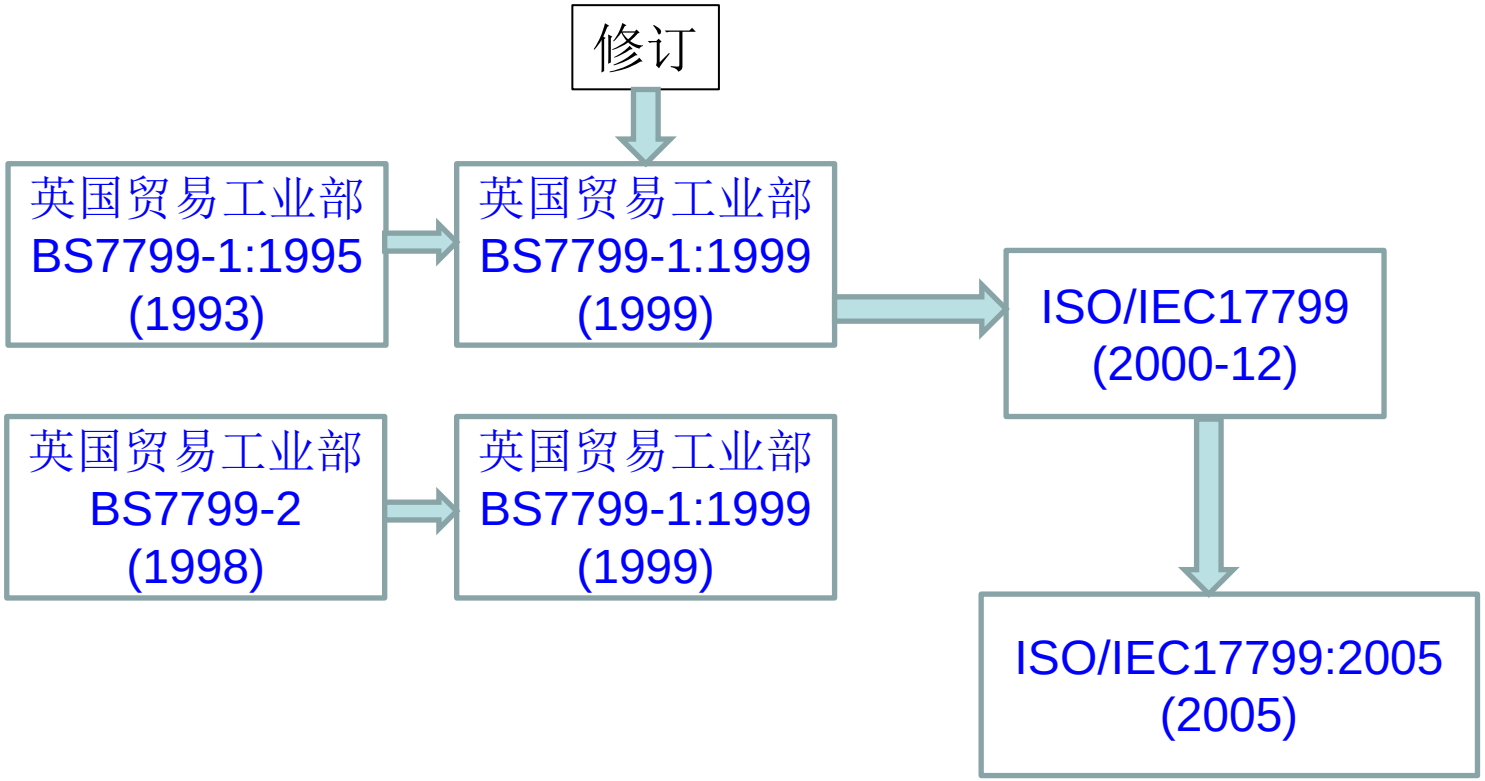
- 英国模式

管理体系	简称	相关标准	服务对象
质量管理体系	QMS	ISO/IEC9000，9001，9004等	顾客
环境管理体系	EMS	ISO/IEC14000	社会
职业安全健康管理体系	OSHMS	OHSAS 18000	员工
信息安全管理体系	ISMS	ISO/IEC 17799，ISO27001	组织

2.2 信息安全管理标准的发展史

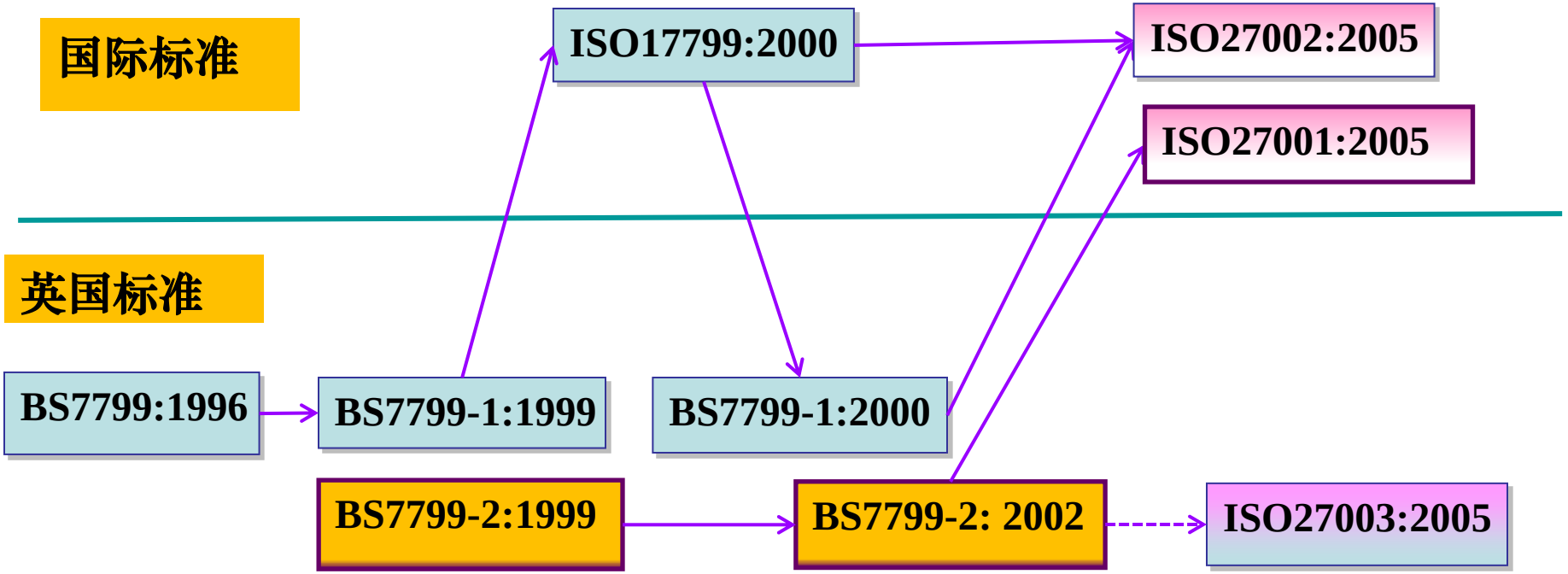
- **BS7799的发展历史**
  - **1993年，英国贸易工业部，BS7799-1:1995《信息安全管理实施规则》；**
  - **1998年，BS7799-2:1998《信息安全管理体系规范》；**
  - **1999年，BS7799-1:1999取代了BS7799-1:1995标准，BS7799-2:1999取代了BS7799-2:1998标准；**
  - **国际标准化组织于2000年12月正式将BS7799转化成国际标准ISO/IEC17799；**
  - **2005年6月15日发布了最新版本ISO/IEC17799:2005。**

2.2 信息安全管理标准的发展史



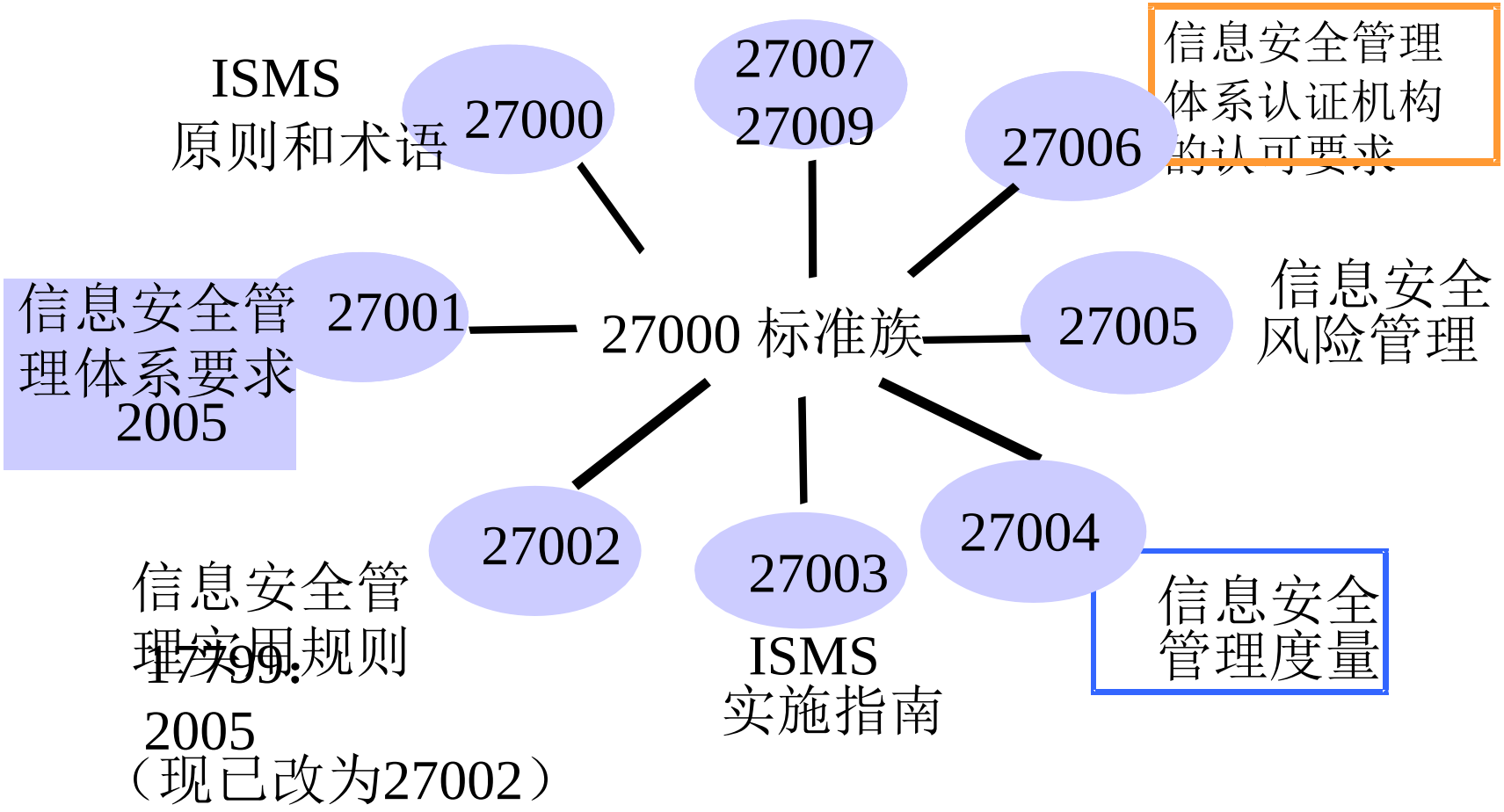
2.2 信息安全管理标准的发展史

- 3. ISO/IEC 2700系列标准的发展历程



2.2 信息安全管理标准的发展史

- **3. ISO/IEC 2700系列标准**

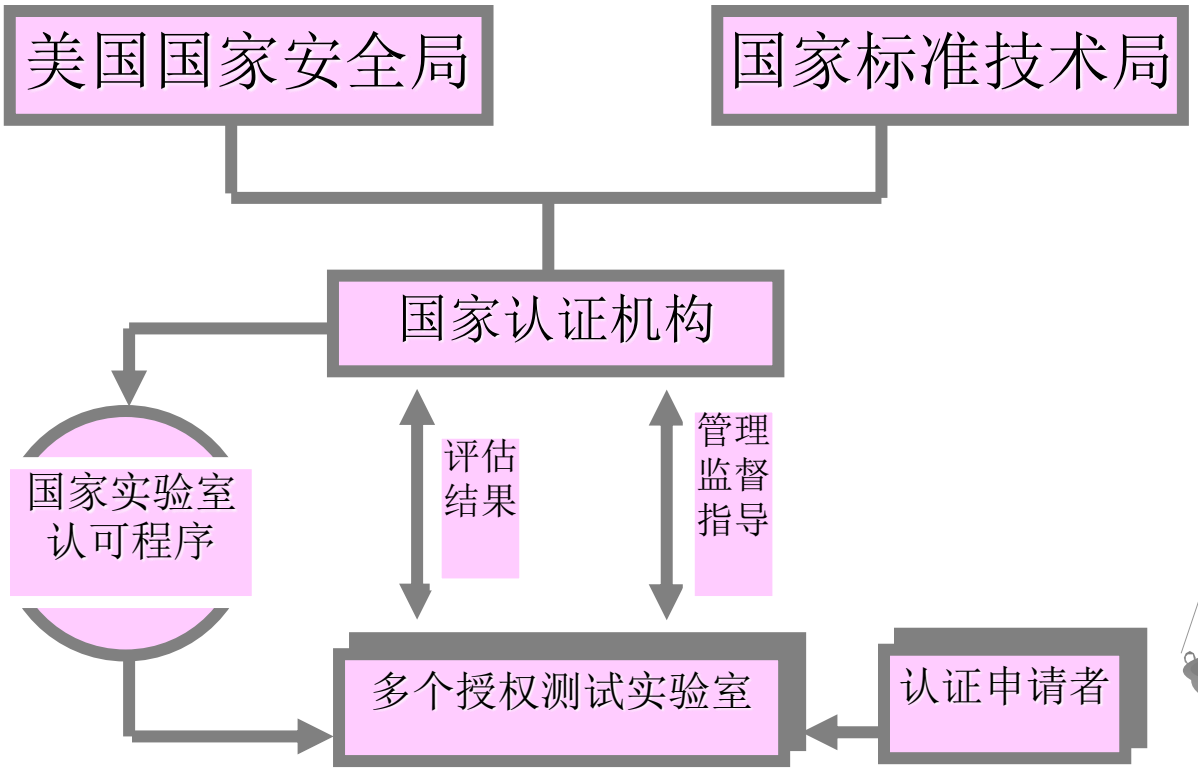


2.2 信息安全管理标准的发展史

- **4. 其他测评相关标准**
  - **15408: 通用准则(CC)**
  - **15292: PP注册程序**
  - **15446: PP和ST生成指南**
  - **15443: IT安全保障框架 (FRITSA)**
  - **18045: 通用评估方法（CEM)**
  - **19790: 密码模块的安全要求**
  - **19791: 运行系统的安全评估**
  - **19792: 生物识别技术的安全测评框架 (SETBIT)**
  - **21827:2002 系统安全工程 – 能力成熟模型 (SSE-CMM)**

2.2 信息安全管理标准的发展史

- 美国测评认证体系模式



2.2 信息安全管理标准的发展史

- 国际互认情况

2.2 信息安全管理标准的发展史

- **5. 我国信息安全管理标准**
  - **GB/T19715.1-2005**《信息安全管理指南 第一部分:IT安全管理的概念和模型》
  - **GB/T19715.2-2005**《信息安全管理指南 第二部分:管理和规划IT安全》
- 信息安全管理要素标准
  - **GB/T19716-2005**《信息技术 信息安全管理实用规则》
  - **GB/T20269-2006**《信息安全技术 信息系统安全管理要求》

2.2 信息安全管理标准的发展史

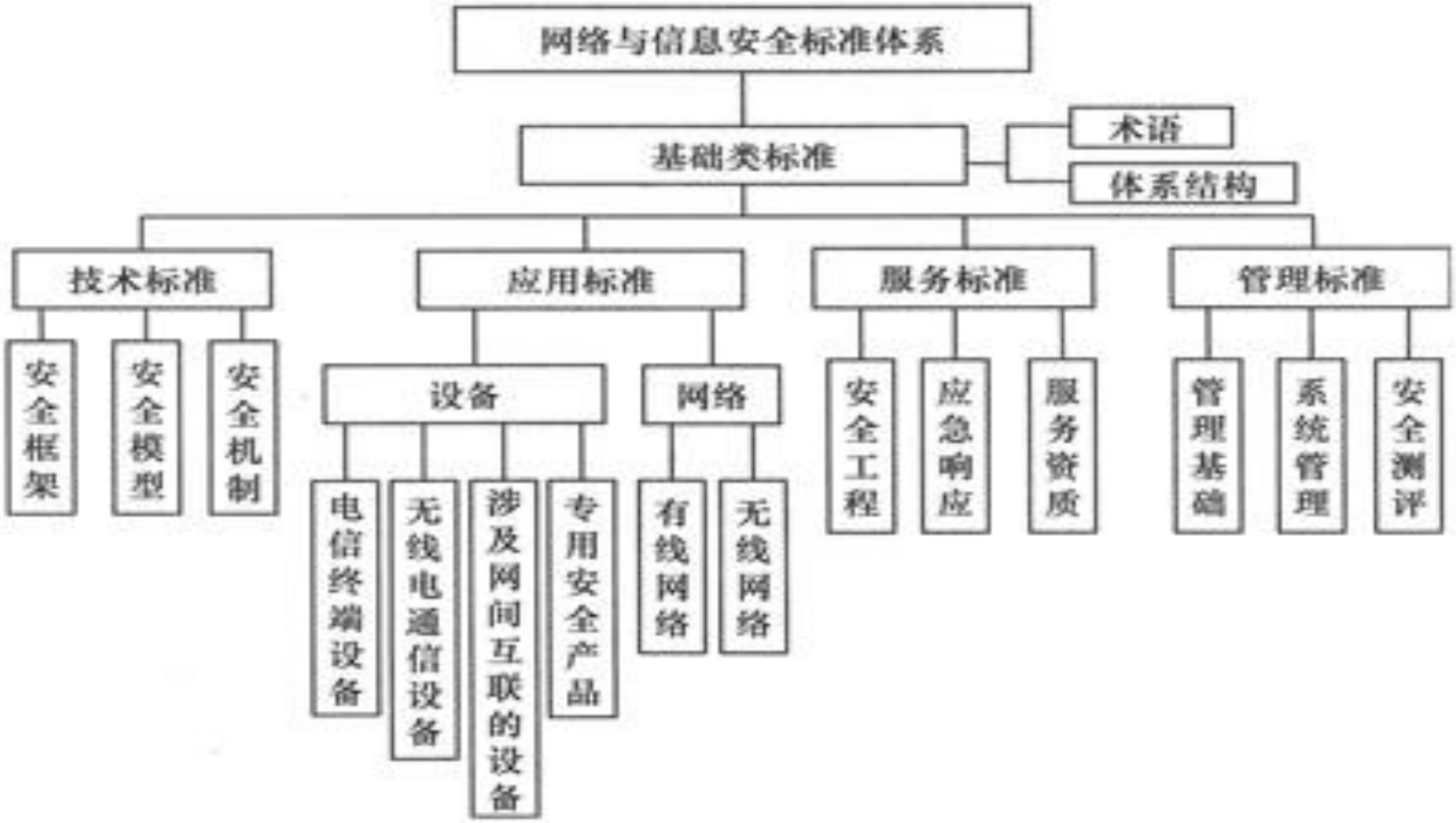
- **4. 我国信息安全管理标准**
  - **GB/T20984-2007《信息安全技术 信息安全风险评估规范》**
  - **GB/Z20985-2007《信息安全技术 信息安全事件管理指南》**
  - **GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》**
  - **GB/T20988-2007《信息安全技术 信息系统灾难恢复规范》**
  - **2007制定**
    - **《信息安全管理体系要求》（27001）**
    - **《信息安全管理体系认证机构的认可要求》（27006）**
    - **《信息安全风险管理规范》**
  - **2007修订**
    - **GB/T 19716-2005《信息技术 信息安全管理实用规则》**
  - **2007预编制**
    - **《灾难恢复计划》**
    - **《信息安全风险评估实施指南》**

2.2 信息安全管理标准的发展史

- 我国各行业落实情况
  - 信息安全等级保护办法 (公通字[2007]43号)
  - 电子银行业务管理办法 (银监会[2006]5号)
  - 国家电子政务工程建设项目管理暂行办法(发改委[2007]55号)
  - 银监会、保监会、电监会、证监会17大安全工作保证要求
  - 2008奥运安保工作要求
    - （民航、铁路、电力、银行、新闻、气象等部门）
  - 国税系统安全评估检查（轮巡、抽查）

2.2 信息安全管理标准的发展史

- 我国安全体系落实架构



2.3 信息安全管理标准介绍

- **1. BS7799**
  - **BS7799-1:《信息安全管理实施规则》**
    - 主要是给负责开发的人员作为参考文档使用;
    - 机构内部实施和维护信息安全的指南。
  - **BS7799-2:《信息安全管理体系规范》**
    - 详细说明了建立、实施和维护ISMS的要求;
    - 指出通过风险评估来鉴定最适宜的控制对象;
    - 根据组织自己的需求采取适当的安全控制。
  - **BS7799标准的最大意义**
    - 最大意义就在于它给管理层一整套可“量体裁衣”的信息安全管理要项、一套与技术负责人或组织高层进行沟通的共同语言，以及保护信息资产的制度框架。

2.3 信息安全管理标准介绍

- **BS7799**
  - 旨在为组织实施信息安全管理体系提供指导性框架，更多体现的是一种目标要求
  - 普适性强
  - 局限
    - 针对性弱
    - 总体上并没有提及实施的细节（通行标准的必然）
    - 落实BS7799标准，组织需补充必要的可实施内容。

2.3 信息安全管理标准介绍

- **CC：**
  - 是国际上最通行的信息技术产品及系统安全性测评标准，也是信息技术安全性评估结果国际互认的基础。
  - CC标准由3个文件构成：
    - （1）ISO/IEC15408-1，介绍和一般模型
    - （2）ISO/IEC15408-2，安全功能要求
    - （3）ISO/IEC15408-3，安全保证要求
  - 与BS7799比较：
    - CC侧重系统和产品的技术指标评价上。

2.3 信息安全管理标准介绍

- **ISO/IEC TR13335**
  - 名称：
    - 曾用名，“IT安全管理指南”，现名，“信息和通信技术安全管理”
  - 是一个信息安全管理方面的指导性标准，目的是为有效实施IT安全管理提供建议和支持。
  - 共分5个部分：
    - ISO/IEC 13335－1：1996 IT安全概念与模型
    - ISO/IEC 13335－2：1997 IT安全管理和计划
    - ISO/IEC 13335－3：1998 IT安全管理技术
    - ISO/IEC 13335－4：2000 安全措施的选择
    - ISO/IEC 13335－5：2001 网络安全管理指南

2.3 信息安全管理标准介绍

- **ISO/IEC TR13335**
  - **与BS7799的比较**
    - **BS7799**只是一个指导性的文件，并不是可依据的认证标准，也没有给出一个全面完整的信息安全管理框架；
    - **ISO/IEC TR13335**在IT安全的具体环节上切入点较深，可实施性较好，另外其风险评估方法过程较清晰。

2.3 信息安全管理标准介绍

- **SSE-CMM**
  - 由美国国家安全局开发，是专门用于系统安全工程能力成熟度模型。该模型将系统安全工程成熟度分为5个等级。
  - 与CC、BS7799比较：
    - SSE-CMM和CC都是评估标准，均可将评估对象划分为不同的等级。
      - CC针对的是安全系统或安全产品的测评；
      - SSE-CMM针对的是安全工程过程。
    - SSE-CMM和BS7799都提出了一系列最佳惯例
      - BS7799是一个认证标准而无实现过程；
      - SSE-CMM是一个评估标准，定义了实现最终安全目标所需要的一系列过程。
      - SSE-CMM和BS7799可以互补使用。

2.3 信息安全管理标准介绍

- **NIST SP 800系列**
  - SP 800系列由美国国家标准技术协会发布，主要内容是针对信息安全技术和管理领域的实践参考指南，包括四项：
    - SP800-12：计算机安全介绍
    - SP800-30: IT系统风险管理指南
    - SP800-34: IT系统应急计划指南
    - SP800-26: IT系统安全自我评价指南

2.3 信息安全管理标准介绍

- **ITIL**
  - 由英国中央计算机与电信局发布
    - 关于IT服务管理最佳实践的建议和指导方针，目的是解决IT服务质量，是一种基于流程的管理方法，尤其适于企业的IT部门。
    - 其精髓体现为“一大功能”和“十大流程”
    - 一大功能：服务台功能。
    - 十大流程：
      - 服务支持：
        - » 事件管理 、问题管理、变更管理、发布管理、配置管理
      - 服务交付
        - » 服务水平管理、可用性管理、IT服务财务管理、容量管理、IT服务持续性管理

2.3 信息安全管理标准介绍

- **ITIL与BS7799相比：**
  - **ITIL关注的信息技术更广泛，侧重于具体的实施流程，但缺少信息安全的内容；**
  - **BS7799可作为ITIL在信息安全方面的补充。**

2.3 信息安全管理标准介绍

- **CobiT**（信息及相关技术控制目标）
  - 美国信息系统审计与控制协会发布
  - 是目前世界上最先进、最权威的安全与信息技术管理和控制标准。主要目的是为业界提供关于IT控制的清晰政策和发展的良好典范。
  - **Cobit与ITIL比较：**
    - 均关注广泛的IT控制，但是更强调目标要求和度量指标，而后者更关注实施流程。
  - 具体在ISMS的建设上
    - Cobit的框架和目标、ITIL的流程都可以供BS7799借鉴，BS7799的目标只是ITIL和Cobit的一个分支

2.4 BS7799信息安全管理体系

- **BS7799的内容**
  - **BS7799-1:《信息安全管理实施规则》**
    - 主要是给负责开发的人员作为参考文档使用；
    - 机构内部实施和维护信息安全。
  - **BS7799-2:《信息安全管理体系规范》**
    - 详细说明了建立、实施和维护信息安全管理体系的要求，指出实施组织需要通过风险评估来鉴定最适宜的控制对象，并根据自己的需求采取适当的安全控制。
  - 最大意义
    - 给管理层一整套可“量体裁衣”的信息安全管理要项；
    - 一套与技术负责人或组织高层进行沟通的共同语言；
    - 保护信息资产的制度框架。

2.4 BS7799信息安全管理体系

- BS7799的内容
  - BS7799-1:《信息安全管理实施规则》
    - 实施细则将管理内容划分为
      - 11个主要方面，39个信息安全管理的控制目标，133项安全控制措施
      - 不够具体，组织可以根据自身增减
    - 信息安全最佳起点：
      - 10项控制措施
        - » 包括三项与法律相关的控制措施和七项与最佳实践相关的控制措施。
        - » 几乎适用于所有组织和大多数环境的
        - » （体现重管理的思想）

2.4 BS7799信息安全管理体系

- BS7799的十项控制措施
  - 与法律相关的控制措施：（三项）
    - （1）知识产权
    - （2）保护组织的记录（保护重要的记录不丢失、破坏、伪造）
    - （3）数据保护和个人信息隐私
  - 与最佳实践相关的措施：（七项）
    - （1）信息安全策略文件
    - （2）信息安全责任分配
    - （3）信息安全意识、教育、培训
    - （4）正确处理应用程序
    - （5）漏洞管理
    - （6）管理信息安全事件和改进
    - （7）业务连续性管理

2.4 BS7799信息安全管理体系

- **BS7799的内容**
  - **BS7799-1:《信息安全管理实施规则》**
    - 作为国际信息安全指导标准ISO/IEC17799基础的指导性文件
    - 包括11大管理要项，134种控制方法。

<table>
<tr><td colspan="4">1．安全方针/策略（Security Policy）</td></tr>
<tr><td colspan="4">2．安全组织（Security Organization）</td></tr>
<tr><td colspan="4">3．资产分类与控制（Asset Classification and Control）</td></tr>
<tr><td>4．人员安全（Personnel Security）</td><td>5．物理与环境安全（Physical and Environmental Security）</td><td>6．通信与运营管理（Communications and Operations Management）</td><td rowspan="2">8．系统开发与维护（Systems Development and Maintenance）</td></tr>
<tr><td colspan="3">7．访问控制（Access Control）</td></tr>
<tr><td colspan="4">9．信息安全事件管理（Information Security Incident Management）</td></tr>
<tr><td colspan="4">10．业务持续性管理（Business Continuity Management）</td></tr>
<tr><td colspan="4">11．法律法规符合性（Compliance）</td></tr>
</table>

2.4 BS7799信息安全管理体系

- **BS7799的内容**
  - **BS7799-2:《信息安全管理体系规范》**
    - 主要特点
      - 提供了安全管理体系规范；
      - 提供了建立信息安全管理体系的目标。
    - 该标准强调信息安全管理是一个面向风险的、持续改进的过程。

2.4 BS7799信息安全管理体系

- **BS7799的内容**
  - **BS7799-2:《信息安全管理体系规范》**
    - 说明了建立、实施和维护信息安全管理体系（ISMS）的要求；
    - 指出实施组织需要通过风险评估来鉴定最适宜的控制对象；
    - 根据自己的需求采取适当的安全控制。
    - **BS7799-2的新版本ISO/IEC27001:2005**

2.4 BS7799信息安全管理体系

- **BS7799的内容**
  - **BS7799-2的新版本ISO/IEC27001:2005**
    - 更注重PDCA的过程管理模式，能够更好的与组织原有的管理体系，如质量管理体系、环境管理体系等进行整合，减少组织的管理过程，降低管理成本。
    - 2005.10，英国信息安全管理体系标准BS7799-2：2002作为国际标准ISO/IEC 27001：2005采用，标志着信息安全管理体系认证进入了一个新阶段。
    - 截至2005.11，全球共签发了1882张认证证书，如：Siemens,NEC,CANON、EPON、IBM等。

2.4 BS7799信息安全管理体系

- BS7799的ISMS建立步骤
  - 1.BS7799信息安全管理体系的准备
  - 2.建立BS7799信息安全管理框架
  - 3.编写BS7799信息安全管理体系文件
  - 4.BS7799信息安全管理体系的运行
  - 5.BS7799信息安全管理体系的审核
  - 6.BS7799信息安全管理体系的管理评审
  - 7.BS7799信息安全管理体系的检查与持续改进

2.4 BS7799信息安全管理体系

- **BS7799体系建立关键步骤**
  - 信息安全管理体系的策划与准备
  - 信息安全管理体系文件的编制
  - 建立信息安全管理框架
  - 信息安全管理体系的运行
  - 信息安全管理体系的审核与评审

2.4 BS7799信息安全管理体系

- 1.BS7799信息安全管理体系的准备

管理承诺

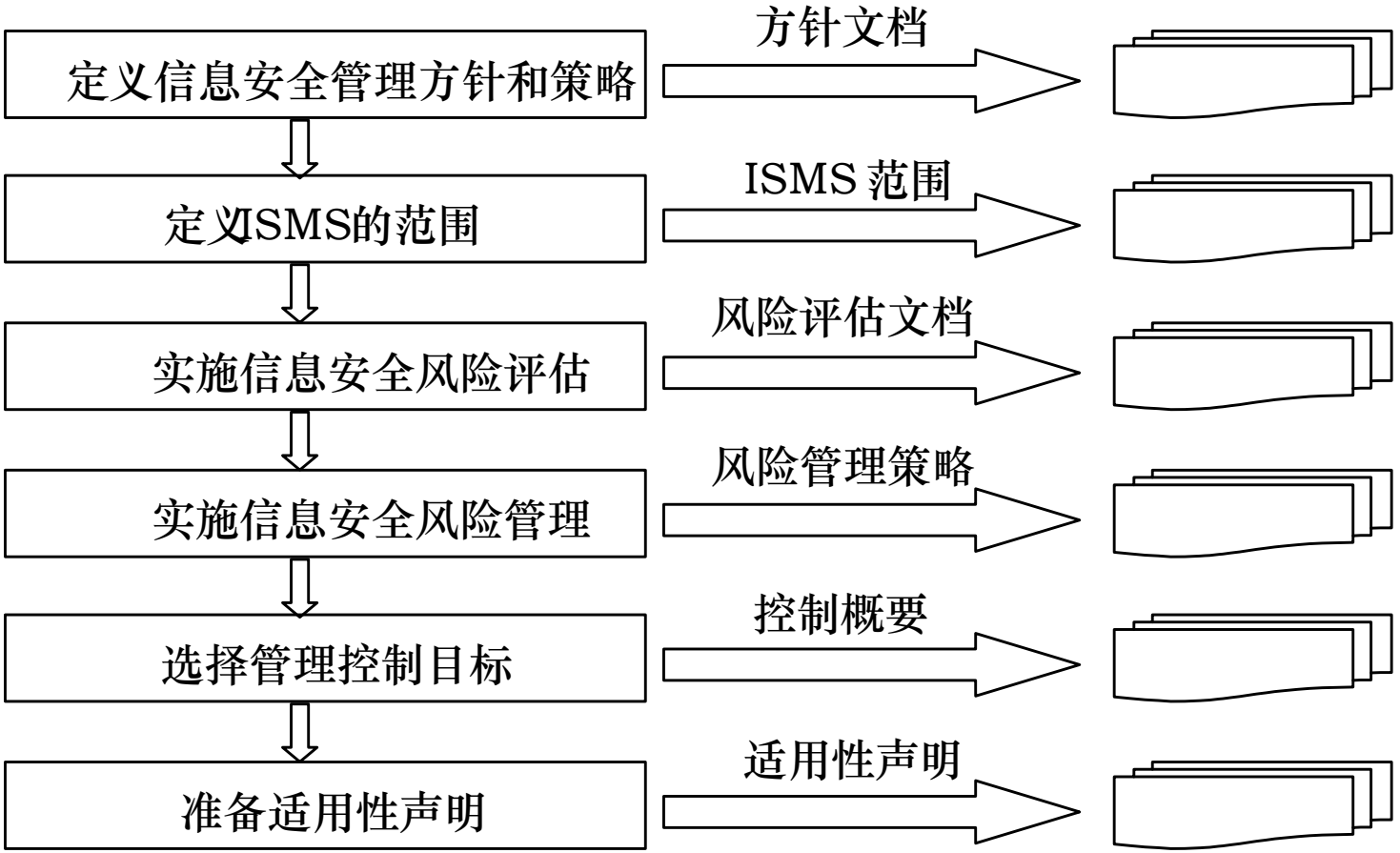
组织与人员建设

编制工作计划

能力要求与教育培训

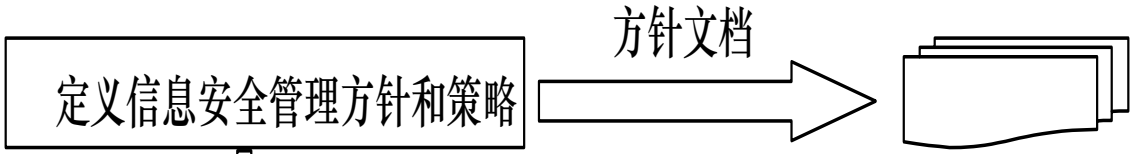
2.4 BS7799信息安全管理体系

- 2.建立BS7799信息安全管理框架



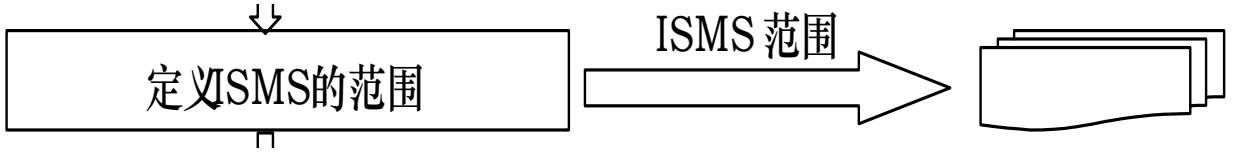
2.4 BS7799信息安全管理体系

- 2.建立BS7799信息安全管理框架
  - 定义安全策略
    - 信息安全策略（**Information Security Policy**）本质上来说是描述组织具有哪些重要信息资产，并说明这些信息资产如何被保护的一个计划。
    - 分为两个层次：信息安全方针，具体的信息安全策略



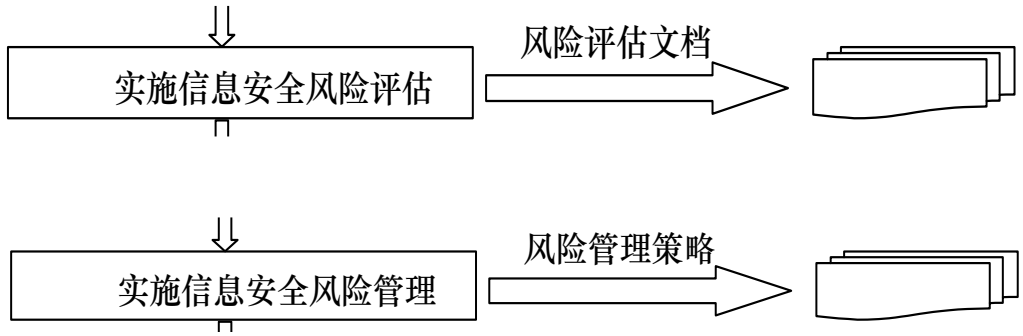
2.4 BS7799信息安全管理体系

- 2.建立BS7799信息安全管理框架
  - 定义ISMS的范围
    - 组织现有部门
    - 办公场所
    - 资产状况
    - 所采用技术



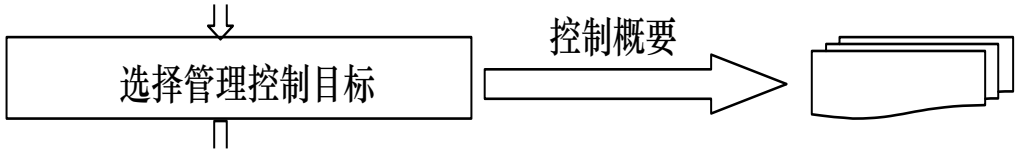
2.4 BS7799信息安全管理体系

- 2.建立BS7799信息安全管理框架
  - 实施信息安全风险评估
    - 对ISMS范围内的信息资产进行鉴定和估价
    - 对信息资产面对的各种威胁和脆弱性进行评估
    - 对已存在的或规划的安全控制措施进行鉴定
  - 实施信息安全风险管理
    - 降低风险
    - 避免风险
    - 转移风险
    - 接受风险

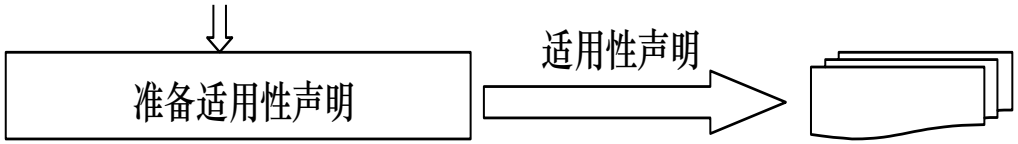


2.4 BS7799信息安全管理体系

- 2.建立BS7799信息安全管理框架
  - 确定控制目标和选择控制措施
    - 控制目标的确定和控制措施的选择原则是成本不超过风险所造成的损失。



  - 准备信息安全适用性声明
    - SOA是适合组织需要的控制目标和控制措施的评论，需要提交给管理者、职员以及具有访问权限的第三方认证机构。



2.4 BS7799信息安全管理体系

- 3.编写BS7799信息安全管理体系文件
  - 文件的作用
    - 阐述声明的作用
    - 规定和指导作用
    - 记录和证实作用
    - 评价合规性作用（信息安全管理体系）
    - 保障责任风险作用（信息安全改进）
    - 平衡培训要求
  - 文件的编写
    - 编写原则
    - 编写前的准备
    - 编写的策划与组织

2.4 BS7799信息安全管理体系

- 3.编写BS7799信息安全管理体系文件
  - 文件的层次
    - 适用性声明
    - ISMS管理手册
    - 程序文件
    - 作业指导书
    - 记录
  - 文件的控制管理
    - 文件控制
    - 记录控制

2.4 BS7799信息安全管理体系

- **4.BS7799信息安全管理体系的运行**
  - 有针对性地宣传信息安全管理体系文件
  - 完善信息反馈与信息安全协调机制
  - 加强有关体系运行信息的管理
  - 加强信息安全体系文件的管理

2.4 BS7799信息安全管理体系

- **5.BS7799信息安全管理体系的审核**
  - 信息安全管理体系审核是指组织为验证所有安全方针、策略和程序的正确实施，检查信息系统符合安全实施标准的情况所进行的系统的、独立的检查和评价，是信息安全管理体系的一种自我保证手段。
    - 管理性审核
    - 技术性审核
  - 审核的分类：
    - 内部信息安全管理体系审核
    - 外部信息安全管理体系审核

2.4 BS7799信息安全管理体系

- **5.BS7799信息安全管理体系的审核**
  - **ISMS审核的主要目的：**
    - 检查BS7799的实施程度与标准的符合性情况；
    - 检查满足组织安全策略与安全目标的有效性和适用性；
    - 识别安全漏洞与弱点；
    - 向管理者提供安全控制目标实现状况，使管理者了解安全问题；
    - 指出存在的重大的控制弱点，证实存在的风险；
    - 建议管理者采用正确的校正行动，为管理者的决策提供有效支持；
    - 满足法律、法规与合同的需要；
    - 提供改善ISMS的机会。

2.4 BS7799信息安全管理体系

- **5.BS7799信息安全管理体系的审核**
  - 体系审核的基本步骤：
    - 确定任务（审核策划）
    - 审核准备
    - 现场审核
    - 编写审核报告
    - 纠正措施的跟踪
    - 全面审核报告的编写和纠正措施计划完成情况的汇总分析

2.4 BS7799信息安全管理体系

- 6.BS7799信息安全管理体系的管理评审
  - 管理评审主要是指组织的最高管理者按规定的时间间隔对信息安全管理体系进行评审，以确保体系的持续适宜性、充分性和有效性。
  - 管理评审的步骤
    - 编制评审计划
    - 准备评审材料
    - 召开评审会议
    - 评审报告分发与保存

2.4 BS7799信息安全管理体系

- 6.BS7799信息安全管理体系的管理评审
  - 管理评审的输入
    - 内、外部信息安全管理体系审核的结果；
    - ISMS方针、风险控制目标和风险控制措施的实施情况；
    - 事故、事件调查处理情况；
    - 事故、事件、不符合项、纠正和预防措施的实施情况；
    - 相关方的投诉、建议及其要求。
  - 管理评审的输出
    - 信息安全管理体系的适宜性、充分性和有效性的结论；
    - 组织机构是否需要调整；
    - 信息安全管理体系文件是否需要修改；
    - 资源配备是否充足，是否需要调整增加；
    - 信息安全方针、策略、控制目标和控制措施是否适宜，是否需要修改；
    - ISMS风险是否需要调整更新。

2.4 BS7799信息安全管理体系

- 6.BS7799信息安全管理体系的管理评审

表 2.3　　ISMS 体系审核与管理评审的比较

	ISMS 体系审核	管理评审
目的	确保 ISMS 体系运行的符合性、有效性	确保 ISMS 体系持续的适宜性、充分性和有效性
类型	第一方、第二方、第三方	第一方
依据	BS7799 标准、体系文件、法律法规	法律法规、相关方面的期望、ISMS 体系审核的结论
结果	第一方：提出纠正措施并跟踪实现 第二方：选择合适的合作伙伴 第三方：进行认证、注册	改进信息安全管理体系，提高信息安全管理水平
执行者	与被审核领域无直接关系的审核员	最高管理者

2.4 BS7799信息安全管理体系

- 8.BS7799信息安全管理体系的检查与持续改进
  - 对信息安全管理体系的审查
    - 日常检查
    - 自治程序
    - 学习其他组织的经验
    - 内部信息安全管理体系审核
    - 管理评审
    - 趋势分析
  - 对信息管理体系的持续改进
    - 纠正性控制
      - 组织应采取措施，以消除不合格的、与实施和运行信息安全管理体系有关的原因，防止问题的再次发生。
    - 预防性控制
      - 组织应针对未来的不合格事件确定预防措施以防止其发生。预防措施应与潜在问题的影响程度相适应。

2.5 基于SSE-CMM的信息安全管理体系

- 系统安全工程能力成熟度模型SSE-CMM
  - （System Security Engineering-Capability Maturity Model，SSE-CMM）
  - 它的提出是为了改善安全系统、产品和服务的性能、价格及可用性。
  - 通过SSE-CMM可以将复杂的信息系统安全工程管理成为严格的工程学和可依赖的体系。
  - 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。

2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM发展史**
  - **1993年4月，美国国家安全局（NSA）对当时各类能力成熟度模型（CMM）工作状况进行研究；**
  - **1996年10月出版了SSE-CMM的第一个版本；**
  - **1999年4月SSE-CMM模型和相应评估方法2.0版发布；**
  - **2002年，国际标准化组织正式公布了系统安全工程能力成熟度模型的标准，即ISO/IEC21827:2002。**

2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM的作用**
  - **SSE-CMM对工程组织的作用（工程乙方）**
    - 工程组织包括系统集成商、应用开发者、产品厂商和服务供应商。
    - 通过可重复和可预测的过程及实施来减少返工；
    - 获得真正工程执行能力的认可，特别是在资源选择方面；
    - 侧重于组织的资格（成熟度）度量和改进。
  - **SSE-CMM对获取组织的作用（工程甲方）**
    - 获取组织包括从内部/外部获取系统、产品和服务的组织以及最终用户。
    - 可重用的（**Request for Proposal，RFP**）标准语言和评定方法；
    - 减少选择不合格投标者的风险（性能、成本和工期风险）；
    - 进行基于工业标准的统一评估，减少争议；
    - 在产品生产和提供服务过程中建立可预测和可重复级的可信度。

2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM的作用**
  - **SSE-CMM对评估机构的作用**
    - 评估机构包括系统认证机构、系统授权机构和产品评估机构。
    - 可重用的过程评定结果，并与系统或产品变化无关；
    - 在安全工程中以及安全工程与其他工程集成中的信任度；
    - 基于能力的显见可信度，减少安全评估工作量。

2.5 基于SSE-CMM的信息安全管理体系

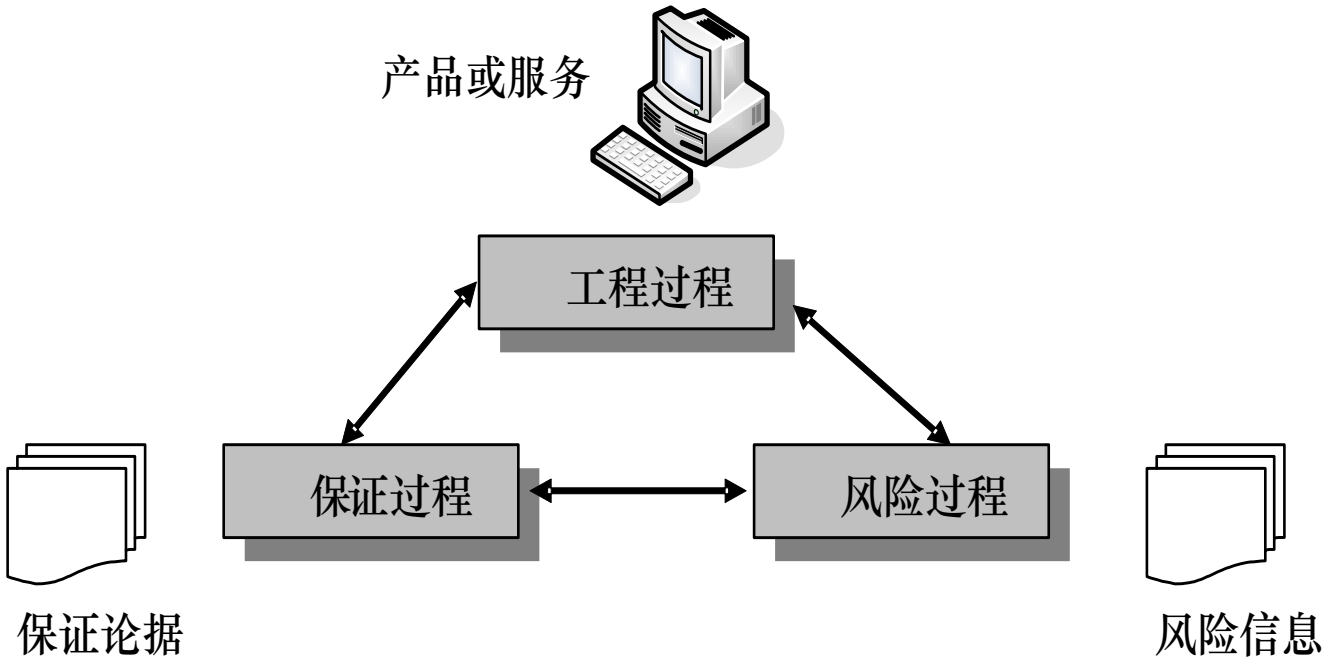
- **SSE-CMM的基本概念**
  - 组织
    - 被定义为公司内部的单位、整个公司或其他实体（如政府机构或服务机构）。
  - 项目
    - 是各种活动和资源的总和，这些活动和资源用于开发或维护一个特定的产品或提供一种服务。
  - 系统
    - 提供某种能力用以满足一种需要或目标的人员、产品、服务和过程的综合；
    - 事物或部件的汇集形成了一个复杂或单一整体（即用来完成某个特定或一组功能的组件的集合）；
    - 功能相关的元素相互组合。

2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM的基本概念**
  - 能力成熟度模型CMM：
    - CMM经过确定当前特定过程的能力和在一个特定域中识别出关键的质量和过程改进问题，来指导和选择过程改进策略。

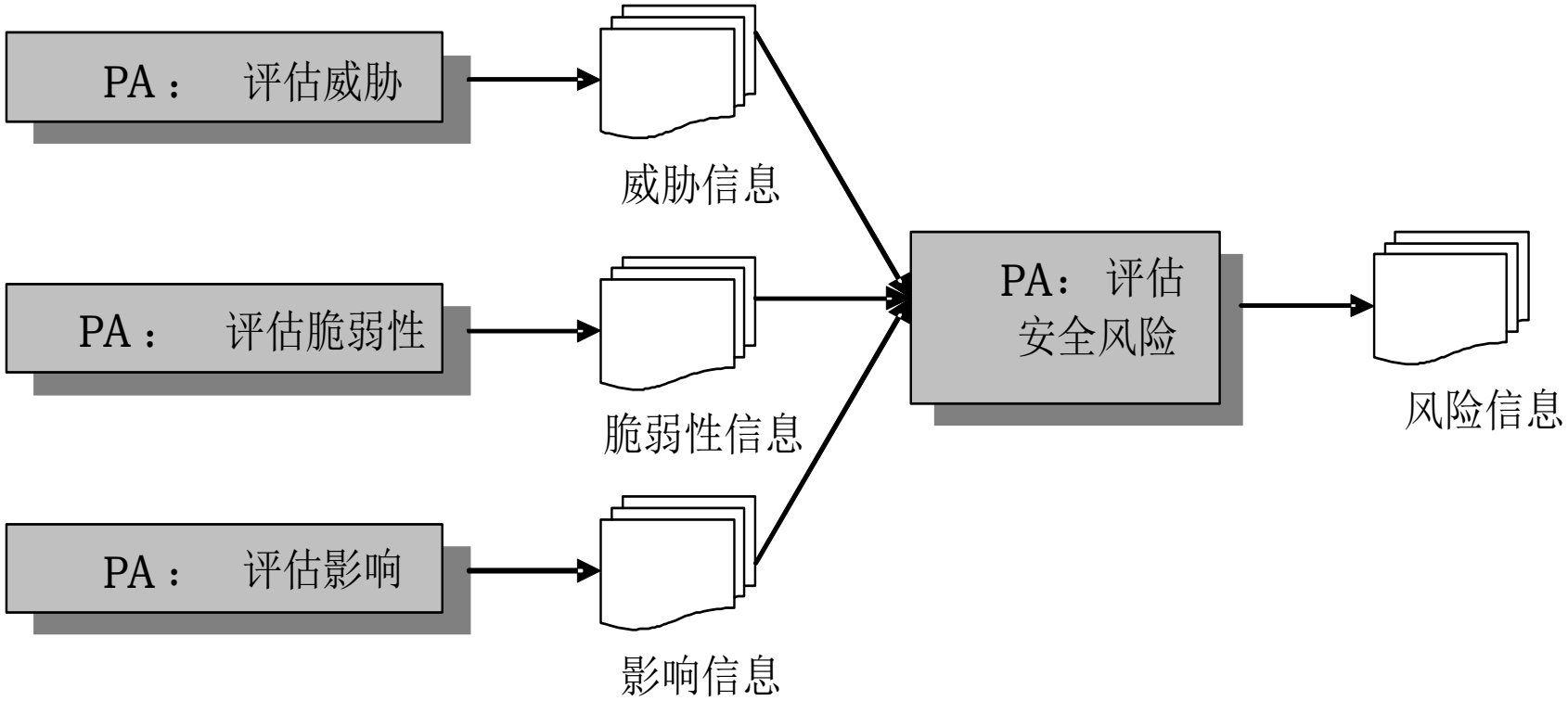
2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM的安全过程**
  - 包括产品服务、保证过程、风险过程
  - 关系如图



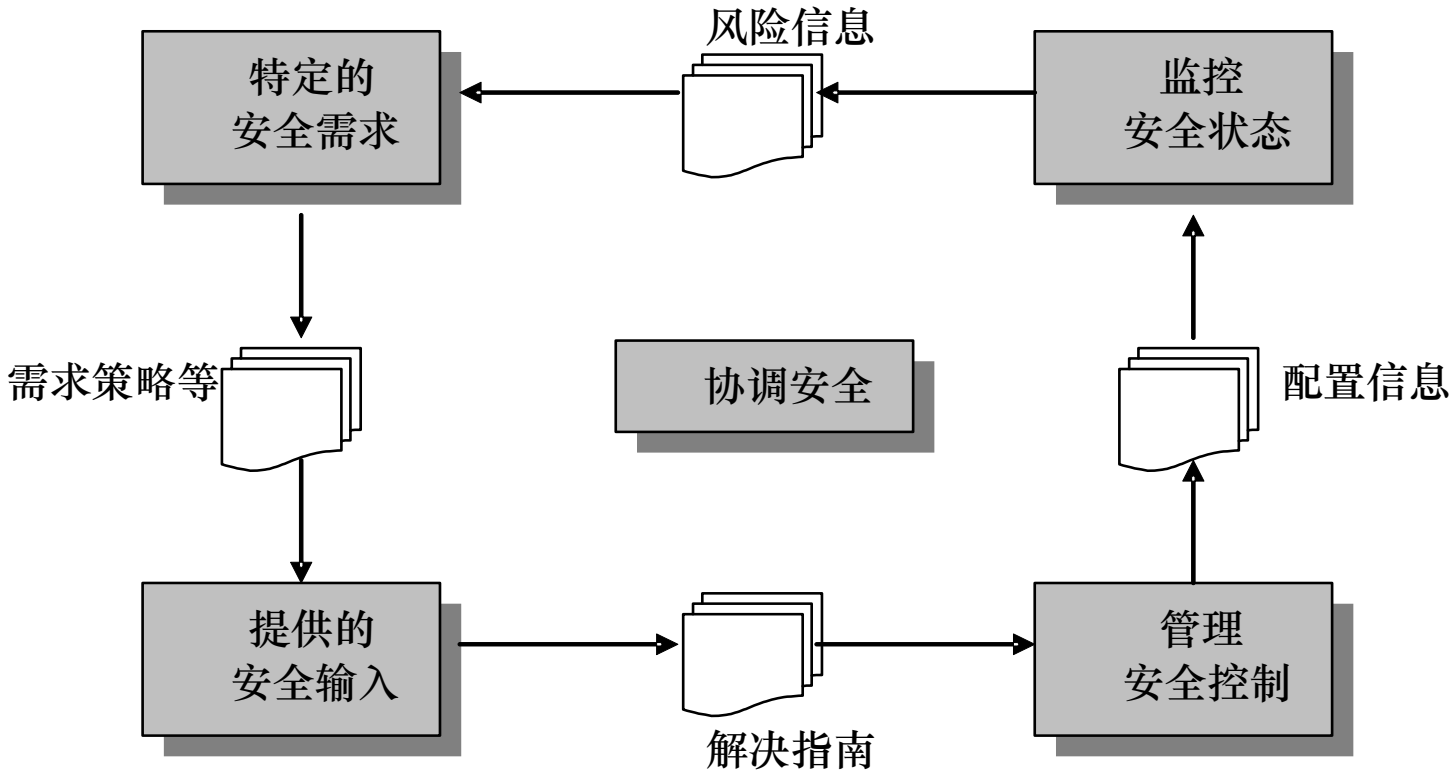
2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM的安全过程**
  - **SSE-CMM风险评估过程**



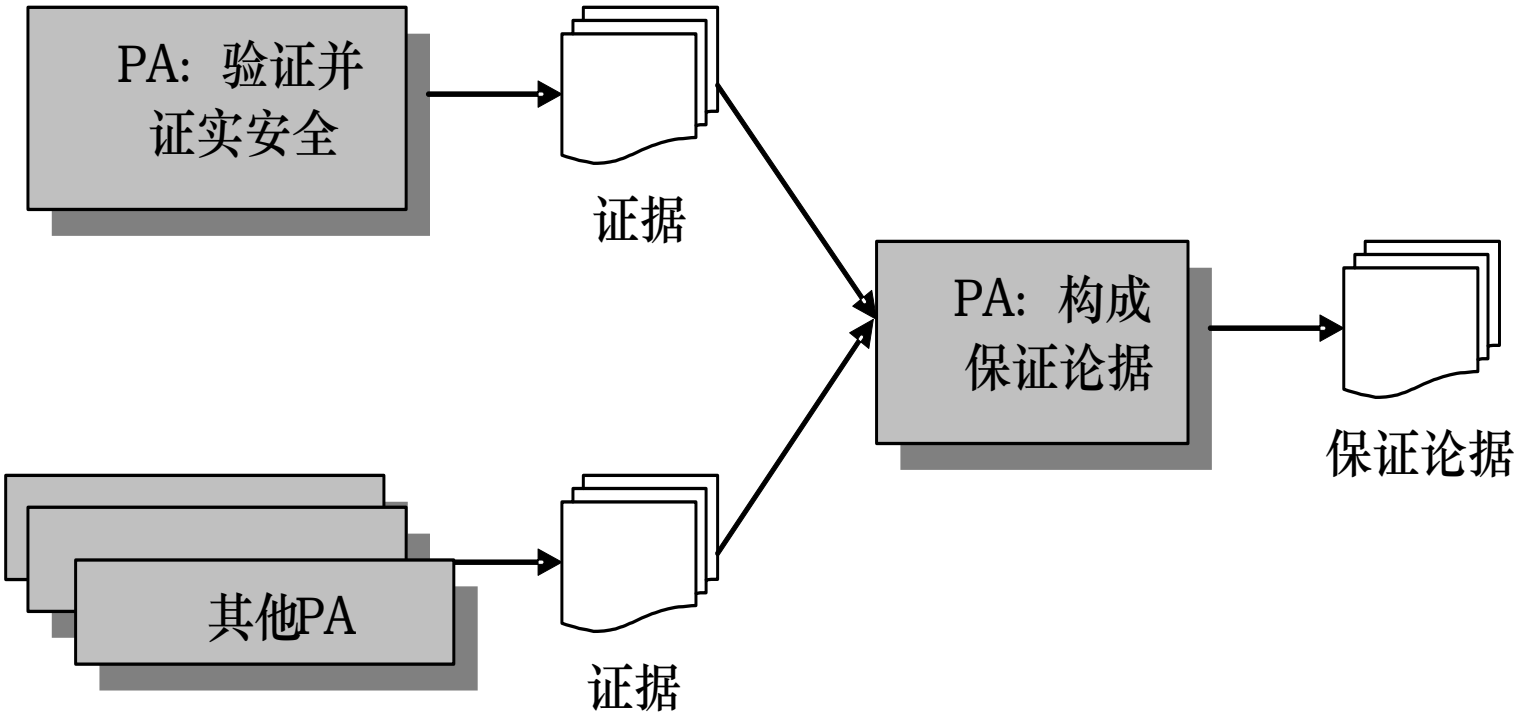
2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM的安全过程**
  - **SSE-CMM工程过程**



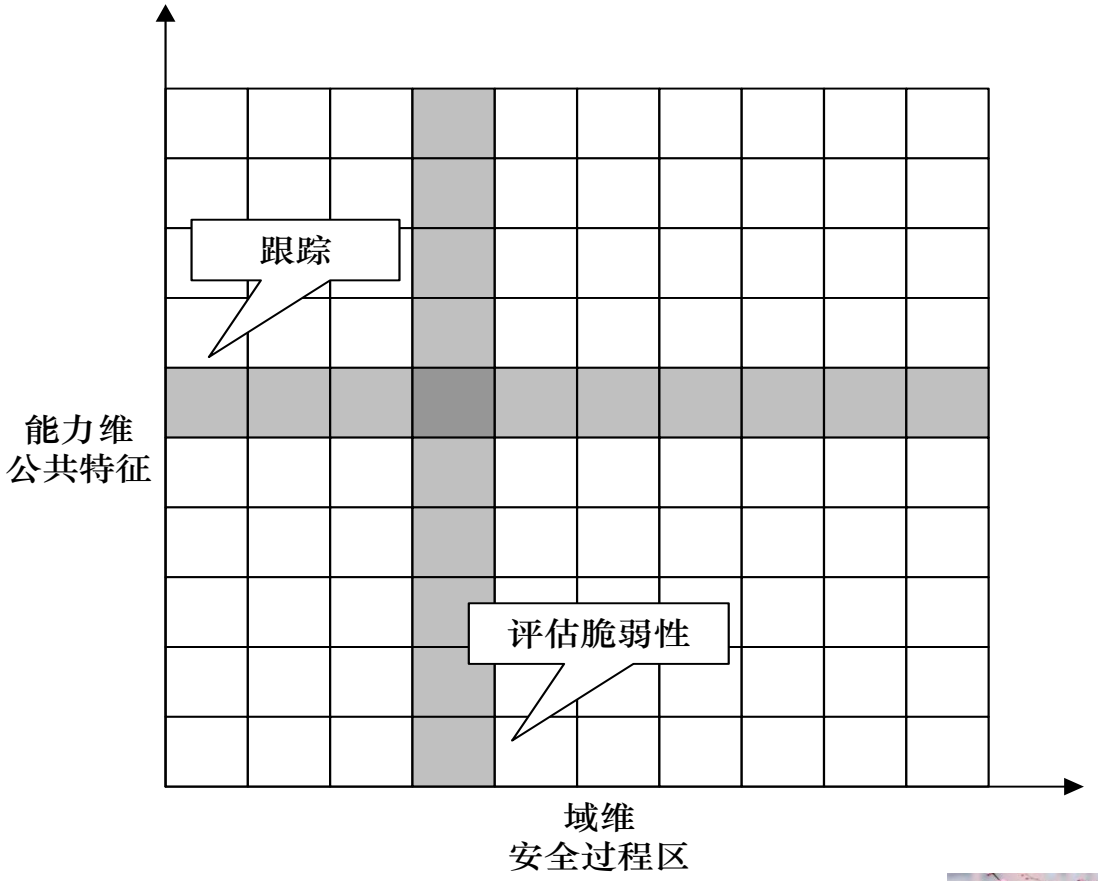
2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM的安全过程**
  - **SSE-CMM保证过程**



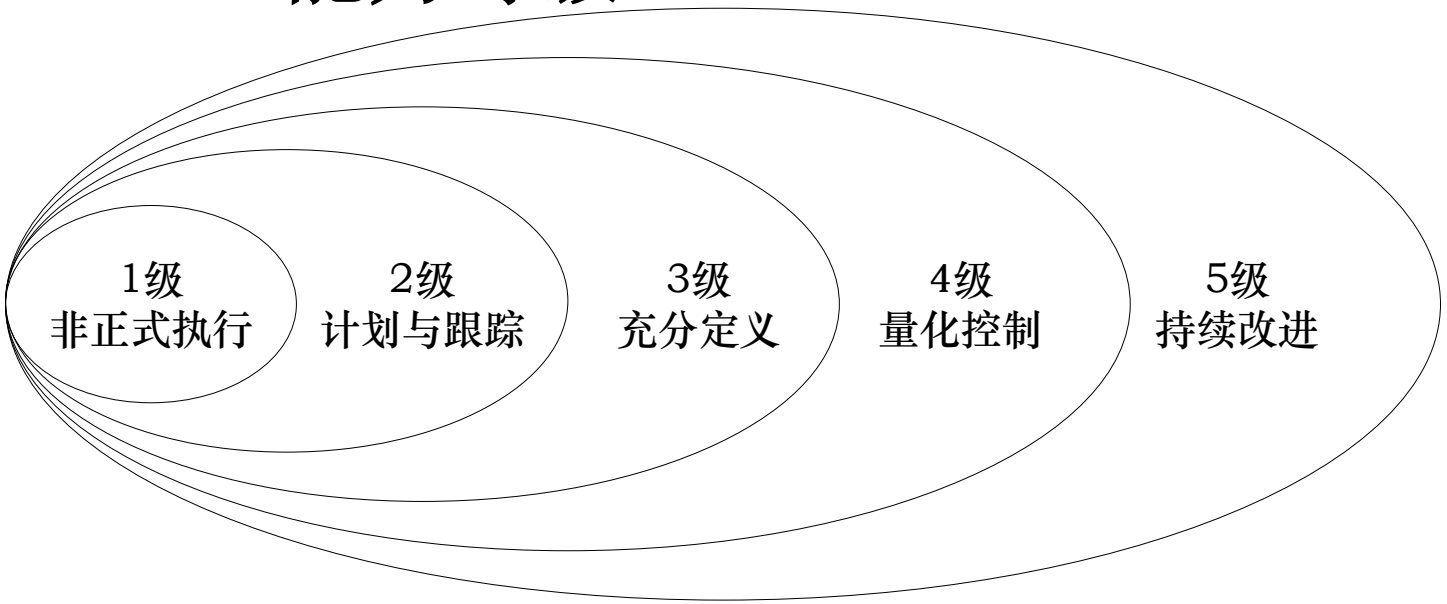
2.5 基于SSE-CMM的信息安全管理体系

- SSE-CMM体系结构



2.5 基于SSE-CMM的信息安全管理体系

- **SSE-CMM能力等级**



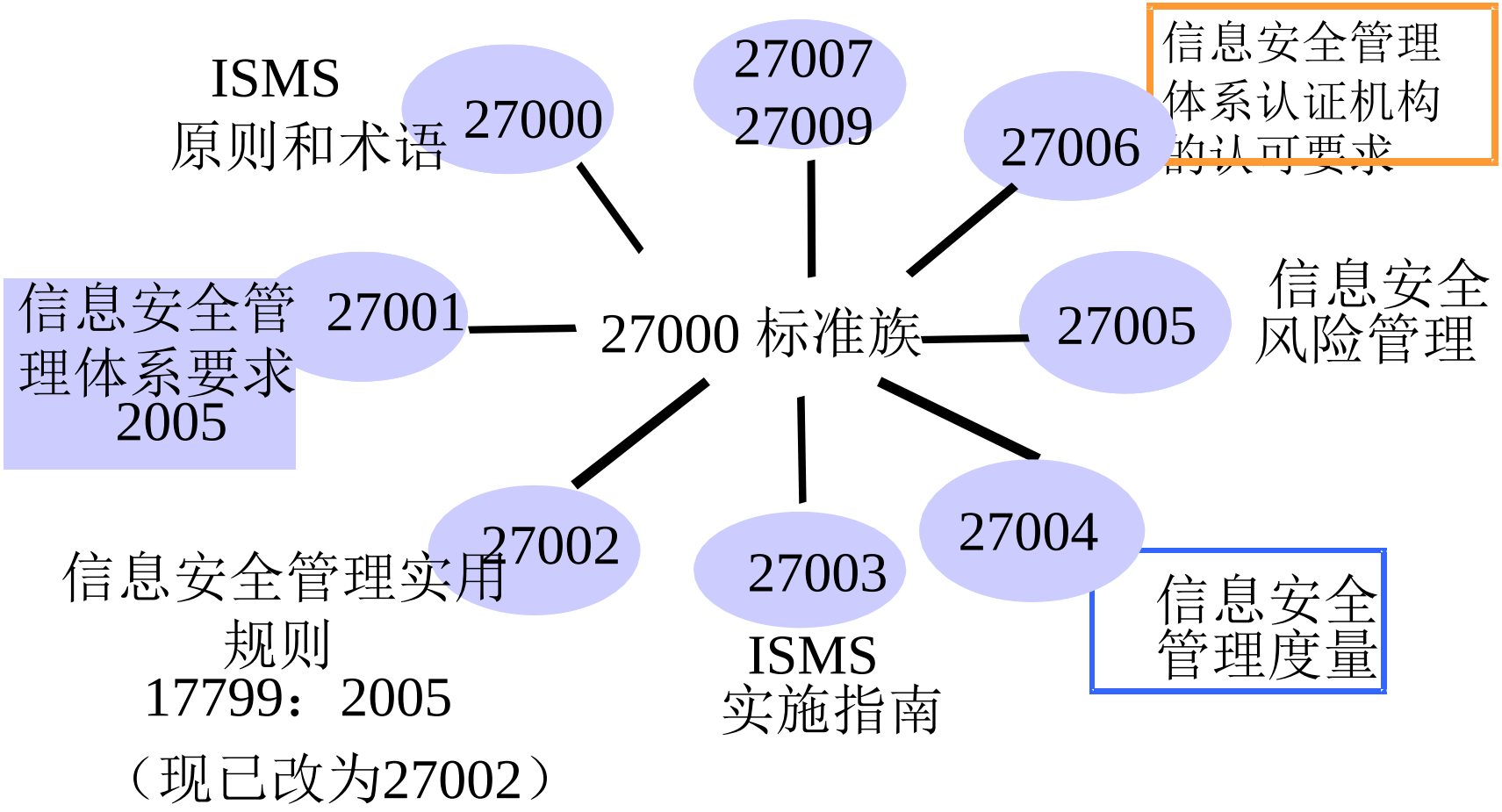
0级	1级	2级	3级	4级	5级
0级并不是真正的级别，因为它不包含任何通用实践，也完全不需要被测量	1级仅要求一个过程域的所有基本实践都被执行，但对执行的结果如何无明确要求	2级强调过程执行前的计划和执行中的检查，这使工程组织可以基于最终结果的质量来管理其实践活动	3级要求过程域包括的所有基本实践都按照一组完善定义的操作规范来进行（标准过程）	4级要求能够对工程组织的表现进行定量的度量和预测。过程管理成为客观的和准确的实践活动	5级要求为过程行为的高效和实用建有定量目标。可以准确地度量过程的持续改善所收到的效益

2.6 ISO/IEC 27001:2005标准

- 1. ISO SC27 WG1的ISMS系列
  - 2005年ISO正式推出27000系列
  - 初步考虑制定将近10个标准全面规范信息安全管理体系(ISMS)
  - 信息安全管理主要活动
    - 1.制定信息安全目标和实现目标的途径；
    - 2.建设信息安全组织机构，设置岗位、配置人员并分配职责；
    - 3.实施信息安全风险评估和管理；
    - 4.制定并实施信息安全策略；
    - 5.为实现信息安全目标提供资源并实施管理；
    - 6.信息安全的教育与培训；
    - 7.信息安全事故管理；
    - 8.信息安全的持续改进。

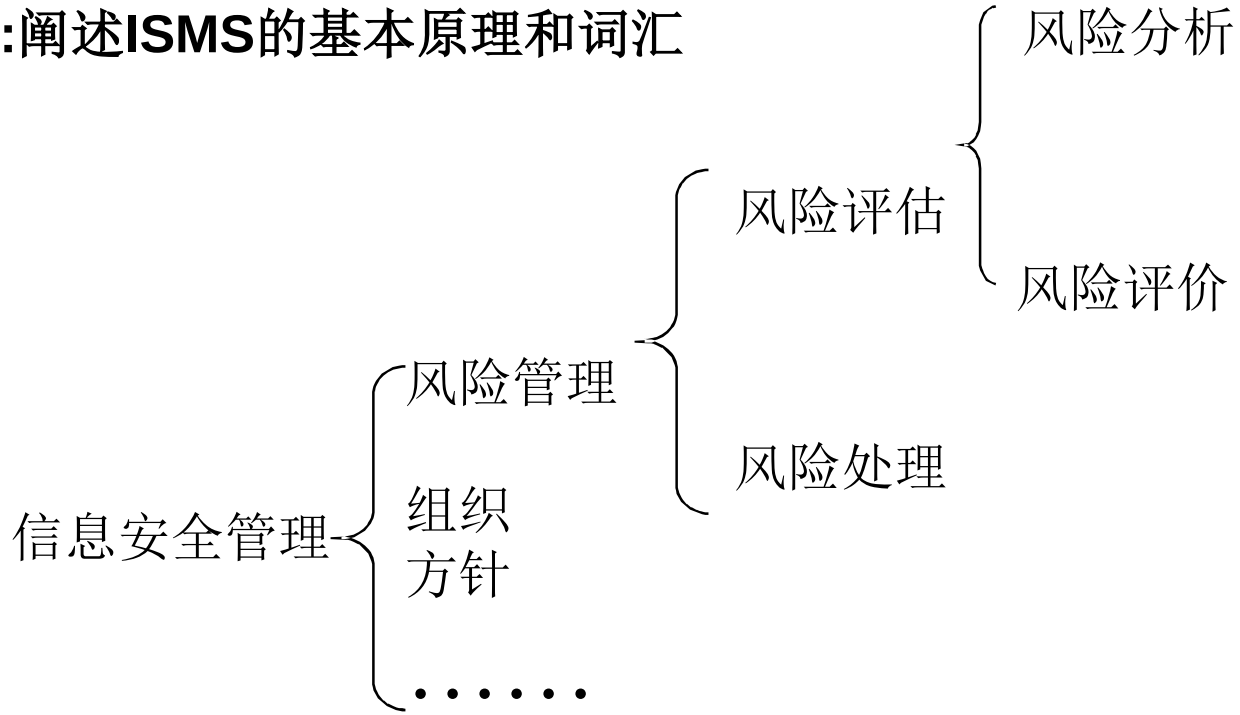
2.6 ISO/IEC 27001:2005标准

- **ISMS 27000安全管理体系**



2.6 ISO/IEC 27001:2005标准

- 信息安全管理标准体系27000
  - 名称:IS 27000 – Information security managementsystem fundamentals and vocabulary (NP)
  - 来源:整合改写13335
  - 内容:阐述ISMS的基本原理和词汇



2.6 ISO/IEC 27001:2005标准

- 信息安全管理标准体系27001
  - 名称:ISO/IEC 27001 – Information security management systems – Requirements(信息安全管理体系要求)
    - 全称：Information technology- Security techniques-Information security management systems-Requirements
  - 来源:源于BS7799-2
  - 内容:提出ISMS的基本要求
  - 状况:2005年正式发布
    - ISMS 信息安全管理体系
      - » 管理体系
      - » 信息安全相关
      - » ISO 27001 的"3 术语和定义-3.7"
    - Requirements 要求

2.6 ISO/IEC 27001:2005标准

- **1. 27001结构**

前　言

引　言

1 范围
2 规范性引用文件
3 术语和定义
4 信息安全管理体系（ISMS）
5 管理职责
6 内部ISMS审核
7 ISMS的管理评审
8 ISMS改进

0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Information security management system
    4.1 General requirements
    4.2 Establishing and managing the ISMS
        4.2.1 Establish the ISMS
        4.2.2 Implement and operate the ISMS
        4.2.3 Monitor and review the ISMS
        4.2.4 Maintain and improve the ISMS
    4.3 Documentation requirements
5. Management responsibility
6. Internal ISMS audits
7. Management review of the ISMS
8. ISMS improvement

附　录　A （规范性附录） 控制目标和控制措施

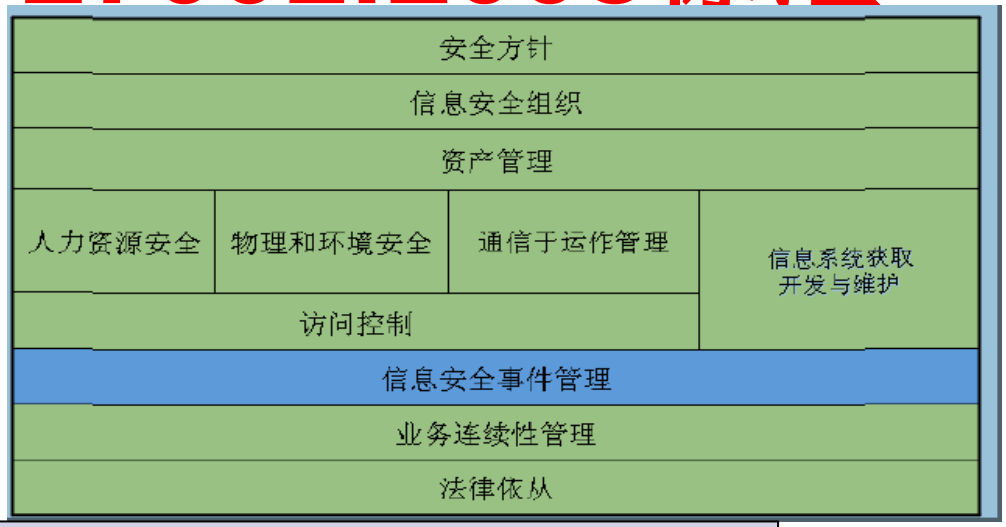
附　录　B （资料性附录） OECD原则和本标准

附　录　C （资料性附录） ISO 9001:2000, ISO 14001:2004和本标准之间的对照

Annex A → **ISO27001:2005, Annex A**
11 Clauses
39 Objectives
133 Controls

2.6 ISO/IEC 27001:2005标准

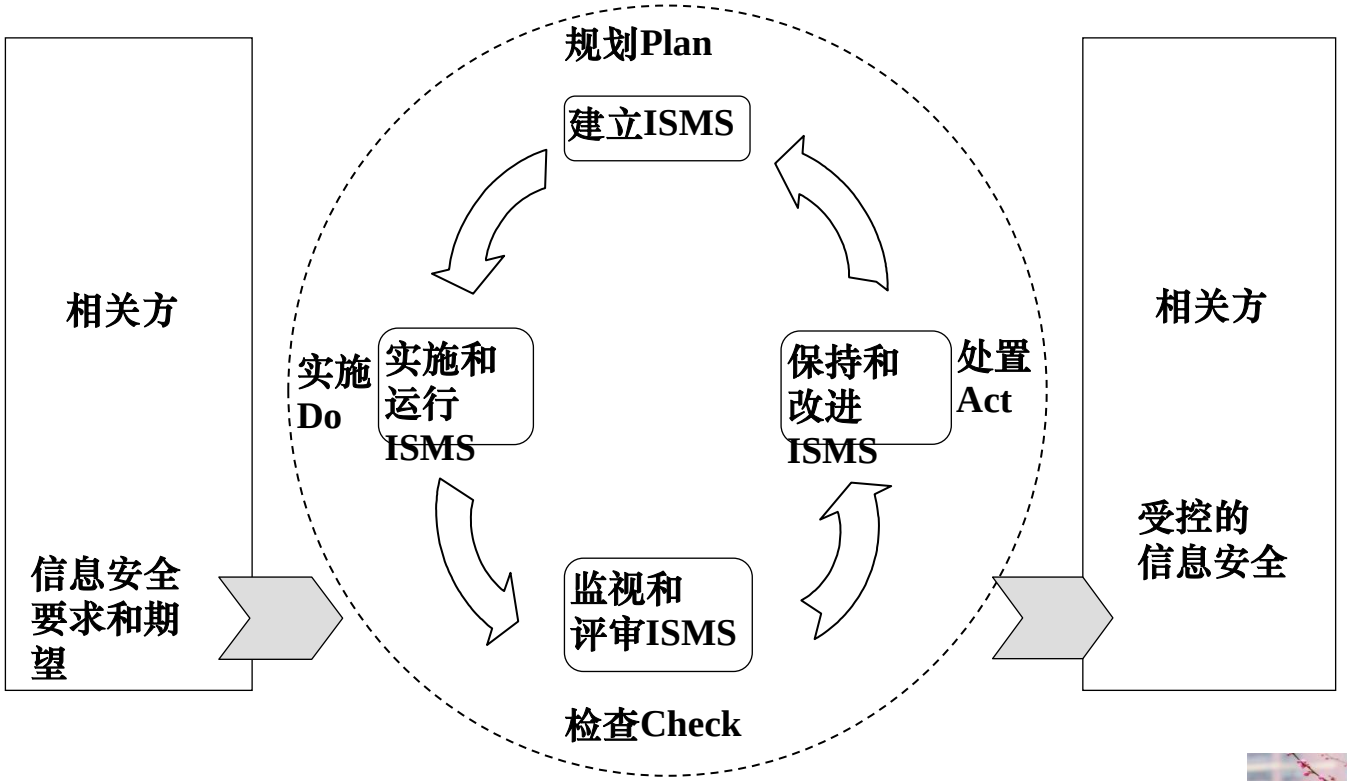
- **2.控制目标与控制措施**
  - **11个域、39个控制目标、133个控制措施**
  - **与BS7799相同**



安全策略（Information Security Policy）			
组织信息安全（Organization of Information Security）			
资产管理（Asset Management）			
人力资源安全（Human Resource Security）	物理和环境安全（Physical and Environmental Security）	通信和操作管理（Communications and Operations Management）	信息系统的获取、开发和维护（Information System Acquisition, Development and Maintenance）
访问控制（Access Control）			
信息安全事故管理（Information Security Incident Management）			
业务连续性管理（Business Continuity Management）			
合规性（Compliance）			

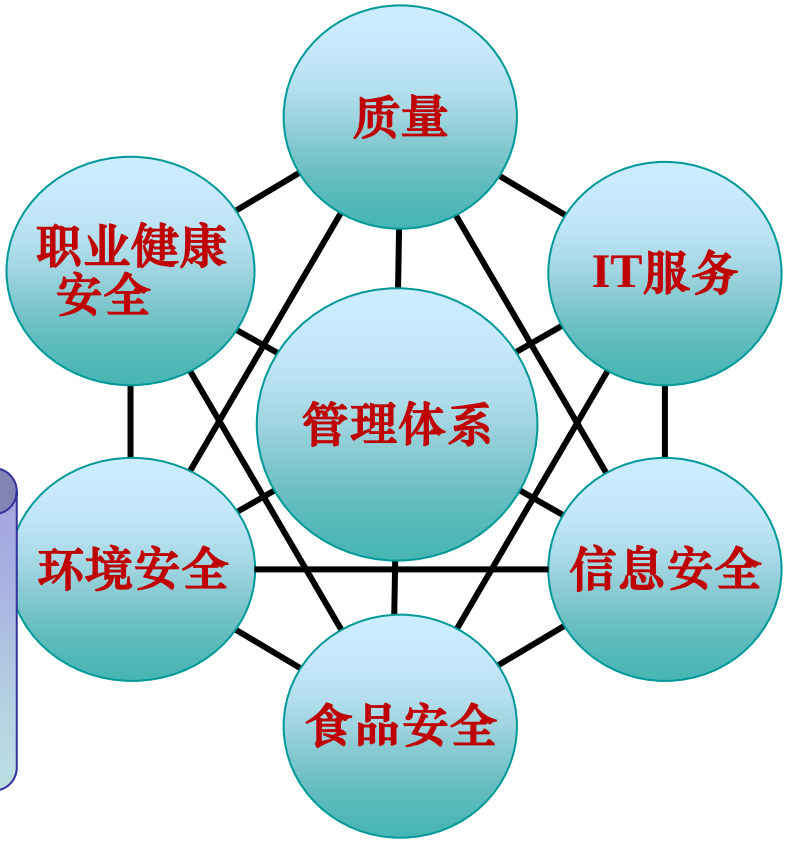
2.6 ISO/IEC 27001:2005标准

- **3. 27001的PDCA模型**
  - 一个组织应在其整体业务活动和所面临风险的环境下建立、实施、运行、监视、评审、保持和改进文件化的ISMS。



2.6 ISO/IEC 27001:2005标准

- 信息安全管理体系(ISMS):
  - 是整个管理体系的一部分，建立在业务风险的方法上，以：
    - 建立
    - 实施
    - 运作
    - 监控
    - 评审
    - 维护
    - 改进
  - 信息安全。



建设了ISMS，尤其是获取了ISO27001认证后，组织将在信息安全方面进入一个强制的良性循环。

2.6 ISO/IEC 27001:2005标准

- **4. 术语和定义**
  - **建立方针和目标并实现这些目标的相互关联或相互作用的一组要素。**
  - **管理体系包括组织结构，策略，规划，角色，职责，流程，程序和资源等。(ISO 27001"3 术语和定义-3.7")**
  - **管理的方方面面以及公司的所有雇员，均囊括在管理体系范围内。**

Quality management system (ISO 9001)

Environmental management system (ISO 14001)

Safety management system (OHSAS 18001)

Human Food Safety management system (HACCP)

IT Service Management System (ISO 20000)

Information security management system (ISO 27001)

2.6 ISO/IEC 27001:2005标准

- 信息安全属性
  - 保护信息的保密性、完整性和可用性(CIA);另外还包括诸如真实性，可核查性，不可否认性和可靠性等特性 (ISO 27001"3 术语和定义-3.4")
  - 机密性（Confidentiality）
    - 信息不能被未授权的个人，实体或者过程利用或知悉的特性 (ISO 27001"3 术语和定义-3.3")
  - 完整性（Integrity）
    - 保护资产的准确和完整的特性(ISO 27001"3 术语和定义-3.8").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）
    - 根据授权实体的要求可访问和利用的特性(ISO 27001"3 术语和定义-3.2").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

2.6 ISO/IEC 27001:2005标准

- 十大管理要项（BS7799）：
  - 信息安全策略：为信息安全提供管理指导和支持
  - 机构安全基础设施，目标包括：
    - 内部信息安全管理；
    - 保障机构的信息处理设施以及信息资产的安全；
    - 当信息处理的责任外包时，维护信息的安全性
  - 资产分类和控制：
    - 对资产进行分类和控制，确保机构资产和信息资产得到适当水平的保护。
  - 人员安全，其目标是：
    - 减少由于人为错误、盗窃、欺诈和设施误用等造成的风险；
    - 确保用户了解信息安全威胁，确保其支持机构的安全策略；
    - 减少安全事故和故障造成的损失，并从事故中吸取教训。
  - 物理和环境安全，其目标包括：
    - 防止对业务场所和信息的非法访问、破坏以及干扰；
    - 防止资产的丢失、破坏、威胁对业务活动的中断；
    - 防止信息或信息处理设施的损坏或失窃。

2.6 ISO/IEC 27001:2005标准

- 十大管理要项（BS7799）：
  - 通信和操作的管理，其目标是
    - 确保信息设施处理的正确、安全操作；
    - 把系统错误的风险降到最低；
    - 保护软件和信息的完整性；
    - 维护信息处理和通信的完整性和有效性；
    - 加强对网络中信息和支持设施的保护；
    - 防止资产损坏和活动的中断；
    - 在机构间交换信息时，防止信息的丢失、篡改以及误用等情况。
  - 系统访问控制，其目标是：
    - 控制对信息的访问；
    - 防止对信息系统的非授权访问；
    - 确保对网络服务的保护；
    - 防止未授权的计算机访问；
    - 检测未授权的活动；
    - 确保便携式计算机和无线网络的信息安全。

2.6 ISO/IEC 27001:2005标准

ISO27001

正式的标准
可认证的标准
管理体系的要求
控制措施的要求

***为设计控制措施提供实施指南**

ISO 17799

实施细则（一整套最佳实践）
控制措施的实施建议和实施指导
ISO27001的附录A的细化与补充

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容

0. 引言
1. 概述
2. 规范性应用文件
3. 术语和定义

27001辅助部分

4. 信息安全管理体系(ISMS)
   - 4.1 总要求
   - 4.2 建立和管理ISMS
     - 4.2.1 建立 ISMS
     - 4.2.2 实施和运维 ISMS
     - 4.2.3 监控和评审 ISMS
     - 4.2.4 维护和改进 ISMS
   - 4.3 文件要求
5. 管理职责
6. ISMS的内部审核
7. ISMS的管理评审

27001核心部分（条款4-8）

27001核心部分

附录B OECD原则与本标准

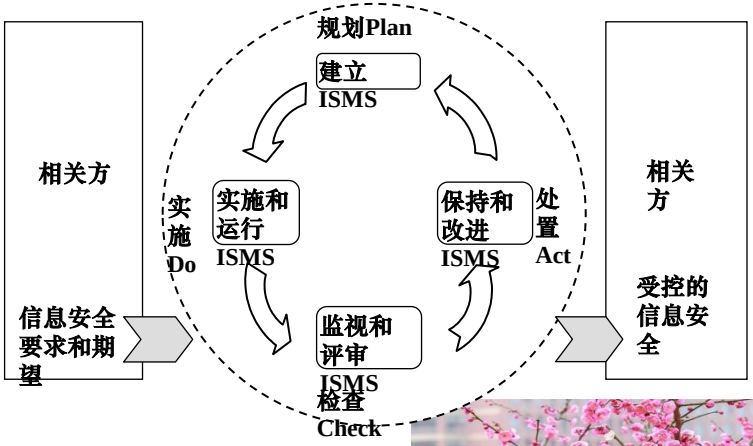
附录C ISO9001:2000和ISO14001:2004对照

参考书目

27001辅助部分

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 条款的重要性
    - 本标准规定的要求是通用的，适用于各种类型、规模和特性的组织。组织声称符合本标准时，对于4、5、6、7和8章的要求不能删减。
    - 为了满足风险接受准则所必须进行的任何控制措施的删减（附录A），必须证明是合理的，且需要提供证据证明相关风险已被负责人员接受。除非删减不影响组织提供由风险评估和适用法律法规要求所确定的安全需求的能力和/或责任，否则不能声称符合本标准。
  - 27001核心内容（4-8条款）
    - 应用于ISMS过程的PDCA模型

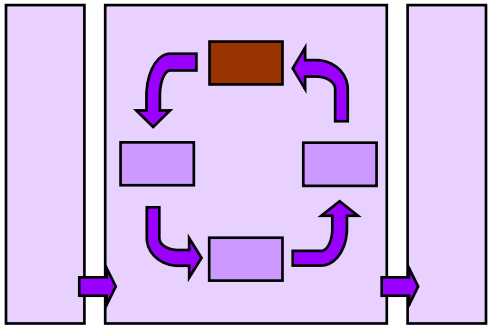


2.6 ISO/IEC 27001:2005标准

- **5. ISO/IEC 27001:2005 内容**
  - **27001核心内容（4-8条款）**

PDCA各阶段	内容	对应标准条款
PLAN	规定你应该做什么 并形成文件	4.1 4.2.1 4.3 5
DO	做文件已规定的事情	4.2.2
CHECK	评审你所做的事情的符合性	4.2.3 6 7
ACT	采取纠正和预防措施， 持续改进	4.2.4 8

2.6 ISO/IEC 27001:2005标准



- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--P：建立ISMS
    - 4.1 总要求

      风险+PDCA+文件化的ISMS
    - 4.2.1 建立ISMS

      a) 范围(Scope of the ISMS)
      b) 策略(ISMS Policy)
      c) ~ h) 风险评估和管理 (Risk Management)
      i) 管理者授权实施和运行ISMS
      j) 适用声明(SOA)
    - 4.3 文件要求
    - 5 管理职责

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--P：建立ISMS
    - 4.2.1 a) ISMS范围
    - 根据组织及其业务特点、位置、资产、技术，确定ISMS的范围和边界，包括对例外于此范围的对象作出详情和合理性的说明 。
      - 组织：所有部门？还是某个业务部？
      - 业务：所有业务系统还是部门相关系统？
      - 位置：一个大楼？还是全北京，全省，全国？
      - 资产：软件、硬件、数据、服务、人员？
    - 拿证过外审须提交文件《ISMS范围》

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--P：建立ISMS
    - 4.2.1 b) ISMS Policy
    - 根据组织及其业务特点、位置、资产和技术，确定ISMS方针，应：
      - 1)为其目标建立一个框架并为信息安全行动建立整体的方向和原则；
      - 2)考虑业务和法律法规的要求，及合同中的安全义务；
      - 3)在组织的战略性风险管理环境下，建立和保持ISMS；
      - 4)建立风险评价的准则[见4.2.1 c]；
      - 5)获得管理者批准。
    - 拿证过外审须提交文件《ISMS策略》

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--P：建立ISMS
    - 4.2.1 c) ~ h) 风险管理
      - C)风险评估方法
      - D)识别风险(执行风险评估)
      - E) 分析风险
      - F) 识别和评价风险处置的可选措施
      - G)为处理风险选择控制目标和控制措施
      - H) 获得管理者对建议的残余风险的批准

如何做风险评估和风险处置?

    - 拿证过外审须提交文件《风险评估方法描述》、《风险评估报告》、《风险处置计划》

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--P：建立ISMS
    - 4.2.1 c) ~ h) 风险管理

ISO27001

正式的标准
可认证的标准
管理体系的要求
控制措施的要求

为风险管理提供方法

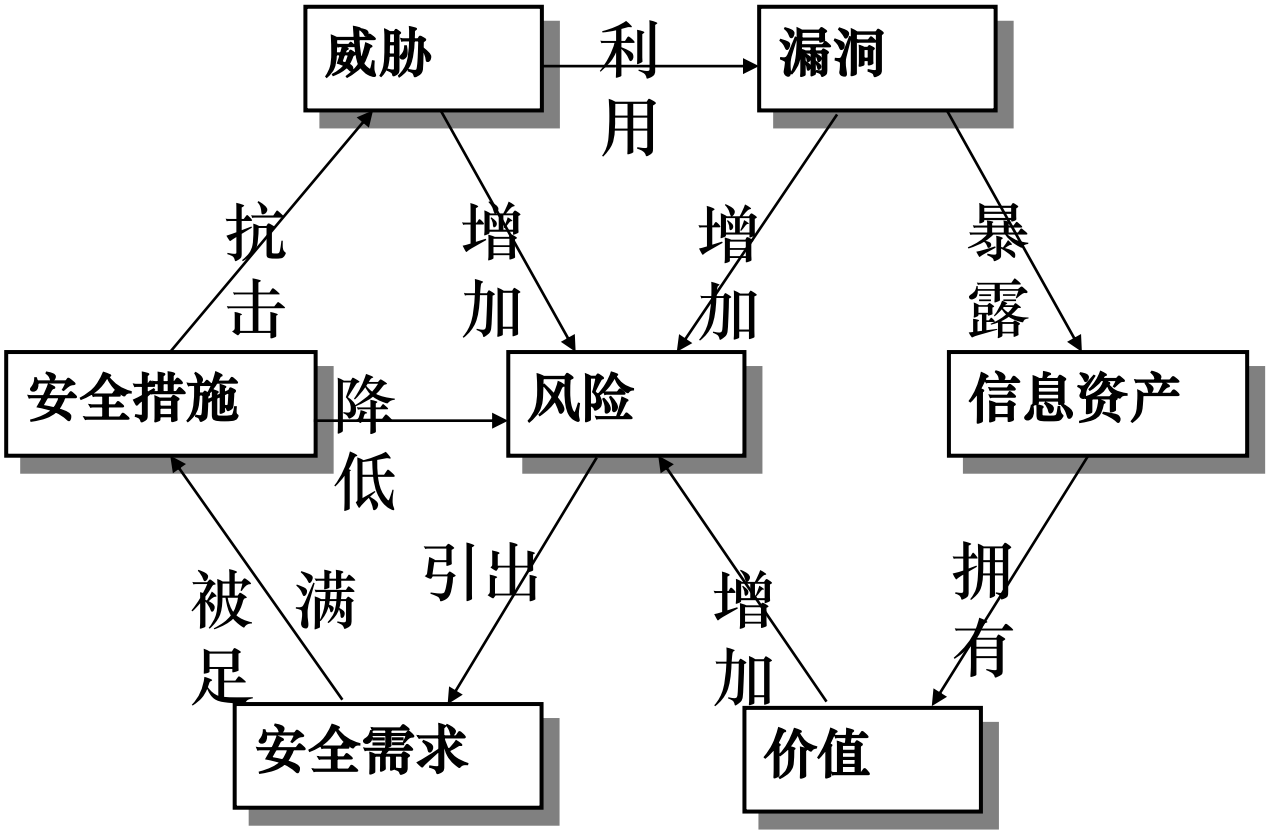
ISO TR 13335

风险管理方法论
提供如何识别风险到风险处置
对ISO27001的风险评估方法的细化和补充

“ISO270014.2.1 c) 注”：风险评估具有不同的方法。在ISO/IEC TR 13335-3（IT安全管理指南：IT安全管理技术）中描述了风险评估方法的例子

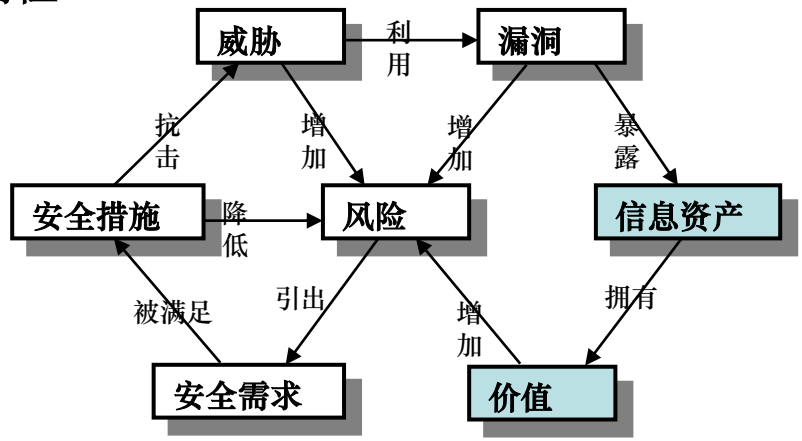
2.6 ISO/IEC 27001:2005标准

- 27001以风险为核心的安全模型



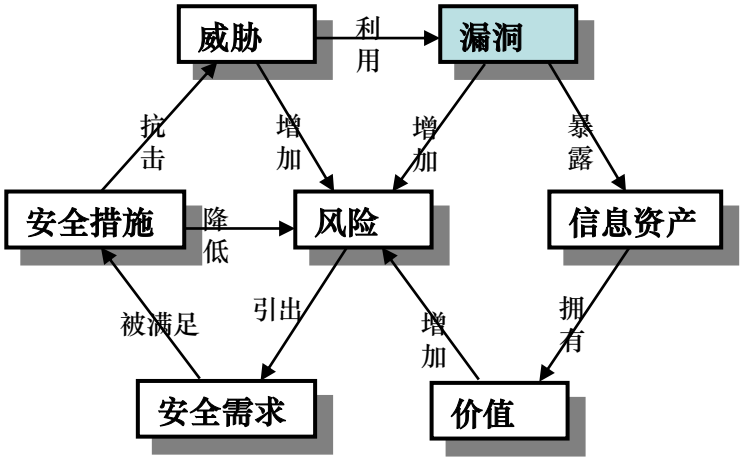
2.6 ISO/IEC 27001:2005标准

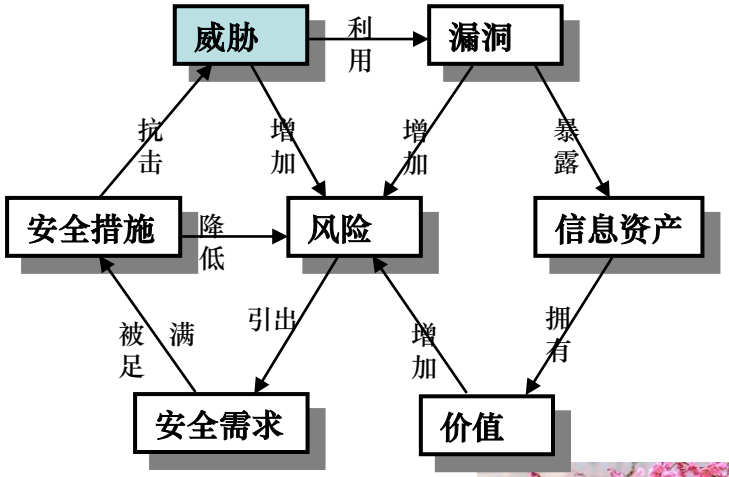
- **27001风险模型**
  - 信息资产与价值
    - 任何对组织有价值的东西[ISO/IEC27001:2005 3 术语和定义]
    - 资产是企业、机构直接赋予了价值因而需要保护的东西。
    - 信息资产是指组织的信息系统、其提供的服务以及处理的数据。
    - 资产（Asset）的根本属性是：价值（C、I、A值）
      - C是机密性，I是完整性，A是可用性



2.6 ISO/IEC 27001:2005标准

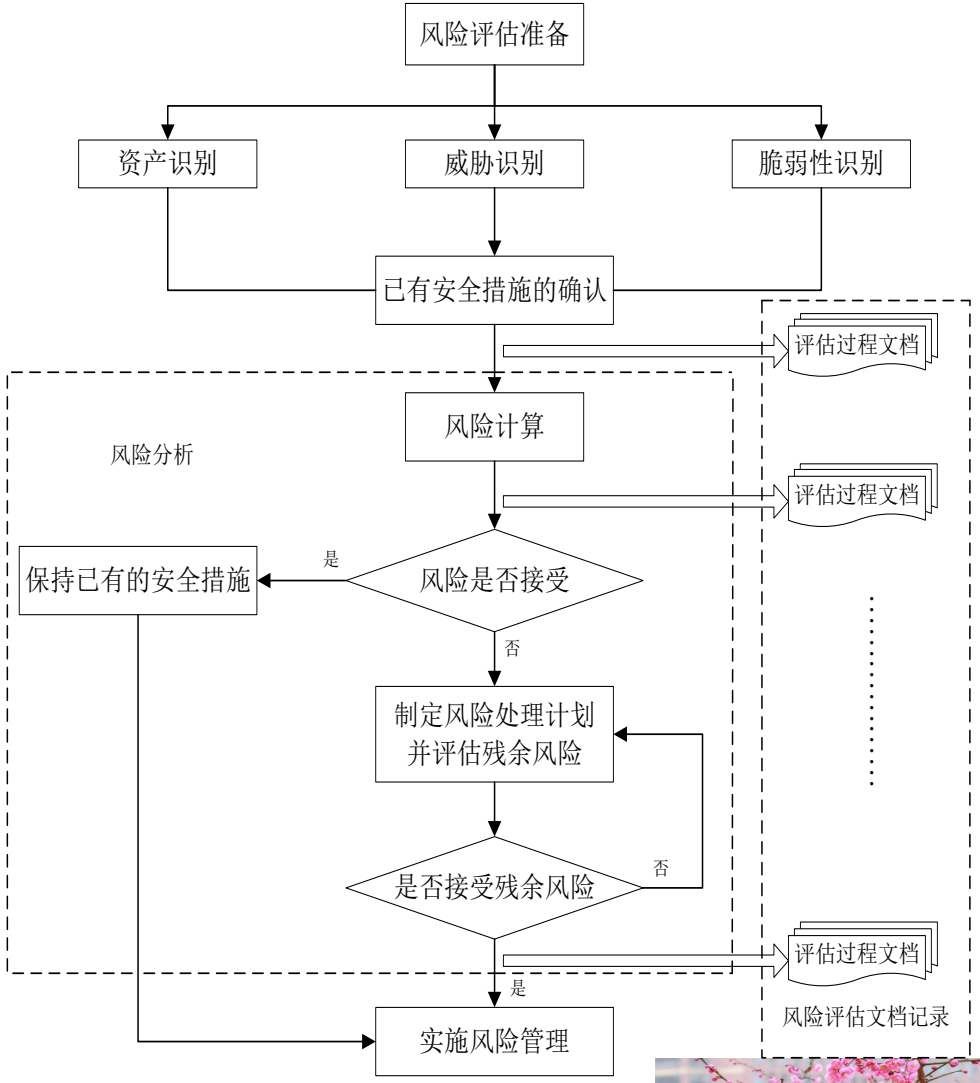
- **27001风险模型**
  - **脆弱性（Vulnerability）与威胁（Threat）**
    - 脆弱性是资产本身存在的，它可以被威胁利用、引起资产或商业目标的损害。
    - 脆弱性包括物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各种资产的脆弱性。
    - 脆弱性的根本属性是：严重程度（脆弱性被利用后对资产的损害程度、脆弱性被利用的难易程度）
    - 威胁是对组织的资产引起不期望事件而造成的损害的潜在可能性。
    - 威胁可以分为人为威胁（故意、非故意）和非人为威胁（环境、故障）2种。
    - 威胁的根本属性是：出现的频率（还包括威胁的能力，威胁的决心。）





2.6 ISO/IEC 27001:2005标准

- **27001风险评估流程**



2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--4.3 文件要求
  - 文件的作用
    - 是指导组织有关信息安全工作方面的内部“法规”--使工作有章可循。
    - 是组织实际工作的标准。ISMS文件是根据ISMS标准和组织需要“量身定做”的实际工作的标准。对一般员工来说，在其实际工作中，可以不过问ISMS标准(ISO/IEC 27001:2005)，但必须按照ISMS文件的要求执行工作。
    - 是控制措施（controls）的重要部分。
    - 提供客观证据--为满足相关方要求，以及持续改进提供依据。
    - 提供适宜的内部培训的依据。
    - 提供ISMS审核（包括内审和外审）的依据，文件审核、现场审核。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--4.3 文件要求
    - 4.3.1 总则
      - 包含文件

序号	文件名称	标准条款
1	ISMS策略和目标	4.3.1 a)
2	ISMS范围	4.3.1 b)
3	风险评估方法的描述	4.3.1 b)
4	风险评估报告	4.3.1 e)
5	风险处理计划	4.3.1 f)
6	适用性声明	4.3.1 i)
7	标准要求的纪录	4.3.1 h)
8	文件控制程序	4.3.2
9	记录控制程序	4.3.3
10	内部审核程序	6
11	管理评审程序	7.1
12	纠正措施程序	8.2
13	预防措施程序	8.3

注1：本标准出现“形成文件的程序”之处，
即要求建立该程序，形成文件，并加以实施和保持。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--4.3.2 文件控制
    - a)批准
    - b)评审、更新并再批准；
    - c)修订状态得到标识；
    - d)在使用处可获得适用文件；
    - e)清晰、易于识别；
    - f)对需要的人员可用，传输、贮存和最终销毁；
    - g)外来文件标识；
    - h)分发控制；
    - i)防止作废文件的非预期使用；
    - j)作废文件的标识。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA--4.3.3 记录控制
    - a)建立并保持，以提供证据。
    - b)保护和控制。应考虑相关法律法规要求和合同义务。
    - c)清晰、易于识别和检索。
    - d)记录的标识、贮存、保护、检索、保存期限和处置所需的控制措施应形成文件并实施。
    - e)记录的详略程度应通过管理过程确定。
    - f)应保留4.2中列出的过程执行记录和所有发生的与ISMS有关的安全事故的记录。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—5 管理
  - 5.1 管理承诺
    - a)制定ISMS方针；
    - b)确保ISMS目标和计划得以制定；
    - c)建立信息安全的角色和职责；
    - d)向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性；
    - e)提供足够资源，以建立、实施、运行、监视、评审、保持和改进ISMS （见5.2.1）；
    - f)决定接受风险的准则和风险的可接受级别；
    - g)确保ISMS内部审核的执行（见第6章）；
    - h)实施ISMS的管理评审（见第7章）。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—5 管理
    - 5.2 资源管理

5.2.1 资源提供

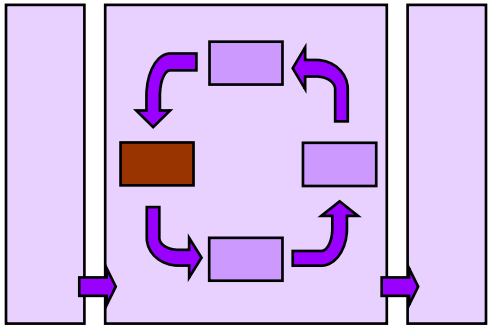
应确定并提供信息安全工作所需的资源－人、财、物

5.2.2 培训、意识和能力

① 确保所有分配有ISMS职责的人员具有执行所要求任务的能力

② 确保所有相关人员意识到其信息安全活动的适当性和重要性，以及如何为达到ISMS目标做出贡献。

2.6 ISO/IEC 27001:2005标准



- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—D：实施

PDCA各阶段	内容	对应标准条款
PLAN	**规定你应该做什么 并形成文件**	4.1 4.2.1 4.3 5
DO	**做文件已规定的事情**	4.2.2
C-检查 监视和评审 ISMS	**对照ISMS方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审。**	4.2.3 6 7
A-处置 保持和改进 ISMS	**基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。**	4.2.4 8

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—D：实施
    - 4.2.2 实施和运行ISMS

a) 制定风险处理计划（见条款5）。

b) 实施风险处理计划。

c) 实施4.2.1 (g）中所选择的控制措施。

d) 测量所选择的控制措施或控制措施集的有效性（见条款4.2.3c)）。

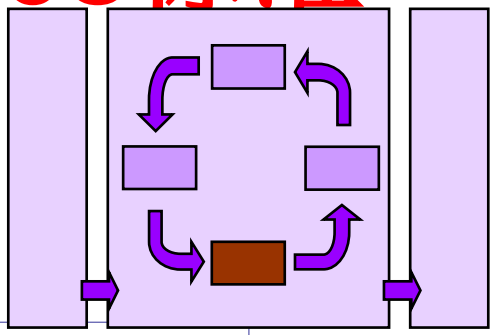
e) 实施培训和意识教育计划（见条款5.2.2）。

f) 管理ISMS的运行。

g) 管理ISMS的资源（见条款5.2）。

h) 事件和事故响应（见条款4.2.3 a）。

2.6 ISO/IEC 27001:2005标准



- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—C：评审

PDCA各阶段	内容	对应标准条款
PLAN	规定你应该做什么 并形成文件	4.1 4.2.1 4.3 5
DO	做文件已规定的事情	4.2.2
CHECK	评审你所做的事情的符合性	4.2.3 6 7
A-处置 保持和改进 ISMS	基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。	4.2.4 8

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—C：评审
    - 4.2.3 监视和评审 ISMS

a) 执行监视和评审程序和其它控制措施。

b) ISMS有效性的定期评审。

c) 测量控制措施的有效性以验证安全要求是否被满足。

d) 按照计划的时间间隔进行风险评估的评审。

e) 按计划的时间间隔，对ISMS进行内部审核（见条款6）。

f) 定期对ISMS进行管理评审（见条款 7）。

g) 考虑监视和评审活动的结果，以更新安全计划。

h) 记录可能影响ISMS的有效性或执行情况的措施和事件（见4.3.3）。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—C：评审
    - 6 内部评审– 术语
      - 审核 audit
        - » 为获得审核证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程。
      - 内部审核 internal audit
        - » 有时称为第一方审核，用于内部目的的，由组织自己或以组织名义进行，可作为组织自我合格声明的基础。（条款4.2.3 注）
      - 审核员 auditor
        - » 有能力实施审核的人员。
      - 审核方案 audit programme
        - » 针对特定时间段所策划，并具有特定目的的一组(一次或多次)审核
      - 符合（合格） conformity
        - » 满足要求
      - 不符合（不合格） nonconformity
        - » 未满足要求

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—C：评审
    - 6 内部评审–条款
      - 按照计划的时间间隔进行内部ISMS审核。
      - 审核方案。
      - 审核的客观和公正，审核员不应审核自己的工作。
      - 文件化内审程序并定义清晰的职责和要求。
      - 受审核区域的管理者应消除不符合及其原因，并跟踪验证。
      - ISO19011:2002 给出了审核指南。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—C：评审
    - 7.1 管理评审– 总则

      - 按照计划的时间间隔进行管理评审，至少一年一次。
      - 包括评估ISMS改进的机会和变更的需要。
      - 包括信息安全方针和信息安全目标。
      - 评审报告和评审记录。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—C：评审
    - 7.2 管理评审– 评审输入

a) ISMS审核和评审的结果；

b) 相关方的反馈；

c) 组织用于改进ISMS执行情况和有效性的技术、产品或程序；

d) 预防和纠正措施的状况；

e) 以往风险评估没有充分强调的脆弱点或威胁；

f) 有效性测量的结果；

g) 以往管理评审的跟踪措施；

h) 可能影响ISMS的任何变更；

i) 改进的建议。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—C：评审
    - 7.3 管理评审– 评审输出

a) ISMS有效性的改进；

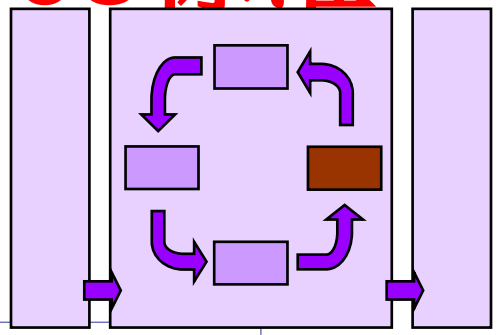
b) 风险评估和风险处理计划的更新；

c) 必要时修改影响信息安全的程序，以响应内部或外部可能影响ISMS的事件；

d) 资源需求；

e) 正在被测量的控制措施的有效性的改进。

2.6 ISO/IEC 27001:2005标准

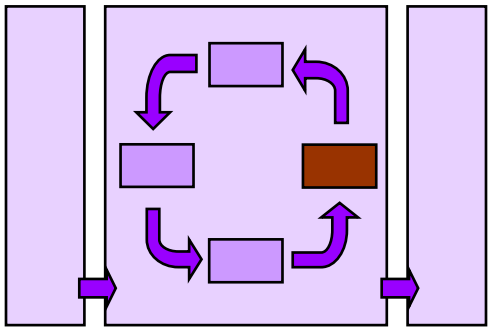


- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—A：处置

PDCA各阶段	内容	对应标准条款
PLAN	规定你应该做什么 并形成文件	4.1 4.2.1 4.3 5
DO	做文件已规定的事情	4.2.2
CHECK	评审你所做的事情的符合性	4.2.3 6 7
ACT	采取纠正和预防措施， 持续改进	4.2.4 8

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—A：处置
    - 4.2.4 保持和改进ISMS



组织应经常：

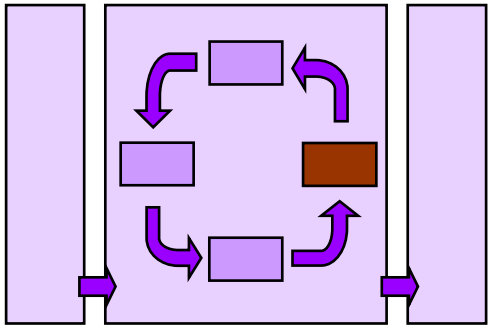
a) **实施已识别的ISMS改进措施。**

b) **依照8.2和8.3采取合适的纠正和预防措施。从其它组织和组织自身的安全经验中吸取教训。**

c) **向所有相关方沟通措施和改进措施，其详细程度应与环境相适应，需要时，商定如何进行。**

d) **确保改进达到了预期目标。**

2.6 ISO/IEC 27001:2005标准



- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—A：处置
  - 8 ISMS改进
    - 持续改进 continual improvement
      - 增强满足要求的能力的循环活动。
    - 预防措施 preventive action
      - 为消除潜在不符合或其他潜在不期望情况的原因所采取的措施。
    - 纠正措施 corrective action
      - 为消除已发现的不符合或其他不期望情况的原因所采取的措施。
  - 8.1 持续改进
    - 组织应通过使用信息安全方针、安全目标、审核结果、监视事件的分析、纠正和预防措施以及管理评审（见第7章），持续改进ISMS的有效性。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—A：处置
    - 8.2 预防措施

① 应确定措施，以消除潜在不符合的原因，防止其发生。

② 预防措施程序应规定以下要求：

a) 识别潜在的不符合及其原因；

b) 评价防止不符合发生的措施需求；

c) 确定和实施所需要的预防措施；

d) 记录所采取措施的结果（见4.3.3）；

e) 评审所采取的预防措施。

③ 应识别变化的风险，并识别针对重大变化的风险的预防措施的要求。

④ 预防措施的优先级要根据风险评估的结果确定。

⑤ 预防不符合的措施通常比纠正措施更节约成本。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001核心内容（4-8条款）
  - PDCA—A：处置
    - 8.3 纠正措施

① 应采取措施消除与ISMS要求不符合的原因，以防止再发生

② 纠正措施程序应规定以下要求：

a) 识别不符合；

b) 确定不符合的原因；

c) 评价确保不符合不再发生的措施需求；

d) 确定和实施所需要的纠正措施；

e) 记录所采取措施的结果（见4.3.3）；

f) 评审所采取的纠正措施。

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
    - 0.2 过程方法
    - 0.3 与其他管理体系的兼容性
    - 重要提示
      - 1.2 应用
      - 2 规范性引用文件
      - 3 术语和定义
    - 附录A 控制目标和控制措施
    - 附录B OECD原则与本标准
    - 附录C ISO9001:2000和ISO14001:2004对照
    - 参考书目

- **5. ISO/IEC 27001:2005 内容**
  - **27001其他相关方面**

0. 引言
1. 范围
2. 规范性应用文件
3. 术语和定义

27001辅助部分

4. 信息安全管理体系(ISMS)
   - 4.1 总要求
   - 4.2 建立和管理ISMS
     - 4.2.1 建立 ISMS
     - 4.2.2 实施和运维 ISMS
     - 4.2.3 监控和评审 ISMS
     - 4.2.4 维护和改进 ISMS
   - 4.3 文件要求
5. 管理职责
6. ISMS的内部审核
7. ISMS的管理评审
8. ISMS 改进

27001核心部分 (条款4-8)

附录A 控制目标和控制措施
附录B OECD原则与本标准

27001核心部分

附录C ISO9001:2000和ISO14001:2004对照
参考书目

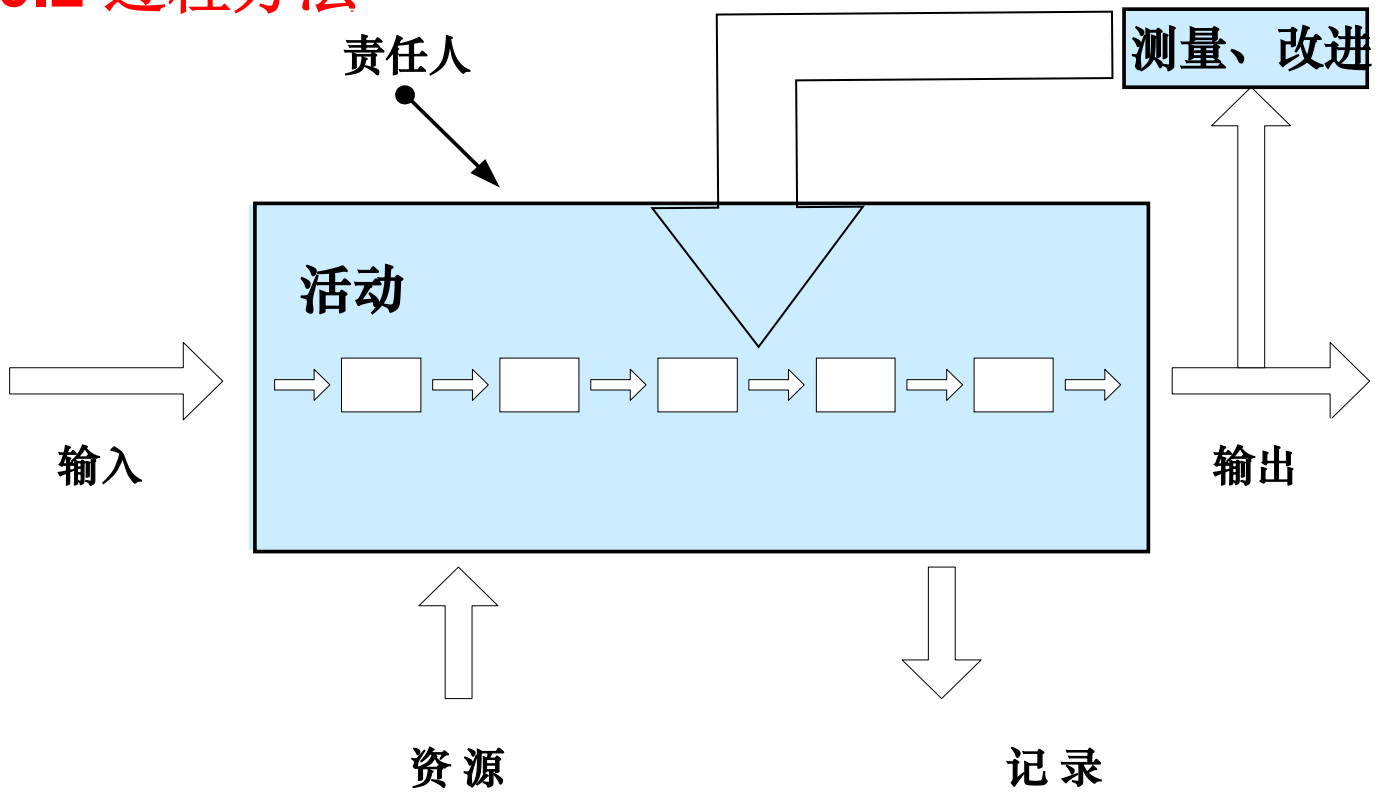
27001辅助部分

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 条款0.2 过程方法
    - 过程 process
      - 一组将输入转化为输出的相互关联或相互作用的活动。
    - 过程方法 process approach
      - 一个组织内过程的系统的运用，连同这些过程的识别和相互作用及其管理，可称之为“过程方法”。
      - （系统地识别和管理组织所应用的过程，特别是这些过程之间的相互作用，称为过程方法。—ISO9000:2000）

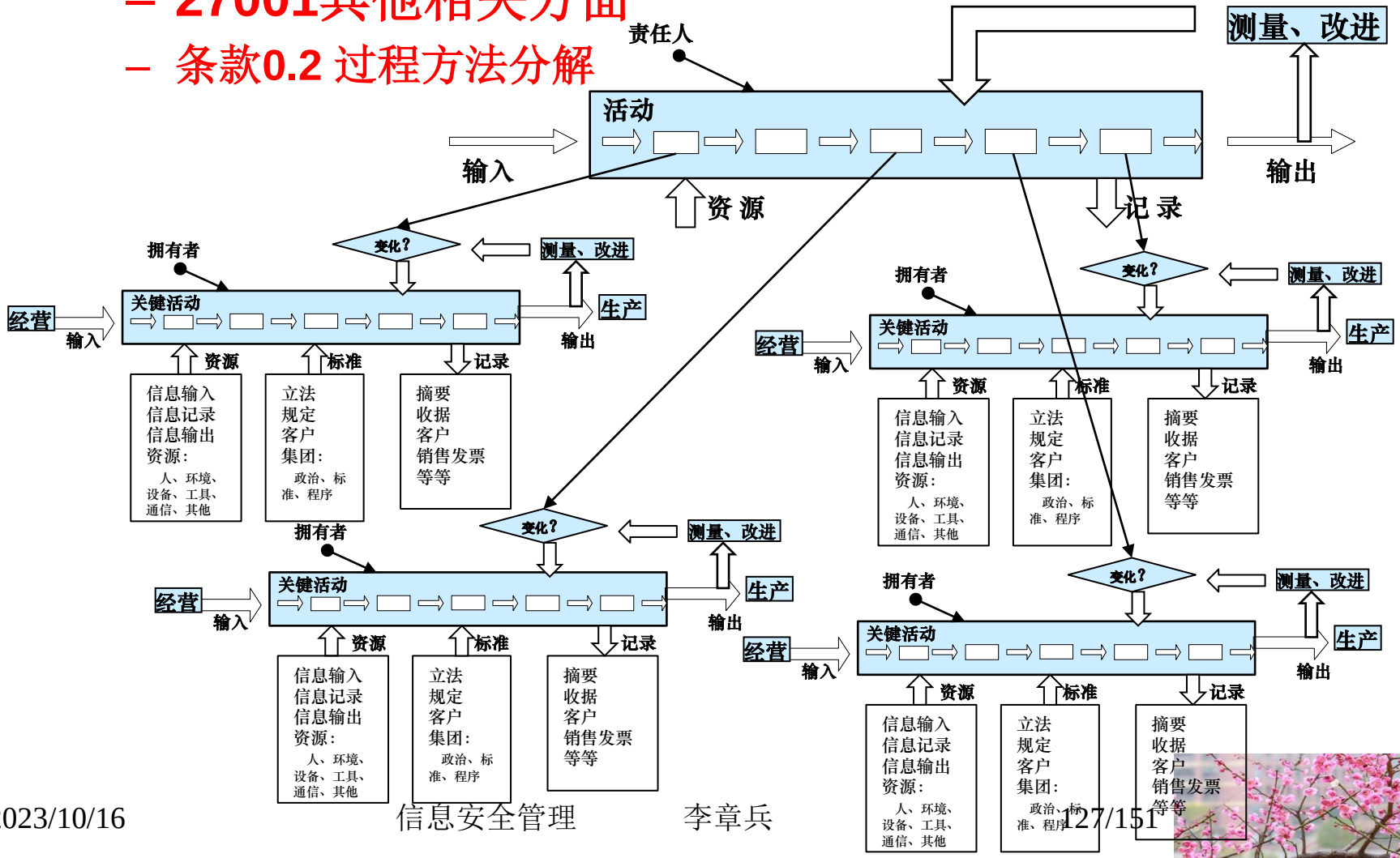
2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 条款0.2 过程方法



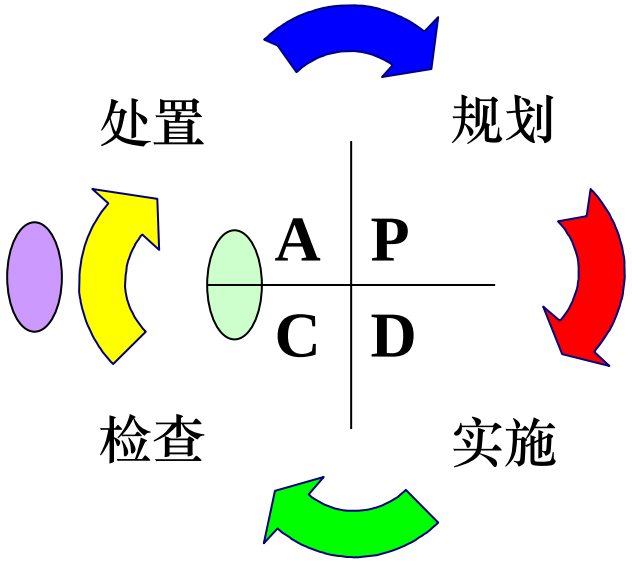
2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 条款0.2 过程方法分解



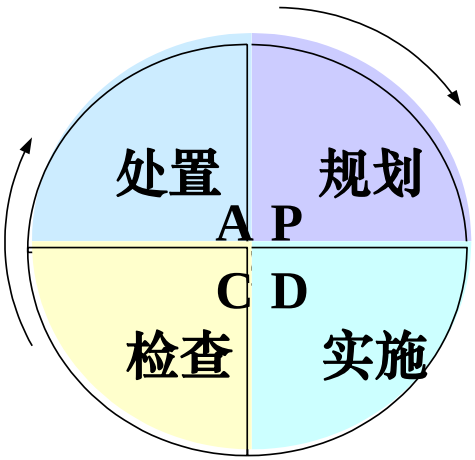
2.6 ISO/IEC 27001:2005标准

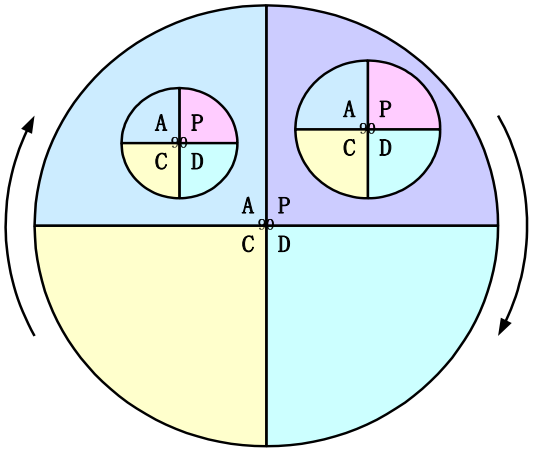
- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 条款0.2 PDCA
    - 持续改进的优秀方法
      - 又称“戴明环”,PDCA循环是能使任何一项活动有效进行的工作程序:
      - P：规划
      - D：实施
      - C：检查
      - A：处置

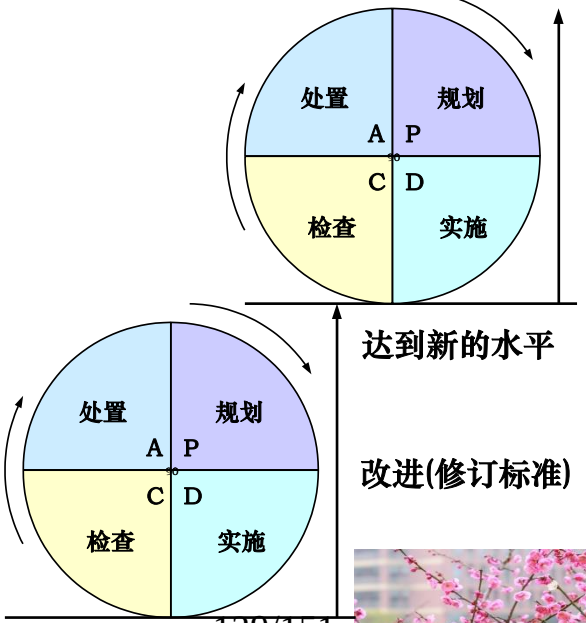


2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 条款0.2 PDCA
    - PDCA特点
      - 1.按顺序进行，它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。
      - 2.组织中的每个部分，甚至个人，均可以PDCA循环，大环套小环，一层一层地解决问题。
      - 3.每通过一次PDCA 循环，都要进行总结，提出新目标，再进行第二次PDCA 循环。







2.6 ISO/IEC 27001:2005标准

- **5. ISO/IEC 27001:2005 内容**
  - **27001其他相关方面**
  - **条款0.2 PDCA**
    - 持续改进的优秀方法
      - 采用**PDCA**模型还反映了治理信息系统和网络安全的**OECD**指南（**2002**版）中所设置的原则
        www.oecd.org
      - **OECD**信息系统和网络安全指南
        - » **OECD Guidelines for the Security of Information System and Network**

① **认识**
② **责任**
③ **反应**
④ **道德规范**
⑤ **民主**
⑥ **风险评估**
⑦ **安全设计与实施**
⑧ **安全管理**
⑨ **再评估**

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 条款0.3 与其它管理体系的兼容性
    - 多种体系如何建设
      - 本标准与GB/T 19001-2000及GB/T 24001-1996相结合，以支持相关管理标准一致、整合的实施和运作。因此，一个设计恰当的管理体系可以满足所有这些标准的要求。表C.1说明了本标准、GB/T 19001-2000（ISO 9001:2000）和GB/T 24001-1996（ISO 14001:2004）的各条款之间的关系。
      - 本标准的设计能够使一个组织将其ISMS与其它相关的管理体系要求结合或整合起来
      - 注：如果一个组织已经有一个运转着的业务过程管理体系（例如，与ISO 9001或者ISO 14001相关的），那么在大多数情况下，在这个现有的管理体系内满足本标准的要求是更为可取的

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 条款3 术语和定义

3.1 资产asset

3.2 可用性availability

3.3 保密性confidentiality

3.4 信息安全information security

3.5 信息安全事件 information security event

3.6 信息安全事故 information security incident

3.7 信息安全管理体系（ISMS） information security management system（ISMS）

3.8 完整性integrity

3.9 残余风险 residual risk

3.10 风险接受risk acceptance

3.11 风险分析risk analysis

3.12 风险评估risk assessment

3.13 风险评价risk evaluation

3.14 风险管理risk management

3.15 风险处理risk treatment

3.16 适用性声明statement of applicability

2.6 ISO/IEC 27001:2005标准

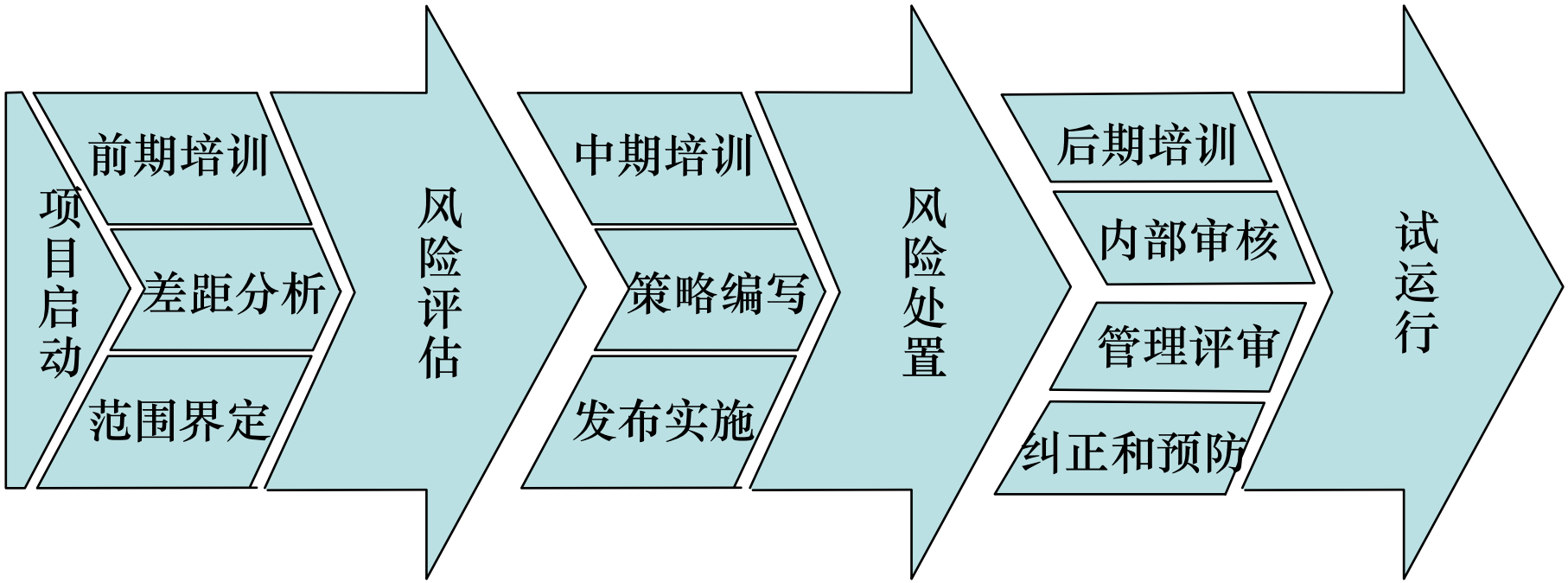
- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 附录A
    - 规范性附录。
    - 直接引用并与ISO/IEC 17799:2005第5到15章一致。
    - 表A.1中的清单并不完备，一个组织可能考虑另外必要的控制目标和控制措施。
    - 在这些表中选择控制目标和控制措施是条款4.2.1规定的ISMS过程的一部分。
    - ISO/IEC 17799:2005第5至15章提供了最佳实践的实施建议和指南
    - 表A.1 控制目标和控制措施

2.6 ISO/IEC 27001:2005标准

- 5. ISO/IEC 27001:2005 内容
  - 27001其他相关方面
  - 附录B
    - 资料性附录。
    - OECD信息系统和网络安全指南中给出的原则适用于治理信息系统和网络安全的所有方针和操作层。
    - 本标准提供信息安全管理体系框架，通过使用PDCA模型以及4、5、6和8所述的过程，来实现的某些OECD原则。
    - 表B.1 OECD 原则 和 PDCA 模型。
  - 附录C
    - 资料性附录。
    - 表C.1 ISO 9001:2000、ISO 14001:2004和本标准之间的对应关系。

2.6 ISO/IEC 27001:2005标准

- 6. ISO 27001 ISMS建立练习



2.6 ISO/IEC 27001:2005标准

- 6. ISO 27001 ISMS建立练习
  - 构建ISMS的第一阶段：风险评估（Plan）
    - 风险评估阶段主要包括以下5个关键步骤:

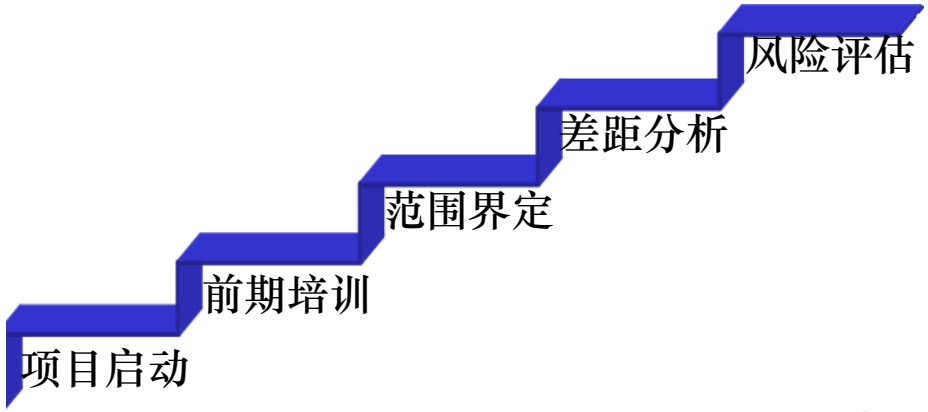
– 项目启动
前期沟通，实施计划，资源准备，启动会议。

– 前期培训
ISO27001标准，风险评估方法。

– 范围界定
书面确定ISMS的范围和界限。

– 差距分析
组织现有的信息安全管理体系与ISO27001的差距。

– 风险评估
资产评估、威胁评估、脆弱性评估、业务影响评估和现实可能性评估，风险处置计划，适用性声明，残余风险批准等。



风险评估是此阶段中最重要的环节。通常耗时1个月以上。

2.6 ISO/IEC 27001:2005标准

- 6. ISO 27001 ISMS建立练习
  - 练习一 ISMS范围确定 (20 min)
    - 假设你是一家公司的安全官，现在考虑把ISO27001引入到公司，需要你确定公司的ISMS范围：
      - - 公司业务
      - 公司方针
      - - 组织
      - - 位置
      - - 资产

2.6 ISO/IEC 27001:2005标准

- 6. ISO 27001 ISMS建立练习
  - 练习二 资产价值、威胁、脆弱性和影响 (30min)
    - **Mr.Risk** 分析当前公司的资产状况，包括他们的价值，主要面临的威胁，可能性以及他们的后果。最终计算得出风险说明和风险处置。(你可以用高中低来描述不同等级)

资产描述	资产价值	威胁可能性	脆弱性 严重程度	风险说明	风险处置
信息资产					
软件资产					
物理资产					
服务资产					

2.6 ISO/IEC 27001:2005标准

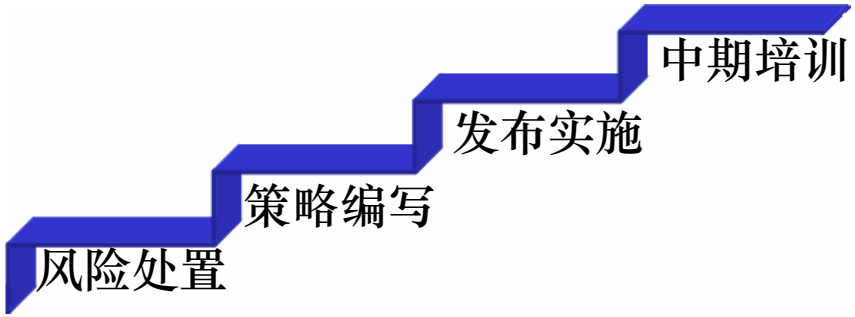
- 6. ISO 27001 ISMS建立练习
  - 构建ISMS的第二阶段：风险处置（Do）
    - 风险处置阶段主要包括以下4个关键步骤:

– 风险处置
风险处置计划的落实：技术方案的落实，管理方案的落实。

– 策略编写
安全规章制度、流程、程序和记录模版等的文件化的ISMS的落实。

– 发布实施
获得管理层的授权，实施和运作ISMS。

– 中期培训
ISMS的全员推广培训



风险处置和策略编写是此阶段中最重要的环节。通常耗时1个月以上。

2.6 ISO/IEC 27001:2005标准

- 6. ISO 27001 ISMS建立练习
  - 练习三、编写策略文件(30 min)
    - 请参考下列模板准备您公司的策略体系

级别名称		文 件名称
级别1	Manual（方针手册）	
	Risk Management Documents（风险管理文件）	
级别2	Standard of Procedure（SOP，程序标准，支持ISMS的程序和控制措施。）	
级别3	Instruction（作业指导书）	
级别4	Record（记录）	

2.6 ISO/IEC 27001:2005标准

- **6. ISO 27001 ISMS建立练习**
  - **构建ISMS的第三阶段：试运行（Check and Action）**
    - 试运行阶段主要包括以下**5**个关键步骤:

– **试运行**
流程和程序等的运行，生成相应的记录。

– **内部审核**
内部审核，分析与ISO27001的差距等。

– **管理评审**
管理层评审ISMS的运行情况等。

– **纠正和预防**
纠正与ISO27001的不符合项，预防潜在的与ISO27001的不符合项。

– **后期培训**
内审员等专业技能培训。

试运行是此阶段中最重要的环节。
通常耗时3个月以上。

2.6 ISO/IEC 27001:2005标准

- 6. ISO 27001 ISMS建立练习
  - 练习四、审核计划 (20min)
    - 请参考下列模板准备你的审核计划:

名称		
公司部门		
日期		
审核范围		
时间	区域	参加人员
审核员		

2.6 ISO/IEC 27001:2005标准

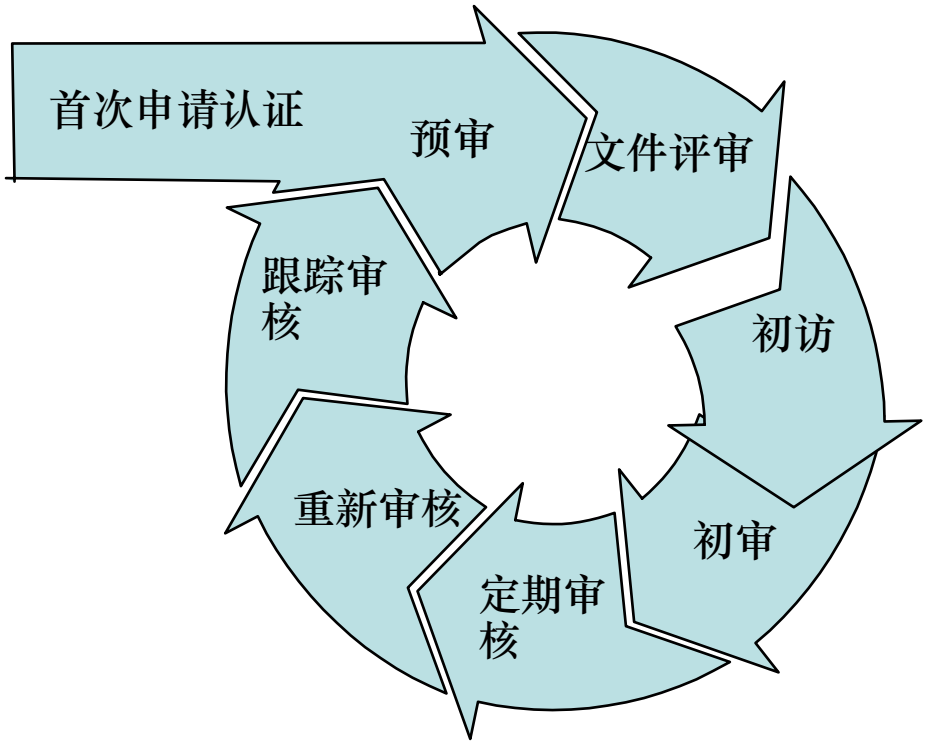
- 6. ISO 27001 ISMS建立练习
  - 练习五、 内部审核 (15 min)
    - 请参考下列模板准备你的审核计划:

内审发现报告			日期
公司部门			
审核领域			
参考条款			
结果:	不符合	观察项	值得努力
发现: 纠正措施:			
审核员			

2.6 ISO/IEC 27001:2005标准

- **7.申请ISO27001认证的基本流程**
  - 作为审核机构，如DNV，完成一次审核主要包括：

- 预审
  非强制要求，可选。
- 文件评审
  通常与初访和初审同时进行，检查组织的风险评估报告和BCP等。
- 初访
  通常阐明审核范围，确认审核标准和回答被审核组织的问题等。
- 初审
  完整审核。
- 定期审核
  每年进行，定期确保体系仍满足要求。
- 重新审核
  每3年进行一次，更新即将过期的证书。
- 跟踪审核
  检查上一次审核时的审核发现的纠正情况，如果上一次是初审，向UKAS提交审核报告，申请颁发证书。



2.6 ISO/IEC 27001:2005标准

- **8.ISMS实例：**
  - 范围

1 Scope of ISMS in XXXX China

Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusion from the scope. (ISO/IEC 27001:2005, Chapter 4.2.1)

1.1 Characteristics of Business

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1.2 Organization

Organizations in scope	Excluded Organizations / Out of Scope
XXXX China internal departments ▪ XX, XX, XX and etc.	

1.3 Location

Locations in scope	Excluded Locations / Out of Scope
Beijing Address: 7, Wangjing Zhonghuan Nanlu, Chaoyang District, P.O.Box 8543, Beijing 100102, P.R.China Location Code: PEK **Shanghai** Address: 7-11/F China Marine Tower, 1 Pudong Avenue, Pudong New Area, Shanghai 200120, P. R. China Location Code: SHA	

1.4 Technology

Technologies in scope	Excluded Technologies / Out of Scope
▪ Data & Voice Networks	

2.6 ISO/IEC 27001:2005标准

- **8.ISMS实例：**
  - 差距分析

C	D	E	F	G	H	
Main section	Sub section	Clause	Requirement Checklist for ISO / IEC 27001	Reference	Score	
5 Management responsibility	5.1 Management commitment	*5.1 Management commitment*	**5.1 Management commitment**			
5 Management responsibility	5.1 Management commitment	*5.1 Management commitment*	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:			
5 Management responsibility	5.1 Management commitment	*5.1 Management commitment*	a) establishing an ISMS policy;	Management Approval	3	We need to be familiar with the CERT website.
5 Management responsibility	5.1 Management commitment	*5.1 Management commitment*	b) ensuring that ISMS objectives and plans are established;	1. Policy should include obj and plans 2. Management Review on obj and plans	1	ISMS Specification
ement bility	gement ent	agement tment	c) establishing roles and responsibilities for information		1	

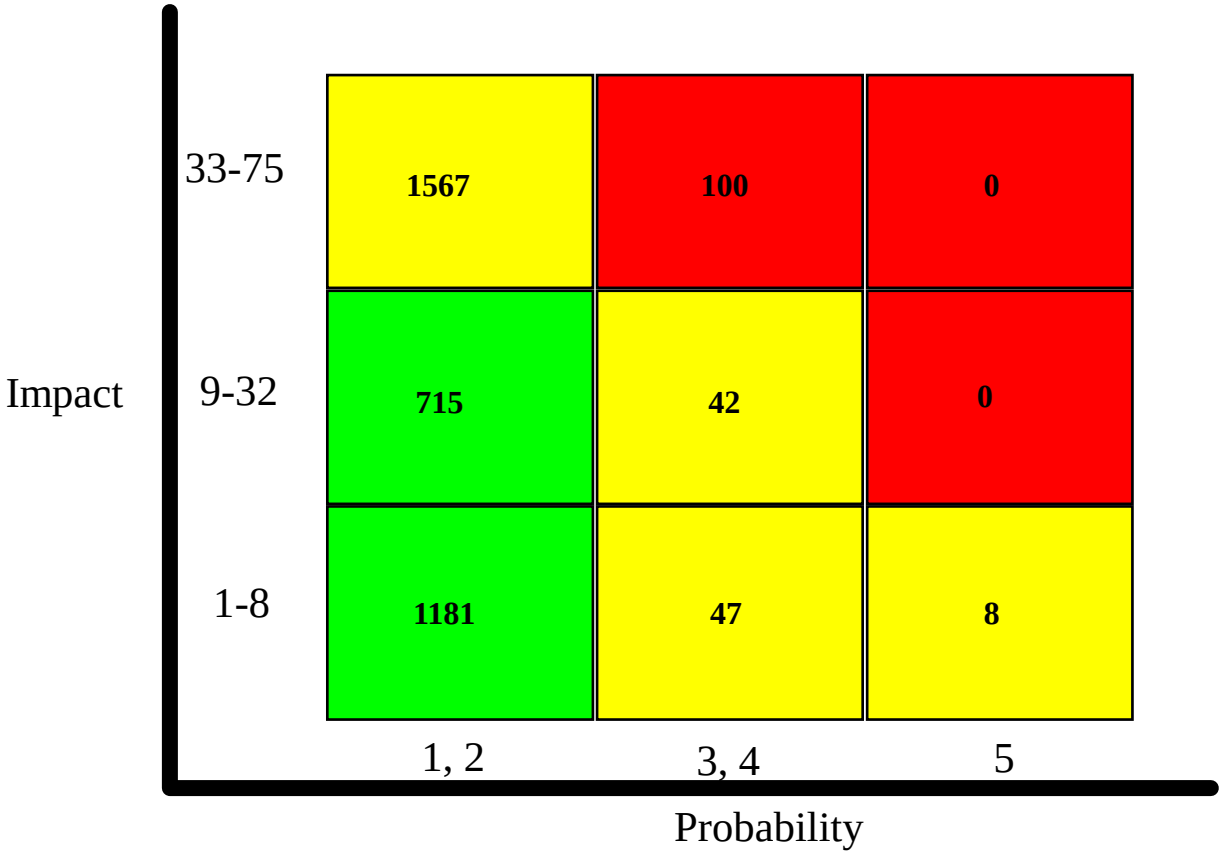
2.6 ISO/IEC 27001:2005标准

- **8.ISMS实例：**
  - 风险评估报告

	A	B	C	D	E	F	G	H	I
1	Assets Category	Assests Type	Assets Group	CIA Cluste	C	I	A	CIA Impact Value	Thr
1008	People	Vendor Contact Person	Software Maintenance Service	B				32	information
1009	People	Vendor Contact Person	Software Maintenance Service	B				32	information
1010	People	Vendor Contact Person	Software Maintenance Service	B				32	information
1011	People	Vendor Contact Person	Software Maintenance Service	B				32	information
1012	People	Vendor Contact Person	Software Maintenance Service	B				32	breaches o
1013	people	Vendor Contact Person	Software Maintenance Service	B				32	unauthoriz
1014	People	Vendor Contact Person	IT Consultant	B				32	ineffectiv
1015	People	Vendor Contact Person	IT Consultant	B				32	ineffectiv
1016	People	Vendor Contact Person	IT Consultant	B				32	Derelictio
1017	People	Vendor Contact Person	IT Consultant	B				32	Derelictio
1018	people	Vendor Contact Person	IT Consultant	B				32	use of sof
1019	people	Vendor Contact Person	IT Consultant	B				32	system fai
1020	people	Vendor Contact Person	IT Consultant	B				32	operationa
1021	People	Vendor Contact Person	IT Consultant	B				32	information
1022	People	Vendor Contact Person	IT Consultant	B				32	information
1023	People	Vendor Contact Person	IT Consultant	B				32	information
1024	People	Vendor Contact Person	IT Consultant	B				32	information
1025	People	Vendor Contact Person	IT Consultant	B				32	breaches o
1026	people	Vendor Contact Person	IT Consultant	B				32	unauthoriz
1027	Hardware	Computer room Cabling	Data Center Cabling	A				75	misuse of
1028	Hardware	Computer room Cabling	Data Center Cabling	A				75	misuse of
1029	Hardware	Computer room Cabling	Data Center Cabling	A				75	misuse of
1030	Hardware	Computer room Cabling	Data Center Cabling	A				75	misuse of
1031	Hardware	Computer room Cabling	Data Center Cabling	A				75	air condit
1032	Hardware	Computer room Cabling	Data Center Cabling	A				75	interceptio

2.6 ISO/IEC 27001:2005标准

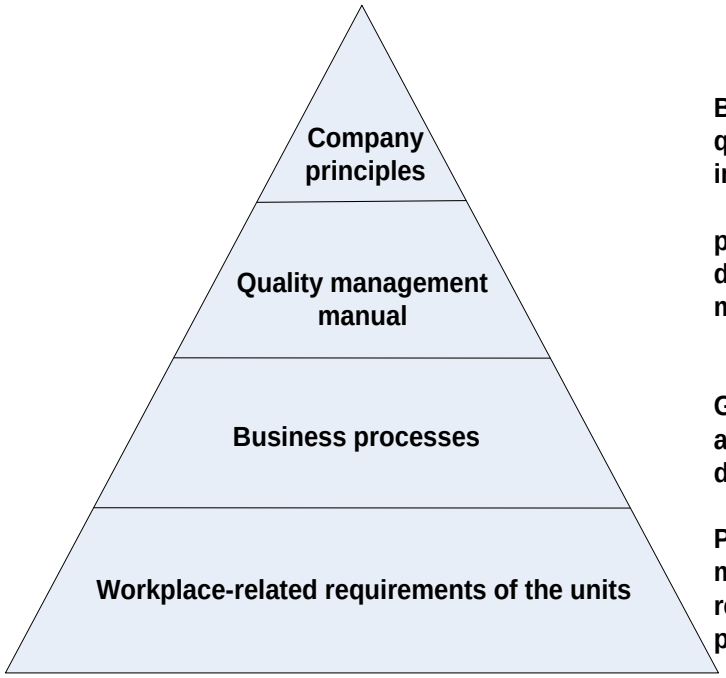
- **8.ISMS实例：**
  - 风险处置计划



We have 100 ***risks,*** among 27 asset groups — **Requires take action**

2.6 ISO/IEC 27001:2005标准

- **8.ISMS实例：**
  - 策略体系



Business model, quality policy, information security → **Information security policy and objective ISMS scope and SOA**

policy Binding description of the management system → **Quality management manual**

Generic guidelines and process descriptions → **Process descriptions, documented procedure, guidelines, circular and RA method**

Process scenarios, manuals, requirements of IT processes → **RA report, RT plan, KPI, Process scenarios, manuals** (Handbook and Checklist) **and records (**Log file, minutes of meeting, application form, checklist form and etc**)**

小结

- 信息安全管理体系的概念,建立步骤,特点;
- PDCA模型;
- BS7799信息安全管理体系;
- 基于SSE-CMM的信息安全管理。
- 不同的组织在建立与完善信息安全管理体系时，可根据自己的特点和具体情况采取不同的步骤和方法。但总体来说，建立信息安全管理体系一般要经过五个基本步骤 。
- 信息安全标准关系到国家的安全及经济利益，在不同国家、地区之间，标准往往成为保护利益和解决冲突的一种重要手段。
- ISO/IEC 27001:2005涵盖了信息安全标准的主要内容，理解和掌握该标准的适用范围、主要结构和内容，对于信息安全管理实践有着重要意义。

作业

- 1.什么是信息安全管理体系ISMS？建立ISMS有什么作用？
- 2.叙述BS7799的主要内容？可以采用哪些模式引入BS7799？
- 3.叙述SSE-CMM的主要思想 。
- 4.PDCA模型中包含哪四个主要活动？
- 5.在建立和实施信息安全管理体系的过程中，如何采用PDCA模型及其思想？
- 6.建立信息安全管理体系一般要经过哪些基本步骤？
- 7.ISO 27001关注的11个安全领域是什么？
- 8.试编写建立ISO27001 ISMS的第一、二、五阶段文件。
- 9.ISO2700系列标准与BS7799、SSE-CMM、CC、TR13335、SP800系列有何区别和联系？