安全管理体系介绍

Agenda

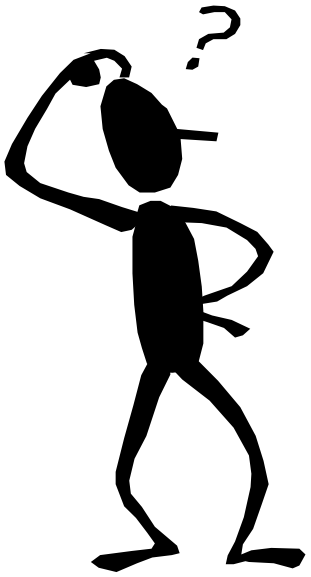
一、信息安全基础知识

二、信息安全管理标准

三、认证相关介绍

信息安全概念

- 什么是信息？
  - 信息是一种资产象其它重要的业务资产一样，对组织具有价值因此需要适当的保护
- 什么是安全？
  - 没有统一的定义
  - 基本含义
    - 客观上不受威胁
    - 主观上不存在恐惧
- 什么是信息安全？
  - ISO的定义为：为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和显露。



信息安全特征

- 信息安全具有以下特征：
  - 保密性：确保只有经过授权的人才能访问信息
  - 完整性：保护信息和信息的处理方法准确而完整；
  - 可用性：确保经过授权的用户在需要时可以访问信息并使用相关信息资产。

信息安全的相对性

- 安全没有100%
  - 完美的健康状态永远也不能达到；
- 安全工作的目标：将风险降到最低
- 安全应该与保护的事物的价值相称；
- 安全需要权衡
  - 可用性与安全性
  - 易用性与安全性
  - 经济性与安全性

信息安全现状

- 重视技术，轻视管理
- 重视产品功能，轻视人为因素
- 重视对外安全，轻视内部安全
- 静态不变的观念
- 缺乏整体性信息安全体系的考虑

信息安全需求

- 强化责任意识，坚决做到责任到人，设备到人，工作到位
- 进一步完善安全规范体系，强化安全操作执行力
- 按照总部统一要求，大力推进安全防护技术手段建设

有关标准

2004 ●2004年9月5号，BS7799-2:2002正式发布，提交ISO，可望近期成为国际标准。

2002 ●BSI对BS7799-2:1999进行了修订，正式引入PDCA过程模型。9月**BS7799-2:2002**公布发行。

2000 ●BS7799-1:1999通过国际化标准组织ISO认可，12月正式成为国际标准ISO/IEC 17799-1:2000《信息技术－信息学安全管理实施细则》

1999 ●BS7799-1:1999与BS7799-2**:1999**经过修订后重新发布

1998 ●英国出版 BS7799-2:1998《信息安全管理体系规范》

1995 ●英国出版 BS7799-1:1995《信息安全管理实施细则》

1993 ●率先由英国贸易工业部进行专案。

有关规定

- 《关于加强信息安全保障工作的意见》（中办国办[2003]27号文件）
  - 我国第一个全面关于信息安全保障工作的文件，是我国今后一段时期内信息安全保障工作的纲领性文件。
  - 文件对中央各部委、各行业和各地区的信息安全保障工作做出原则性、战略性的规定。
  - 总体要求：坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全 。

有关标准及法规

- 《信息安全风险管理指南》
- 《电信网和互联网安全风险评估实施指南》(YDC051-2007)
- 《电信网和互联网安全等级保护实施指南》(YDC050-2007)
- SOX

Agenda

一、信息安全基础知识

二、信息安全管理标准

三、认证相关介绍

信息安全管理

- 信息安全管理的重要意义
  - 在当今全球一体化的商业环境中，信息的重要性被广泛接受，信息系统在商业和政府组织中得到了真正的广泛的应用。许多组织对其信息系统不断增长的依赖性，加上在信息系统上运作业务的风险、收益和机会，使得信息安全管理成为企业管理越来越关键的一部分。
- ISO27001/ISO17799

ISO27001/ISO17799

ISMS Standard Set _ Future

ISO/IEC Standard	Description
27000	Vocabulary and definitions
27001	Requirement (BS7799-2)
27002	Code of Practice (ISO17799)
27003	Implementation Guidance
27004	Metrics and Measurement
27005	Risk Management (BS 7799-3)

ISO27001/ISO17799体现原则

- 制定信息安全方针为信息安全管理提供导向和支持
- 控制目标和控制方式的选择建立在风险评估基础之上
- 预防控制为主的思想原则
- 全员参与原则
- 动态管理原则
- 遵循管理的一般循环模式—PDCA持续改进模式
- 商务持续性原则

ISO27001

- Chapter 0 : 简介
- Chapter 1 : 范围
- Chapter 2 : 引用标准
- Chapter 3 : 术语和定义
- Chapter 4 : 信息安全管理体系
- Chapter 5 : 管理责任
- Chapter 6 : ISMS内部审核
- Chapter 7 : ISMS管理评审
- Chapter 8: ISMS改进
- 附件A（强制性）控制目标和控制措施
- 附录B OECD 准则和本国际标准
- 附录C 本标准与ISO9001:200、ISO14001：2004 标准的对应关系

ISO27001

- Chapter 0：简介
  - 0.1总则
    - 本标准为业务经理及其职员提供了建立和管理一个有效的信息安全管理体系(ISMS)的模型。
    - 采用ISMS是企业(组织)的一项战略性决策。
    - 企业的ISMS的设计和实施受各种业务需求、具体的目标、安全要求、所采用的过程以及组织的规模和结构的影响。
    - 期望随着时间而变化(改进)。
    - 本标准能够用户内部/外部(认证机构)评价企业满足顾客、法律法规和企业自身要求的能力。
  - 0.2过程方法
    - 过程IPO：通过利用资源和管理将输入转化为输出的一项活动。
    - 过程方法：组织内过程系统的应用,连同这些过程的识别和相互作用及其管理。
    - PDCA模型:
  - 0.3与其他管理体系的兼容性
    - 本标准与ISO9001:2000和ISO14001:2004协调一致，以支持与相关管理标准的结合和整合的实施和运行。表C.1注了本标准与ISO9001:2000和ISO14001:2004的章节间的对应关系

ISO27001

- Chapter 0：简介（续）
  - 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

规划（建立ISMS）	建立与管理风险和改进信息安全有关的ISMS方针、目标、过程和程序，以提供与组织总方针和总目标相一致的结果。
实施（实施和运行ISMS）	实施和运行ISMS方针、控制措施、过程和程序。
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。
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。

ISO27001

- Chapter 1：范围
  - 总则
    - **ISMS**是设计用于有足够的和适当的安全控制以确保信息资产，并给顾客及其它相关以信心。这将转化为维护和改善组织的竞争力、现金周转、收益率、法律符合性和商业形象。
  - 应用
    - 本标准规定的要求是通用的，意在适用于各种类型、不同规模、不同性质的企业。
    - 当本标准的任何要求由于组织及其业务的特点而不适用时，可以考虑进行删减。
    - 如果进行删减，除非删减不影响组织提供(满足风险评估和使用法律法规要求决定的)信息安全的能力、责任，否则不能声称符合本标准。
    - 对（满足风险接受准则的）控制方式的任何删减，必须评估其合理性，同时必须提供相关风险已经使相关责任人接受的证据.
    - 对4、5、6、7、8章节的任何要求的删减都是不可接受的。

ISO27001

- Chapter 2：引用标准
  - ISO/IEC 17799：2005 信息技术－安全技术－信息安全管理实施指南

ISO27001

- Chapter 3：术语和定义
  - 3.1 资产：任何对组织有价值的事物
  - 3.2可用性:需要时，授权实体可以访问和使用的特性。
  - 3.3 机密性:信息不可用或不被泄漏给未授权的个人、实体和过程的特性。
  - 3.4 信息安全:保护信息的保密性、完整性、可用性及其他属性，如：真实性、可核查性、可靠性、防抵赖性。
  - 3.5信息安全事件（**Event**）：信息安全事件是指识别出的发生的系统、服务或网络事件表明可能违反信息安全策略或防护措施失效；或以前未知的与安全相关的情况。
  - 3.6信息安全事故（**Incident**）：信息安全事故是指一个或系列非期望的或非预期的信息安全事件，这些信息安全事件可能对业务运营造成严重影响或威胁信息安全。
  - **3.7**信息安全管理体系（**ISMS**）：整体管理体系的一部分，基于业务风险方法以建立、实施、运行、监视、评审、保持和改进信息安全。

ISO27001

- Chapter 3：术语和定义（续）
  - **3.8** 完整性:保护资产的正确和完整的特性
  - 3.9残余风险:实施风险处置后仍旧残留的风险。
  - 3.10风险接受:接受风险的决策。
  - **3.11** 风险分析:系统地使用信息以识别来源和估计风险
  - **3.12** 风险评估:风险分析和风险评价的全过程
  - **3.13** 风险评价:将估计的风险与既定的风险准则进行比较以确定重要风险的过程。
  - **3.14** 风险管理:指导和控制一个组织的风险的协调的活动
  - **3.15** 风险处置:选择和实施措施以改变风险的过程。
  - **3.16** 适用性声明:与组织ISMS 相关并适用于组织ISMS 的控制目标和控制措施的文件化的陈述。

ISO27001

- Chapter 4：信息安全管理体系（ISMS）
  - 4.1总要求
    - 组织应根据整体业务活动和风险，建立、实施、运行、监视、评审、保持并改进文件化的信息安全管理体系。
  - 4.2建立并管理ISMS
    - 建立ISMS
    - 实施和运行ISMS
    - 监视和评审ISMS
    - 保持和改进ISMS
  - 文件要求
    - 总则
    - 文件控制
    - 记录控制

ISO27001

- Chapter 5：管理责任
  - **5.1** 管理层承诺
    - 管理者通过以下活动，对建立、实施、运作、监督、审查、维护和改善**ISMS**作出的承诺提供证据。
    - 制定信息安全策略；
    - 确保信息安全目标和计划的制定；
    - 规定信息安全的作用和责任；
    - 向组织传达满足信息安全目标和符合信息安全策略的重要性，法律和持续性改善需要方面的责任。
    - 提供充分的资源以制定、实施、运作和维护**ISMS. (**第**5.2.1**章**)**
    - 确定风险的可接收水平；
    - 进行**ISMS**管理审查；**(**见第**6**章**)**
  - **5.2**资源管理
    - **5.2.1** 资源提供
    - **5.2.2** 培训、意识和能力

ISO27001

- Chapter 5：管理责任（续）
  - **5.1 管理层承诺**
  - **5.2资源管理**
    - **5.2.1 资源提供，**
      - **企业应确定并提供需要的资源:**
        - 建立、实施、运作和维护ISMS;
        - 确保信息安全程序支持业务要求；
        - 识别和确定法律和法规要求、合约中规定的安全义务；
        - 通过对所有实施控制的正确应用保持足够的安全；
        - 在必要时进行执行审核，并对审查结果作出适当的反应；
        - 必要时，改善ISMS的有效性。
    - **5.2.2 培训、意识和能力**
      - **企业应确保所有ISMS中所有责任相关人员有能力完成要求的任务，经由:**
        - 确定从事ISMS人员所必要的能力;
        - 提供能力培训，必要时，委派有能力的人以满足这些要求；
        - 评价所“提供的培训”和“采取的措施”的有效性；
        - 维护教育、培训、技能、经历和资格的记录；

ISO27001

- Chapter 6 : ISMS内部审核
  - 应按策划的时间间隔进行**ISMS**内部审核，以确定组织**ISMS**的控制目标、控制措施、过程和程序是否：
    - **a)** 符合本标准及相关法律法规的要求；
    - **b)** 符合已识别的信息安全要求；
    - **c)** 得到有效地实施和保持；
    - **d)** 按期望运行。
  - 应策划审核方案，考虑受审核过程和区域的状况及重要性，以及上次审核的结果。应规定审核准则、范围、频次和方法。
  - 审核员的选择和审核的实施应保证审核过程的客观和公正。不能审核自己的工作。
  - 形成文件的程序，以规定策划和实施审核、报告结果和保持记录（见**4.3.3**）的职责和要求。

ISO27001

- Chapter 7 : ISMS管理评审
  - 7.1总则
    - 管理者应按策划的时间间隔（至少一年一次）评审组织的**ISMS**，以确保其持续的适宜性、充分性和有效性。评审应包括评价**ISMS**改进的机会和变更的需要，包括安全方针和安全目标。评审结果应清楚地写入文件，并保持记录
  - 7.2评审输入
    - 管理评审的输入应包括：
      - **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**业绩和有效性的技术、产品或程序；
      - **d)** 纠正和预防措施的实施情况；
      - **e)** 上次风险评估未充分指出的脆弱性或威胁；
      - **f)** 有效性测量的结果；
      - **g)** 上次管理评审所采取措施的跟踪验证；
      - **h)** 任何可能影响**ISMS**的变更；
      - **i)** 改进的建议。
  - 7.3评审输出

ISO27001

- Chapter 7 : ISMS管理评审（续）
  - 7.1总则
  - 7.2评审输入
  - 7.3评审输出
    - 管理评审的输出应包括与以下方面有关的任何决定和措施：
      - **a) ISMS**有效性的改进；
      - **b)** 更新风险评估和风险处置计划；
      - **b)** 必要时，修订影响信息安全的程序和控制措施，以反映可能影响**ISMS**的内外事件，包括以下方面的变化：
        - **1)** 业务要求；
        - **2)** 安全要求；
        - **3)** 影响现有业务要求的业务过程；
        - **4)** 法律法规要求；
        - **5)** 合同责任；
        - **6)** 风险等级和/或风险接受准则。
        - **c)** 资源需求；
        - **d)** 改进测量控制措施有效性的方式。

ISO27001

- Chapter 8: ISMS改进
  - 8.1持续改进
    - 企业应通过信息安全策略、安全目标、审查结果、监督的事件分析、矫正措施、预防措施以及管理审查，持续改善ISMS的有效性.
  - 8.2纠正措施
    - 企业应该采取措施，以消除与ISMS的实施、运作相关的不合格的原因，防止再次发生。
    - 应编制形成文件化的“纠正措施程序文件”，并规定以下方面的要求:
      - (1)识别ISMS实施/运作的不合格项；
      - (2)确定不合格项发生的原因；
      - (3)评价(确保不合格项不再发生)措施的需求；
      - (4)确定和实施所需的纠正措施；
      - (5)记录所采取纠正措施的结果；
      - (6)审查所采取的纠正措施；
  - 8.3预防措施

ISO27001

- Chapter 8: ISMS改进（续）
  - 8.1持续改进
  - 8.2纠正措施
  - 8.3预防措施
    - 企业应该确定措施，以消除潜在不合格的原因，防止其发生。
    - 预防措施应与潜在问题的影响程度相适应。并编制形成文件化的“预防措施程序文件”，以规定以下方面的要求:
      - (1)识别潜在的不合格项及其原因；
      - (2)确定和实施必须的预防措施；
      - (3)记录所采取预防措施的结果；
      - (4)审查所采取的预防措施；
      - (5)识别风险的变化情况，将注意力集中到变化重大的风险上。
    - 预防措施的优先事项必须基于风险评估的结果。
    - 注: 采取措施预防不合格通常比矫正措施划算。

ISO27001

附录A（强制性）控制目标和控制措施

<table>
<tr><td colspan="4">安全方针（1,2）</td></tr>
<tr><td colspan="4">安全组织 (2,11)</td></tr>
<tr><td colspan="4">资产管理 (2,5)</td></tr>
<tr><td>人力资源安全 (3,9)</td><td>物理与环境安全(2,13)</td><td>通信与运行管理(10,32)</td><td>信息系统的获取、开发与维护(6,16)</td></tr>
<tr><td colspan="2">访问控制(7,25)</td><td colspan="2">信息安全事件管理(2,5)</td></tr>
<tr><td colspan="4">业务持续性管理 (1,5)</td></tr>
<tr><td colspan="4">符合性 (3,10)</td></tr>
<tr><td colspan="4">附注：(m，n)— m：执行目标的数目 n：控制方法的数目
m:39 n:133</td></tr>
</table>

ISO27001

- 表A.1 中所列出的控制目标与控制措施直接从引用 **ISO/IEC17799：2005 第5 到15 章。**

附录A (强制性)控制目标和控制措施

- 安全方针（1,2）
  - 5.1信息安全方针 目标：为信息安全提供符合业务要求和相关法律法规的管理指导和支持
    - 5.1.1信息安全方针文档
      - 控制措施：信息安全方针文档应经过管理层的批准，并向所有员工和外部相关方公布和沟通
    - 5.1.2信息安全方针评审
      - 控制措施：应按策划的时间间隔或当发生重大变化时，对信息安全方针文档进行评审，以确保其持续的适宜性、充分性和有效性

附录A (强制性)控制目标和控制措施

- 安全组织(2,11)
  - 6.1内部组织 目标：在组织内部管理信息安全
    - 6.1.1信息安全管理委员会
    - 6.1.2信息安全协调
    - 6.1.3信息安全职责分配
    - 6.1.4信息处理设施授权过程
    - 6.1.5保密协议
    - 6.1.6与监管机构的联系
    - 6.1.7与特许利益团体的联系
    - 6.1.8信息安全的独立评审
  - 6.2外部组织 目标：保持组织的被外部组织访问、处理、沟通或管理的信息及信息处理设备的安全
    - 6.2.1识别与外部组织相关的风险
    - 6.2.2当与客户接触时强调安全
    - 6.2.3在第三方协议中强调安全

附录A (强制性)控制目标和控制措施

- 资产管理(2,5)
  - 7.1资产责任 目标：实现并保持组织资产的适当保护
    - 7.1.1资产列表
    - 7.1.2资产所有者关系
    - 7.1.3资产的可接受实用
  - 7.2资产分类 目标：确保信息可以得到适当程度的保护
    - 7.2.1分类指南
    - 7.2.2信息标识和处置

附录A (强制性)控制目标和控制措施

- 人力资源安全 (3,9)
  - 8.1 雇佣前 目标：确保员工、合同访和第三方用户了解他们的责任并适合于他们所考虑的角色，减少盗窃、滥用或设施误用的风险
    - 8.1.1角色和职责
    - 8.1.2选拔
    - 8.1.3雇佣条款和条件
  - 8.2 雇佣中目标：确保所有的员工、合同方和第三方用户了解信息安全威胁和相关事宜、他们的责任和义务，并在他们的日常工作中支持组织的信息安全方针，减少人为错误的风险
    - 8.2.1管理职责
    - 8.2.2信息安全意识、教育和培训
    - 8.2.3惩戒过程
  - 8.3 雇佣终结或变更 目标：：确保员工、合同方和第三方用户离开组织或雇佣变更时以一种有序的方式进行
    - 8.3.1终结责任
    - 8.3.2归还资产
    - 8.3.3移出访问权限

附录A (强制性)控制目标和控制措施

- 物理与环境安全(2,13)
  - 9.1 安全区域 目标：防止对组织办公场所和信息的非授权物理访问、破坏和干扰
    - 9.1.1物理安全边界
    - 9.1.2物理进入控制
    - 9.1.3办公室、房间和设施的安全
    - 9.1.4防范外部和环境的威胁
    - 9.1.5在安全局域工作
    - 9.1.6公共访问和装卸区域
  - 9.2 设备安全目标：预防资产的丢失、损坏或被盗，以及对组织业务活动的干扰
    - 9.2.1设备选址和保护
    - 9.2.2支持设施
    - 9.2.3电缆安全
    - 9.2.4设备维护
    - 9.2.5场外设备安全
    - 9.2.6设备的安全销毁或重用
    - 9.2.7财产转移

附录A (强制性)控制目标和控制措施

- 通信与运行管理(10,32)
  - 10.1 操作程序及职责目标：确保信息处理设施的正确和安全操作
  - 10.2 第三方服务交付管理 目标：实施并保持信息安全的适当水平，确保第三方交付的服务符合协议要求
  - 10.3 系统规划与验收 目标：最小化系统失效的风险
  - 10.4 防范恶意代码和移动代码 目标：保护软件和信息的完整性
  - 10.5 备份 目标：保持信息和信息处理设施的完整性和可用性
  - 10.6 网络安全管理 目标：确保网络中的信息和支持性基础设施得到保护
  - 10.7 媒体处置 目标：防止对资产的未授权泄漏、修改、移动或损坏，及对业务活动的干扰
  - 10.8 信息交换 目标：应保持组织内部或组织与外部组织之间交换信息和软件的安全
  - 10.9 电子商务服务 目标：确保电子商务的安全及他们的安全使用
  - 10.10 监督 目标：检测未经授权的信息处理活动

附录A (强制性)控制目标和控制措施

- 访问控制(7,25)
  - 11.1 访问控制的业务要求 目标：控制信息访问
  - 11.2 用户访问管理 目标：确保授权用户的访问，并预防信息系统的非授权访问
  - 11.3 用户责任 目标：预防未授权用户的访问，信息和信息处理设施的破坏或被盗
  - 11.4 网络访问控制 目标：防止对网络服务未经授权的访问
  - 11.5 操作系统访问控制 目标：防止对操作系统的未授权访问
  - 11.6 应用系统和信息访问 目标：防止对应用系统中信息的未授权访问
  - 11.7 移动计算和远程工作 目标：确保在使用移动计算和远程工作设施时信息的安全

附录A (强制性)控制目标和控制措施

- 信息系统的获取、开发和维护(6,16)
  - 12.1 信息系统安全要求目标：确保安全成为信息系统的内置部分
  - 12.2 应用系统的正确处理 目标：防止应用系统信息的错误、丢失、未授权的修改或误用
  - 12.3 加密控制 目标：通过加密手段来保护细腻的保密性、真实性或完整性
  - 12.4 系统文档安全 目标：确保系统文档的安全
  - A.12.5 开发和支持过程的安全 目标：保持应用系统软件和信息的安全
  - 12.6 技术漏洞管理 目标：减少由利用公开的技术漏洞带来的风险

附录A (强制性)控制目标和控制措施

- **信息安全事件管理(2,5)**
  - 13.1 报告信息安全事件和弱点 目标：确保与信息系统有关的安全事件和弱点的沟通能够及时采取纠正措施
    - 13.1.1报告信息安全事件
    - 13.1.2报告信息安全弱点
  - 13.2 信息安全事故的管理和改进 目标：确保使用持续有效的方法管理信息安全事故
    - 13.2.1职责和程序
    - 13.2.2从信息安全事件中学习
    - 13.2.3收集证据

附录A (强制性)控制目标和控制措施

- 业务连续性管理(1,5)
  - 14.1 业务连续性管理的信息安全方面 目标：防止业务活动的中断，保护关键业务流程不会受信息系统重大失效或自然灾害的影响，并确保他们的及时恢复
    - **14.1.1**在业务连续性管理过程中包含信息安全
    - **14.1.2**业务连续性和风险评估
    - **14.1.3**开发并实施包括信息安全的连续性计划
    - **14.1.4**业务连续性计划框架
    - **14.1.5BCP** 的测试、保持和再评估

附录A (强制性)控制目标和控制措施

- 符合性 (3,10)
  - 15.1 与法律法规要求的符合性 目标：避免违反法律、法规、规章、合同要求和其他的安全要求
  - 15.2 符合安全方针、标准，技术符合性 目标：确保系统符合组织安全方针和标准
  - 15.3 信息系统审核的考虑因素 目标：最大化信息系统审计的有效性，最小化来自/对信息系统审计的影响

Agenda

一、信息安全基础知识

二、信息安全管理标准

三、认证相关介绍

认证需要具备的条件

- 建立了ISMS 体系
- 完备的文件体系
  - 安全方针
  - 适应性申明**SOA**
  - 必须的程序文件
  - 风险评估方法\计划\结果\处置措施等
  - **……**
- 正式运行了3个月以上
- 有运行的全部记录

认证基础、方法和结果

- 认证的基础:
  - 标准ISO27001:2005/ISO17799:2005
- 认证的方法:
  - 抽样检验、对组织体系的符合性
- 认证的结果:
  - 未通过认证
    - 严重不合格
  - 通过认证
    - 一般不合格
    - 观察项

谢谢！