信息安全意识培训与案例分析

内 容 介 绍

- 信息安全基础知识
- 信息安全案例分析
- ISO27001标准简介
- ISO27001实施流程

1、背景—信息时代

- 我们已经身处信息时代
- 信息时代的特征
  - 计算机和网络成为重要的生产工具
  - 计算机和网络在我们的生活中也起到了非常重要的作用
  - 传统的时间和空间观发生了巨大变化
  - 信息成为人类社会发展的重要资源
  - 信息爆炸
  - 安全的概念被不断扩展和延伸

2、关键资产—信息

- 什么是信息？

信息是经过加工的数据或消息。

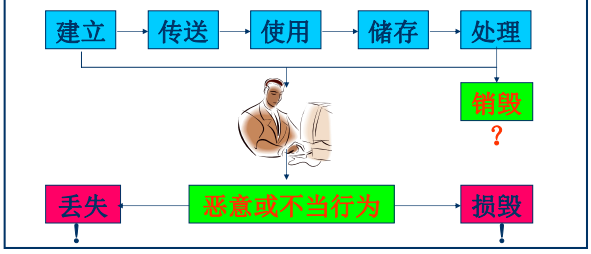
信息是对决策者有价值的数据。

2、关键资产—信息

- 企业应保护什么信息？
  - 知识产权；
  - 技术秘密；
  - 重要的合同；
  - 客户资料；
  - 软件产品的源代码；
  - 财务数据；
  - 内部文件；
  - ……

2、关键资产—信息

- 信息的生命周期：



2、关键资产—信息

- 信息的存在形式
  - 打印或写在纸上；
  - 存在于计算机或网络中；
  - 以邮寄、电子邮件方式交换；
  - 言语交谈；
  - 传输的电波等等。

赛 宝 认 证 中 心
CEPREI Certification Body

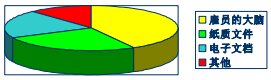
2、关键资产—信息

- 信息的存储介质
  - 纸、胶片；
  - 硬盘、U盘、光盘、磁带、磁光盘；
  - 计算机网络；
  - 员工大脑；

赛 宝 认 证 中 心
CEPREI Certification Body

2、关键资产—信息

- 组织的“信息”在哪里？
  - 雇员的大脑：42%；
  - 纸质文件：26%；
  - 电子文档：20%
  - 其他：12%；



“不论信息采取何种方式或采取何种手段共享或存储，它总应得到妥善保护”

赛 宝 认 证 中 心
CEPREI Certification Body

2、关键资产—信息

- 信息为什么会有安全问题
  - 信息具有重要的价值
    - 信息社会对信息的高度依赖
    - 信息的高附加值会引起盗窃、滥用等威胁

赛 宝 认 证 中 心
CEPREI Certification Body

信息具有重要的价值

广州好又多商业机密泄漏，巨亏4200万元

赛 宝 认 证 中 心
CEPREI Certification Body

2、关键资产—信息

- 信息为什么会有安全问题
  - 信息系统固有的脆弱性
    - 信息本身易传播、易毁坏、易伪造
    - 信息平台的脆弱性

信息系统固有的脆弱性

纽约股市闪电崩盘10分钟,华尔街蒸发万亿美元

赛 宝 认 证 中 心
CEPREI Certification Body

2、关键资产—信息

- 信息为什么会有安全问题
  - 信息安全管理的不健全
    - 未被采纳的策划案——放弃也是一种选择
    - 公用设备——如U盘

赛 宝 认 证 中 心
CEPREI Certification Body

信息安全管理的不健全

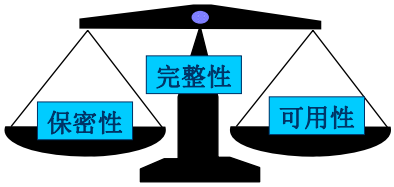
凯恩股份技术图纸和文件泄漏，1年之内损失2000万

KAN 浙江凯恩特种材料股份有限公司
ZHEJIANG KAN SPECIALITIES MATERIAL CO.,LTD.

赛 宝 认 证 中 心
CEPREI Certification Body

3、信息安全的定义

- ISO/IEC17799：2005
  保持信息的保密性、完整性、可用性；
  另外，也包括其他属性，如：真实性、可核查性、不可否认性和可靠性。



赛 宝 认 证 中 心
CEPREI Certification Body

3、信息安全的定义

- 保密性Confidentiality：
  信息不被可用或不被泄漏给未授权的个人、实体和过程的特性 。
- 完整性Integrity：
  保护资产的准确和完整的特性。
- 可用性Availability：
  需要时，授权实体可以访问和使用的特性 。

赛 宝 认 证 中 心
CEPREI Certification Body

4、为什么需要信息安全

- 国家安全的需要
  - 政治、军事、经济、教育对信息的依赖
  - 要符合法律、法规的要求
- 组织持续发展的需要
  - 信息是组织的重要资产
  - 提高服务水平的重要措施
  - 保护核心资产、知识产权，获得竞争优势
  - 向贸易伙伴证明对信息安全的承诺
  - 内部管理的工具——控制及信心
- 保护个人隐私与财产的需要

4、为什么需要信息安全

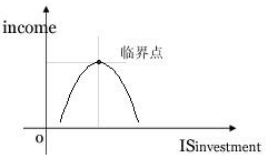
- 信息安全能帮助企业盈利吗
  - 降低成本
    - a)良好的信息安全规划和风险评估会减少企业盲目的IT投资；
    - b)减少了因系统中断、服务中断而带来的客户不满意度以及相关的失效处理成本；

赛 宝 认 证 中 心
CEPREI Certification Body

4、为什么需要信息安全

根据Alfred Marshall在*Principles of Economics*（*经济学原理*） 中的论断：
任何要素的过分使用都会引起报酬递减

$Y_{income} = f(IS_{investment})$



赛 宝 认 证 中 心
CEPREI Certification Body

4、为什么需要信息安全

- 信息安全能帮助企业盈利吗
  - 增加收入
    - a)保护核心信息资产、知识产权，获得竞争优势；
    - b)增强可用性，提高企业反应速度，获得更高客户满意度；

赛 宝 认 证 中 心
CEPREI Certification Body

内 容 介 绍

- 信息安全基础知识
- 信息安全案例分析
- ISO27001标准简介
- ISO27001实施流程

赛 宝 认 证 中 心
CEPREI Certification Body

案 例 一

原华为工程师

网上盗卖充值卡

赛 宝 认 证 中 心
CEPREI Certification Body

案 例 二

创维两工程师

偷卖技术换股份

案 例 三

广州好又多

商业资讯被外泄

案 例 四

苏州医疗器械总厂

技术专利被侵占

案 例 五

张氏铜锣

技术秘密泄露

案 例 六

日常工作中常见的

信息安全事件

1、打印机——打印件滞留带来信息漏洞
2、打印纸背面——好习惯换取大损失
3、电脑易手——新员工真正的入职导师
4、共享文件——局域网中获得公司内部机密的通道。
5、经营数据统计对比——聪明反被聪明误
6、入职培训——信息保卫战从此被动
7、传真机——你总是在半小时后才拿到发给你的传真
8、公用设备——等于公用信息
9、产品痕迹——靠“痕迹”了解你的未来

10、光盘刻录——资料在备份过程中流失
11、邮箱——信息窃取的中转站
12、隐藏分区——长期窃取公司资料必备手法
13、私人电脑——大量窃取资料常用手段
14、会议记录——被忽视的公司机密
15、未被采纳的策划案——放弃也是一种选择
16、客户——你的机密只是盟友的谈资
17、解聘后半小时——不要给他最后的机会。
18、入职后一星期——新人在第一个星期里收集的资料是平时的5倍。

企业面临的信息安全问题

1、项目成果、技术秘密外泄
2、关键技术人员跳槽
3、标底信息提前透露
4、客户资料泄密
5、信息系统瘫痪
6、财务数据失控
7、专利被侵权
……

我们面临着众多的信息安全问题

木马 病毒	拒绝服务攻击	已知蠕虫攻击
商业间谍	Cookie欺骗攻击	信用卡大盗
钓鱼攻击	零日蠕虫攻击	金融数据泄漏
命令注入攻击	非法修改参数	数据库特权混用
恶意移动代码	专利数据泄漏	缓冲区溢出
暴力破解攻击	目录遍历攻击	会话劫持攻击
跨站脚本攻击	数据破坏攻击	非法修改表单
数据小偷 ……		

怎 么 办 ？

通常想法：技术路线

- 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 备 技 术：业务连续性技术，前提就是对数据的备份。

信息安全＝技术＋产品＝防病毒软件＋防火墙＋入侵检测系统＋… ？

但技术和产品达不到人们需要的水准

- 例如:微软的Windows NT、IBM的AIX等常见的企业级操作系统，大部分只达到了美国国防部TCSEC C2级安全认证，而且核心技术和知识产权都是国外的，不能满足国家涉密信息系统或商业敏感信息系统的需求。

技术往往落后于风险的出现

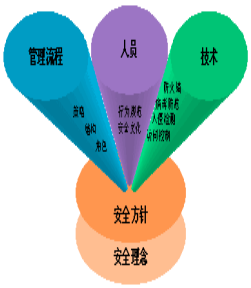
- 在计算机病毒与病毒防治软件的对抗过程中，经常是在一种新的计算机病毒出现并已经造成大量损失后，才能开发出查杀该病毒的软件，

技术管理不当，带来新风险

- 即使某些安全技术和产品在指标上达到了实际应用的某些安全需求，如果配置和管理不当，还是不能真正地实现这些安全需求。
  - 例如，虽然在网络边界设置了防火墙，但出于风险分析欠缺、安全策略不明或是系统管理人员培训不足等原因，防火墙的配置出现严重漏洞，其安全功效将大打折扣。
  - 再如，虽然引入了身份认证机制，但由于用户安全意识薄弱，再加上管理不严，使得口令设置或保存不当，造成口令泄漏，那么依靠口令检查的身份认证机制会完全失效。

我们观点：信息安全不是单纯的技术问题

- 信息安全是组织的一个业务问题，需要管理的承诺和支持
- 信息安全技术并不能解决所有的安全问题
- 信息安全要从多方面进行管理:
  - 人员
  - 物理安全
  - 网络安全
  - 业务持续性
  - 知识产权
  - ……

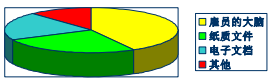


三分技术，七分管理

统计数据表明，在所有的计算机安全事件中，人为因素占52%，自然灾害占 25% ，技术错误占10%，组织内部人员作案占10%，仅有3%左右是由外部不法人员的攻击造成。属于管理方面的原因比重高达70%以上，而这些安全问题中的95%是可以通过科学的信息安全管理来避免。

三分技术，七分管理

- 组织的“信息”在哪里？
  - 雇员的大脑：42%；
  - 纸质文件：26%；
  - 电子文档：20%
  - 其他：12%；



信息安全保障的三大要素

信息安全＝防患意识＋管理流程＋严格的制度
＋法律保障＋优秀的执行团队
＋先进技术＋……

信息安全整体解决方案

在组织内建立和实施基于最新国际标准ISO/IEC27001:2005（由BS7799发展而来）的信息安全管理体系（ISMS）。

它是目前国际上最先进的信息安全整体解决方案它以组织风险评估为基石，运用PDCA过程方法和133项信息安全控制措施来帮助组织解决信息安全问题，实现信息安全目标。

赛 宝 认 证 中 心
CEPREI Certification Body

基于风险的信息安全管理体系

信息安全建设的宗旨之一，就是在综合考虑成本与效益的前提下，通过恰当、足够、综合的安全措施来控制风险，使残余风险降低到可接受的程度。

赛 宝 认 证 中 心
CEPREI Certification Body

内 容 介 绍

- 信息安全基础知识
- 信息安全案例分析
- ISO27001标准简介
- ISO27001实施流程

赛 宝 认 证 中 心
CEPREI Certification Body

信息安全管理体系

- ISMS定义
- ISMS标准产生发展的动力
- ISMS标准的构成
- ISMS标准的发展历史
- ISO27000标准族介绍

赛 宝 认 证 中 心
CEPREI Certification Body

ISMS定义

信息安全管理体系（Information Security Management System，简称ISMS）

是基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的体系，是一个组织整个管理体系的一部分。

赛 宝 认 证 中 心
CEPREI Certification Body

ISMS标准产生发展的动力

- 信息化
  - -- 业务对信息的依赖
  - -- 信息系统日益复杂
- 全球化
  - -- 全球工厂
  - -- 竞争优势
- 社会责任
  - -- 保护自己、保护别人

ISMS标准构成

- ISO/IEC27002：2005 （BS7799 Part 1）
  Code of Practice for Information Security Management
  信息安全管理实践指南
- ISO/IEC27001：2005 （BS7799 Part 2）
  Information Security Management Systems-Requirement
  信息安全管理体系-要求

ISMS标准的发展历史

- **BS7799-1 操作规则**
  - 1995年版
  - 1999年版
  - ISO/IEC17799：2000
  - ISO/IEC17799：2005
  - ISO/IEC27002：2005
- **BS7799-2 认证规范**
  - 1998年版
  - 1999年版
  - 2002年版
  - ISO/IEC27001：2005

ISO27000标准族介绍

27000～27009：ISMS基本标准，
27010～27038：ISMS标准族的解释性指南与文档

主题

ISO27001标准内容简介

ISO27001控制目标和措施

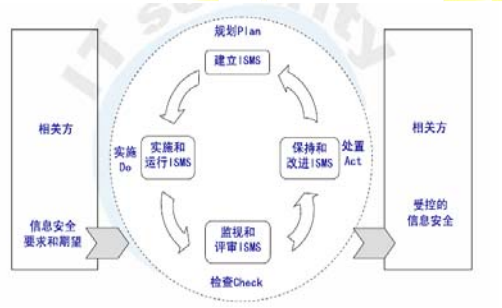
ISO/IEC27001 标准内容

- **前言、简介**
- **正文（八章）**
  范围、参考标准、术语和定义、信息安全管理体系、
  管理职责、ISMS内审、ISMS管理评审、ISMS改进。
- **附录（三个）**
  A、 控制目标和控制措施　　B、OECD和本国际标准
  C、本标准与ISO9001:2000、ISO14001:2004标准的对应关系

ISO/IEC27001 标准特点

- **适用于各种类型、不同规模和业务性质的组织**
- **采用PDCA的过程方法**
- **与其他管理体系兼容**

ISO/IEC27001 信息安全管理模式



赛 宝 认 证 中 心
CEPREI Certification Body

ISO/IEC27001条款删减要求

- 对第4、5、6、7和8条款的内容不能删减
- 对任何控制的删减必须满足风险接受的准则， 并提供证据和说明理由

赛 宝 认 证 中 心
CEPREI Certification Body

ISMS 文件架构

赛 宝 认 证 中 心
CEPREI Certification Body

ISO/IEC27001结构

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 引言	0.1总则	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
	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。

赛 宝 认 证 中 心
CEPREI Certification Body

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

赛 宝 认 证 中 心
CEPREI Certification Body

4. 信息安全管理体系	4.2 建立并管理ISMS	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 内部审核		组织应该通过定期的内部审核来确定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 控制目标和控制措施	A.5 安全方针 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，共11大控制领域39个控制目标133个控制措施。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 ISO9001:2000 ISO14001:1999和本标准之间的一致性		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。
参考书目		

标准附录

- 附录A：是规范性的（normative）附录，应作为4.2.1规 定的ISMS过程的一部分。
- 附录B：是资料性（informative）的附录。
- 附录C：是资料性（informative）的附录。

附录A：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	5.1.1-5.1.2
6. 组织信息安全	6.1 内部组织	6.1.1-6.1.8
	6.2 外部伙伴	6.2.1-6.2.3
7. 资产管理	7.1 资产责任	7.1.1-7.1.3
	7.2 信息分类	7.2.1-7.2.2
8. 人力资源安全	8.1 聘用前的控制	8.1.1-8.1.3
	8.2 聘用期间	8.2.1-8.2.3
	8.3 解聘和职位变更	8.3.1-8.3.3
9. 物理与环境安全	9.1 安全区域	9.1.1-9.1.6
	9.2 设备安全	9.2.1-9.2.7

10. 通信与操作管理	10.1 操作程序和责任	10.1.1-10.1.5
	10.2 第三方服务交付管理	10.2.1-10.2.3
	10.3 系统规划及验收	10.3.1-10.3.2
	10.4 抵御恶意和移动代码	10.4.1-10.4.2
	10.5 备份	10.5.1 信息备份
	10.6 网络安全管理	10.6.1-10.6.2
	10.7 介质处理	10.7.1-10.7.4
	10.8 信息的交换	10.8.1-10.8.5
	10.9 电子商务服务	10.9.1-10.9.3
	10.10 监视	10.10.1-10.10.6

11 访问控制	11.1 访问控制的业务需求	11.1 访问控制策略
	11.2 用户访问管理	11.2.1-11.2.4
	11.3 用户责任	11.3.1-11.3.3
	11.4 网络访问控制	11.4.1-11.4.7
	11.5 操作系统访问控制	11.5.1-11.5.6
	11.6 应用和信息访问控制	11.6.1-11.6.2
	11.7 移动计算和通信	11.7.1-11.7.2
12. 信息系统获取、开发与维护	12.1 信息系统的安全需求	12.1.1 安全需求分析
	12.2 应用程序中正确的处理	12.2.1-12.2.4
	12.3 密码控制	12.3.1-12.3.2
	12.4 系统文件的安全	12.4.1-12.4.3
	12.5 开发和支持过程的安全	12.5.1-12.5.5
	12.6 技术漏洞管理	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	13.1.1-13.1.2
	13.2 管理信息安全事件和改进	13.2.1-13.2.3
14. 业务连续性管理	14.1 业务连续性管理的信息安全方面	14.1.1-14.1.5
15. 符合性	15.1 符合法律要求	15.1.1-15.1.6
	15.2 符合安全策略和标准	15.2.1-15.2.2
	15.3 信息系统审计的考虑	15.3.1-15.3.2

表B.1 OECD原理和PDCA模型

OECD原理	相应的ISMS过程和PDCA阶段
意识 参与者应当意识到信息系统和网络的安全需要，并且知道为提高安全性他们能做些什么。	该项活动是实施（Do）阶段的一部分（见4.2.2和5.2.2）
职责 所有参加者对信息系统和网络的安全负责。	该项活动是实施（Do）阶段的一部分（见4.2.2和5.1）
响应 参加者应当以及时和合作的方式行动防止、查明并且对安全事件作出反应。	这是检查阶段（见4.2.3和6至7.3）的监视活动和处置（Act）阶段（见4.2.4和8.1至8.3）的响应活动。策划（Plan）和检查（Check）阶段的一些方面也可能包括这些。
风险评估 参与者应当管理风险评估。	该项活动是策划（Plan）阶段的一部分（见4.2.1），风险再评估是检查（Check）阶段的一部分（见4.2.3和6.到7.3）。

表B.1 OECD原理和PDCA模型

安全性设计与实施 参与者应当将安全性作为信息系统和网络的基本要素。	一旦完成风险评估，对风险处理控制的选择作为策划（Plan）阶段（见4.2.1）的一部分。此时实施（Do）阶段（见4.2.2和5.2）包括实现和这些控制的使用
安全管理 .参与者应当采用综合方案进行安全管理	.风险管理包括对意外事件、正在进行的维护、复查和审核进行的预防、检测和响应过程。所有这些都包含在策划（Plan）、实施（Do）、检查（Check）和处置（Act）阶段。
再评估 .参与者应当复查和再评估信息系统和网络的安全性，对安全方针进行适当的更改、实践、测量和程序化。	信息安全的再评估是检查（Check）阶段的一部分（见4.2.3 和6到7.3）。采用定期复查应当检查信息安全管理系统的有效性，改进安全性是处置（Act）阶段的一部分（见4.2.4 和8.1~8.3）。

表C.1 ISO 9001:2000、ISO 14001:2004 和本标准之间的对应关系

本标准	ISO 9001:2000	ISO 14001:2004
0 概述 0.1 总则 0.2过程方法 0.3与其它管理体系的兼容性	0 概述 0.1总则 0.2过程方法 0.3 与ISO9004的关系 0.4与其它管理体系的兼容性	概述
1 范围 1.1 总则 1.2 应用	1 范围 1.1 总则 1.2 应用	1 范围
2 引用标准	2引用标准	2引用标准
3 术语和定义	3 术语和定义	3 术语和定义

表C.1 ISO 9001:2000、ISO 14001:2004 和本标准之间的对应关系

4 ISMS要求	1. QMS要求	4 EMS要求
4.1 总要求	4.1 总要求	4.1 总要求
4.2 ISMS的建立和管理		
4.2.1 建立ISMS		
4.2.2 实现和运做ISMS		4.4 实施与运行
4.2.3 监视和评审ISMS	8.2.3 过程的监视和测量	4.5.1 监视与测量
	8.2.4 产品的监视和测量	
4.2.4保持和改进ISMS		4.5.2不符合、纠正和预防措施
4.3 文件要求	4.2文件要求	
4.3.1 总则	4.2.1 总则	
	4.2.2 质量手册	
4.3.2 文件控制	4.2.3 文件控制	4.4.5文件控制
4.3.3 记录控制	4.2.4 记录控制	4.5.34 记录控制

5 管理职责 5.1 管理承诺	5 管理职责 5.1 管理承诺 5.2 以顾客为关注焦点 5.3 质量方针 5.4 策划 5.5 职责、权限与沟通	4.2 环境方针 4.3 策划
5.2 资源管理 5.2.1 资源提供 5.2.2培训、意识和能力	6 资源管理 6.1 资源提供 6.2 人力资源 6.2.2 能力、意识和培训 6.3 基础设施 6.4 工作环境	4.2.2培训、意识和能力
6. 内部ISMS审核	8.2.2 内部审核	4.5.5 内部审核
7. ISMS的管理评审 7.1总则 7.2评审输入 7.3评审输出	5.6管理评审 5.6.1总则 5.6.2评审输入 5.6.3评审输出	4.6管理评审

表C.1 ISO 9001:2000、ISO 14001:2004和本标准之间的对应关系

8. ISMS改进 8.1持续改进 8.2纠正措施 8.3预防措施	8. 改进 8.5.1持续改进 8.5.2纠正措施 5.5.3预防措施	4.5.3不符合、纠正和预防措施
附录A 控制目标和控制措施 附录B OECD原则和本标准 附录C ISO9001:2000、ISO14001:2004和本标准之间的对照	附录A ISO14001:1996和ISO9001:2000的联系	附录A 规范使用指南 附录B ISO14001:2004和ISO 9001:2000的联系

主题

ISO27001标准内容

ISO27001控制目标和措施

ISO 27001:2005 附录 A

- 11个控制域
- 39个控制目标
- 133个控制措施

控制域结构—例子

8 :Human resources security

控制域

控制目标

8.1 Prior to employment
8.2 During employment
8.3 Termination or change of employment

8.3.1 Termination responsibilities
8.3.2 Return of assets
8.3.3 Removal of access rights

控制措施

11个控制领域

安全方针（1,2）

- 建立适合的企业信息安全方针
- 方针表明公司的信息安全管理到底要干什么，也就是建立信息安全的意图、目的或者方向
- 方针可以是多级的，既有宏观的策略，又有针对每一个细节的二级甚至更低层策略

信息安全组织（2,11）

- 在组织内部管理信息安全
  - 在组织建立信息安全部门，如信息安全管理委员会/小组
  - 清楚定义各角色的安全职责
  - 信息处理设备的授权
  - 应识别和定期评审反映组织信息保护需要的保密或不许泄露协议的需求
- 保持被外部组织访问、处理、通信或管理的组织信息和信息处理设施的安全

赛 宝 认 证 中 心
CEPREI Certification Body

资产管理（2,5）

- 明确资产责任，保持对组织资产的适当保护
  - 识别重要资产，并形成清单
  - 指导资产的所有者
- 将信息进行归类，确保信息资产受到适当程度的保护
  - 应根据资产其对组织的价值、法律要求、敏感性和危险程度进行分类
  - 对信息进行标识，如标明信息的密级。不同等级的信息其处理方式不同

赛 宝 认 证 中 心
CEPREI Certification Body

人力资源安全（3,9）

- 人作为特殊的一种信息载体，是管理体系的主体，也是管理体系中最难管理的一个环节
- 我们应该从人员在组织中的生命周期的三个阶段识别了相应的控制措施：
  - 聘用前的职责描述、人员筛选以及聘用条件约束等
  - 在职期间的管理职责和教育训练
  - 以及离职时的相关要求

赛 宝 认 证 中 心
CEPREI Certification Body

物理与环境安全（2,13）

- 物理环境是整个组织正常运营的支撑，保障信息安全时，物理环境的安全需要同样进行控制
- 包括组织环境周界划分、出入管控、安全区域等管理措施，此外，针对设备的安置和维护工作也有相应的控制

赛 宝 认 证 中 心
CEPREI Certification Body

通信及操作安全（10,32）

- 信息是在组织的各项业务中产生的，保护信息安全的目的就在于保证业务的持续性，组织日常的运作是信息安全管理的主要组成部分
- 这包括日常的操作、变更的控制、容量的规划、备份、恶意软件防护、存储介质处理、信息交换、电子商务以及监控等管理要求

赛 宝 认 证 中 心
CEPREI Certification Body

访问控制（7,25）

- 当今信息安全管理区别于传统的保密，就是通过访问控制，在保障信息的机密性的同时，保持可用性和完整性
- 访问控制是信息安全管理之中的主要技术体现
- 标准从访问控制策略开始，规范了用户管理、用户职责的方法，并从网络、操作系统、应用系统和信息等层次给出了各级访问控制的要求
- 移动办公和远程工作也需要规范管理

系统获得、开发与维护（6,16）

- 信息系统本身设计开发的安全性，维护当中的安全性，以及获得一个新的信息系统时所需要关注的安全要求

赛 宝 认 证 中 心
CEPREI Certification Body

信息安全事件管理（2,5）

- 及时报告信息安全事件
- 信息安全意外事件的管理
- 从意外事件的处理当中取得经验教训

赛 宝 认 证 中 心
CEPREI Certification Body

业务持续性管理（1,5）

- 对那些可能导致业务中断的事件，通过制定一套业务连续性管理计划，构建一个业务连续管理的氛围和文化，在出现重大故障和灾害时，依照组织的业务需求，保持关键业务的连续
- 信息安全管理的业务连续性是组织整体的业务连续性管理的重要组成部分

赛 宝 认 证 中 心
CEPREI Certification Body

符合性（3,10）

- 识别的适用法律要求
- 知识产权保护
- 组织记录的保护
- 数据保护以及个人信息的隐私
- 防止信息处理设备的误用

赛 宝 认 证 中 心
CEPREI Certification Body

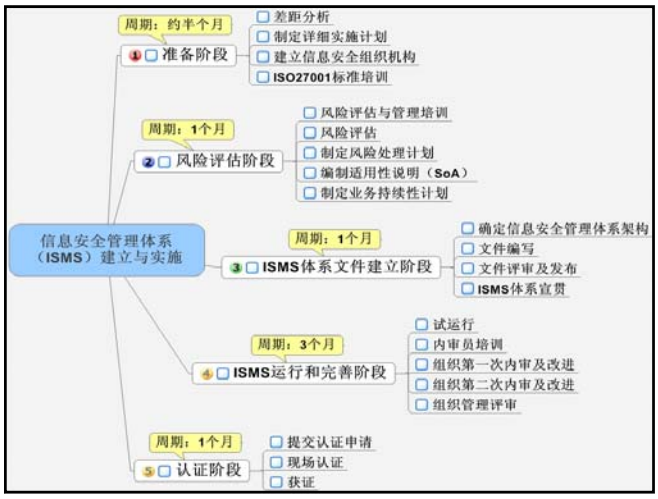
小 结

一、信息安全方针				
二、信息安全组织				
三、资产管理				
四、人力资源安全	五、物理与环境安全	六、通信及操作管理	七、访问控制	八、系统获取、开发和维护
九、信息安全事件管理				
十、业务持续性管理				
十一、符合性				

赛 宝 认 证 中 心
CEPREI Certification Body

内 容 介 绍

- 信息安全基础知识
- 信息安全案例分析
- ISO27001标准简介
- ISO27001实施流程



主题

如何建立信息安全管理体系

信息安全管理体系建立与实施过程

信息安全管理体系认证

1、确立信息安全方针

- 信息安全策略是一个组织信息安全的最高方针。
- 信息安全策略应该简单明瞭，通俗易懂，并形成书面文件，发给组织内的所有员工。
- 对所有相关员工进行信息安全策略的培训，对信息安全负有特殊责任的人员要进行特殊的培训，以使信息安全方针真正根植于组织所有员工的脑海中并落实到实际工作中。

2、定义ISMS的范围

- ISMS范围确定需要重点考虑信息安全管理领域；
- 组织应该根据实际情况，在整个组织范围内、或在个别部门和领域架构ISMS；
- 将组织划分成不同的信息安全控制领域，以利于组织对有不同需求的领域进行适当的信息安全管理。

3、进行信息安全风险评估

- 信息安全风险评估的复杂程度将取决于风险的复杂程度和受保护资产的敏感程度，所采用的评估措施应与组织对信息资产保护的需要相一致；
- 风险评估主要是对ISMS范围内的信息资产、脆弱性、所受到的威胁、已有安全控制措施进行识别和评估。
- 风险评估主要依赖于信息和系统的性质、使用信息的目的、系统环境等因素，风险评估时需要将直接后果和潜在后果一起考虑。

4、信息安全风险管理

根据风险评估的结果进行相应的风险管理，主要包括以下措施：

- 降低风险：在转移风险前先采取措施降低风险；
- 避免风险：如采用不同的技术、更改操作流程等；
- 转移风险：通常只有风险不能被降低或避免且被第三方接受时才采用；一般用于低概率、发生给组织造成重大损失或影响的风险。
- 保持风险：用于那些在采取降低和避免风险措施后，出于实际和经济方面的原因，只要组织进行运营，就必然存在和必须接受的风险。

5、确定控制目标选择控制措施

- 选择原则是费用不超过风险所造成的损失（成本意识）；
- 信息安全是一个动态的系统工程，组织应适时对控制目标和措施进行校验和调整，以适应变化的情况，使组织的信息资产得到有效、经济、合理的保护。

赛 宝 认 证 中 心
CEPREI Certification Body

6、准备信息安全适用性声明

信息安全适应性声明记录了组织内相关的风险控制目标和针对它采用的各种控制措施；向组织内外表明对信息安全风险的态度和作为，以表明组织已经全面、系统地审视了组织的信息安全系统，并将所有有必要管理的风险控制在能够接受的范围内。

赛 宝 认 证 中 心
CEPREI Certification Body

主题

如何建立信息安全管理体系

信息安全管理体系建立与实施过程

信息安全管理体系认证

赛 宝 认 证 中 心
CEPREI Certification Body

准备阶段（Preparation）

- 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。
- 差距分析：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。

赛 宝 认 证 中 心
CEPREI Certification Body

实现阶段（Realization）

- 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。

赛 宝 认 证 中 心
CEPREI Certification Body

运行阶段（Operation）

- 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：内审计划，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

成功的关键因素

- 建立反映业务目标的安全方针
- 持续改进方法与公司文化一致
- 管理层强大的支持和承诺
- 对安全需求有良好的理解，有适宜的风险评估和风险管理机制
- 对所有管理者和雇员能有效传达安全意识
- 信息安全方针和标准的指南分发给所有雇员和临时人员
- 提供合适的培训和教育
- 有一套完整和均衡的测量系统，用来评价信息安全管理及持续改进建议的执行情况

主题

如何建立信息安全管理体系

信息安全管理体系建立与实施过程

信息安全管理体系认证

1、认证的价值

➢ 符合法律法规要求

证书的获得，可以向客户和合作伙伴表明：组织遵守了所有适用的法律法规，从而保护企业和相关方的信息系统安全、知识 产权、商业秘密等。

1、认证的价值

➢ 维护企业的声誉、品牌和客户信任

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。

1、认证的价值

➢ 履行好信息安全管理责任

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。

1、认证的价值

➢ 增强员工的意识、责任感和相关技能

强化员工的信息安全意识，规范组织信息安全行为，减少人为原因造成的不必要的损失

1、认证的价值

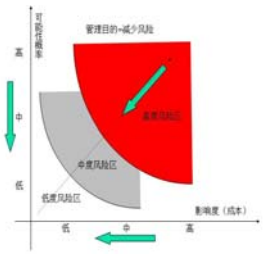
- 获得竞争优势

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，现在很多投标项目已经开始要求ISO27001的符合性了。

1、认证的价值

- 实现风险管理

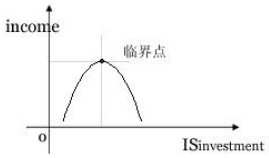
有助于更好地了解信息系统，并找到存在的问题以及保护的办法，保证组织自身的信息资产能够在一个合理而完整的框架下得到妥善保护。



1、认证的价值

- 减少损失，降低成本

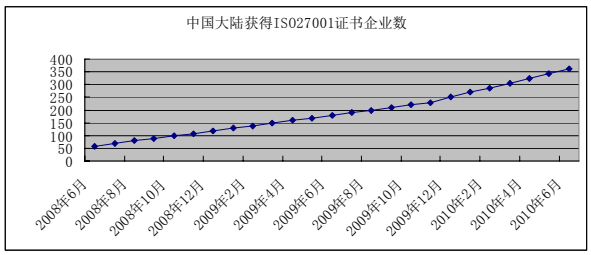
ISMS的实施，能降低因为潜在安全事件发生而给组织带来的损失，在信息系统受到侵袭时，能确保业务持续开展并将损失降到最低程度



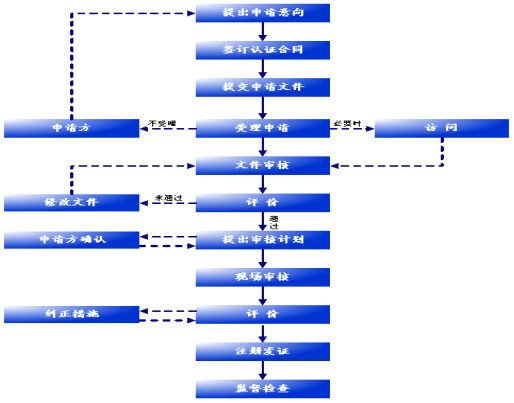
2、全球ISMS认证情况（2010年7月）

Japan	3572	Italy	61	Mexico	24	Netherlands	12
India	490	Poland	56	Brazil	23	Singapore	12
UK	448	Spain	43	Turkey	21	Indonesia	11
Taiwan	373	Ireland	37	UAE	20	Pakistan	11
China	373	Austria	35	Slovakia	19	Bulgaria	10
Germany	138	Thailand	34	France	18	Norway	10
Korea	106	Hong Kong	32	Slovenia	16	Russian Federation	10
USA	96	Romania	30	Philippines	15	Kuwait	9
Czech Republic	85	Australia	29	Pakistan	14	.....	.....
Hungary	71	Greece	28	Saudi Arabia	13	TOTAL	6573

2、全球ISMS认证情况（2010年7月）



3、认证审核过程



总　　结

- 信息安全基础知识
- 信息安全案例分析
- ISO27001标准简介
- ISO27001实施流程

赛 宝 认 证 中 心
CEPREI Certification Body

Questions ?

赛 宝 认 证 中 心
CEPREI Certification Body

谢　谢！