企业信息化发展与安全保障体系构建

曲成义 研究员

2008.9.

“十七大”胡总书记报告指出：

“全面认识工业化、信息化、城镇化、市场化、国际化深入发展的新形式新任务”

“大力推进信息化与工业化融合”

应深刻认识“五化并举”和“二化融合”的战略意义

大力推进信息化与工业化的融合

- 它深刻反映工业化时代特征
- 是信息化(政务、产业、社会）发展中的战略举措
- 对信息化有重大导向作用
- 确保信息化发展的主动权
- 是科学发展的必然选择
- 是产业增长方式、结构调整、流程优化、资源配置、节能降耗、技术创新、能力建设、基础设施的战略推动力
- 是装备制造业的数字化、网络化、智能化，服务业的信息化、现代化的战略选择
- 由“制造”向“创造”，由“粗放”向“精细”，由“资源型”向“创新型”发展的必由之路

信息化与工业化融合的特征

- 信息技术的深层次渗透
- 智能工具与知识管理的涌现
- 机制和技术创新的催化
- 效率和质量的倍增效应
- 增长方式和产业结构的转变

“中央企业”信息化目标

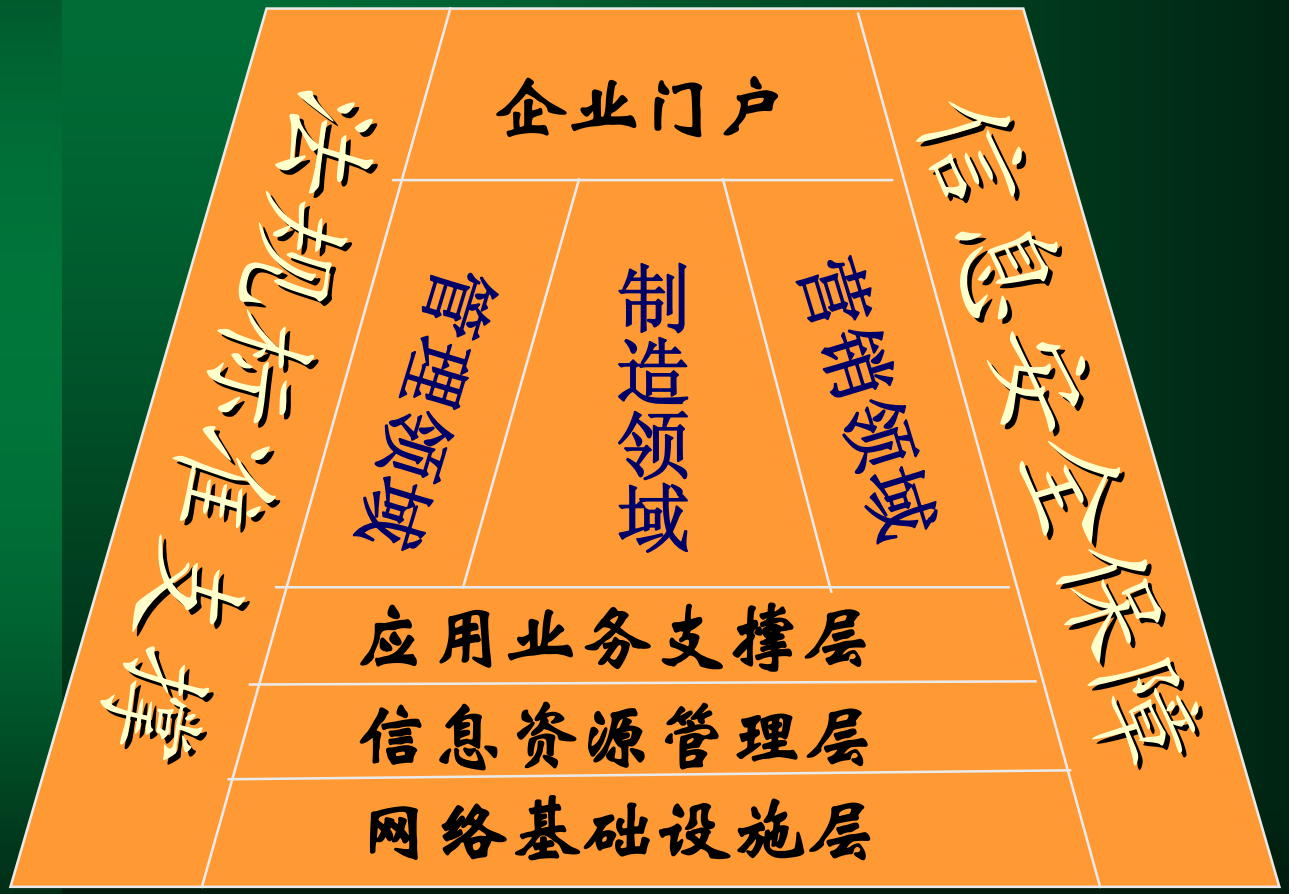
国资委和国信办的国资发［２００７］８号

２０１０年，向信息化集成、共享、协同转变，其信息化基础设施、核心应用、综合管理达到或接近同行业的世界先进水平

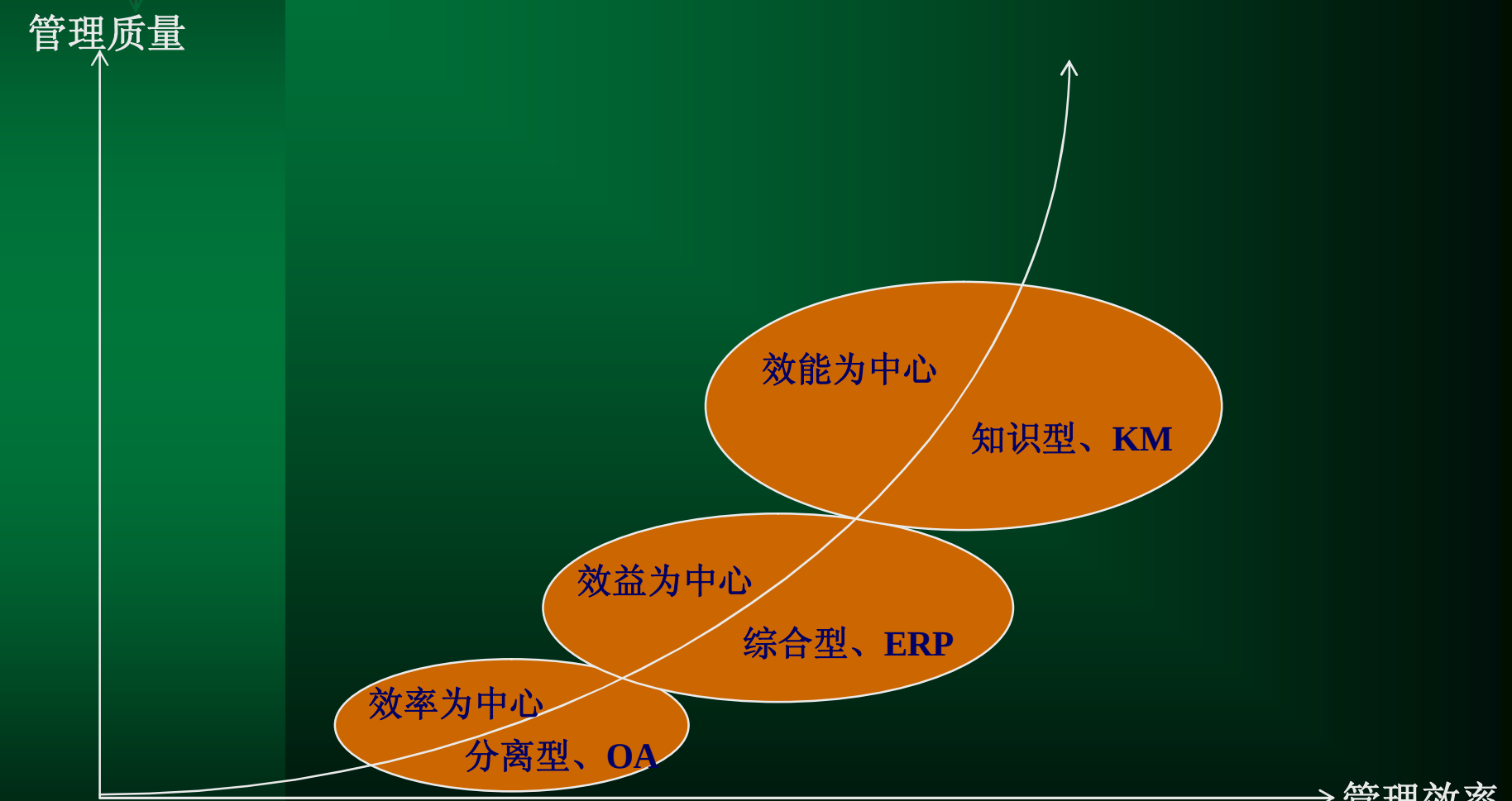
- - - - - - - -

“国资委”决定今后将对央企信息化水平进行年度评价,推进央企信息化的发展

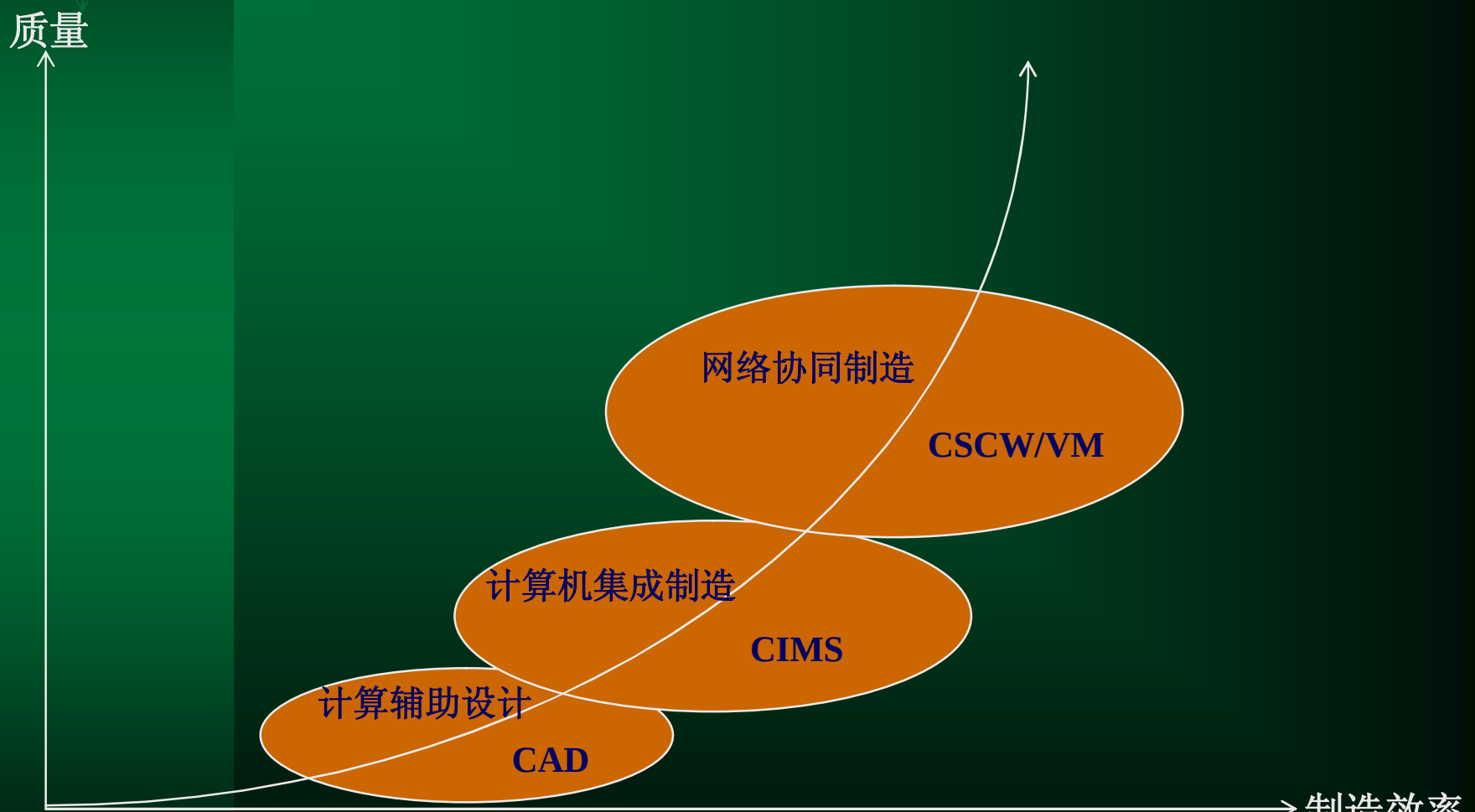
企业信息化体系结构



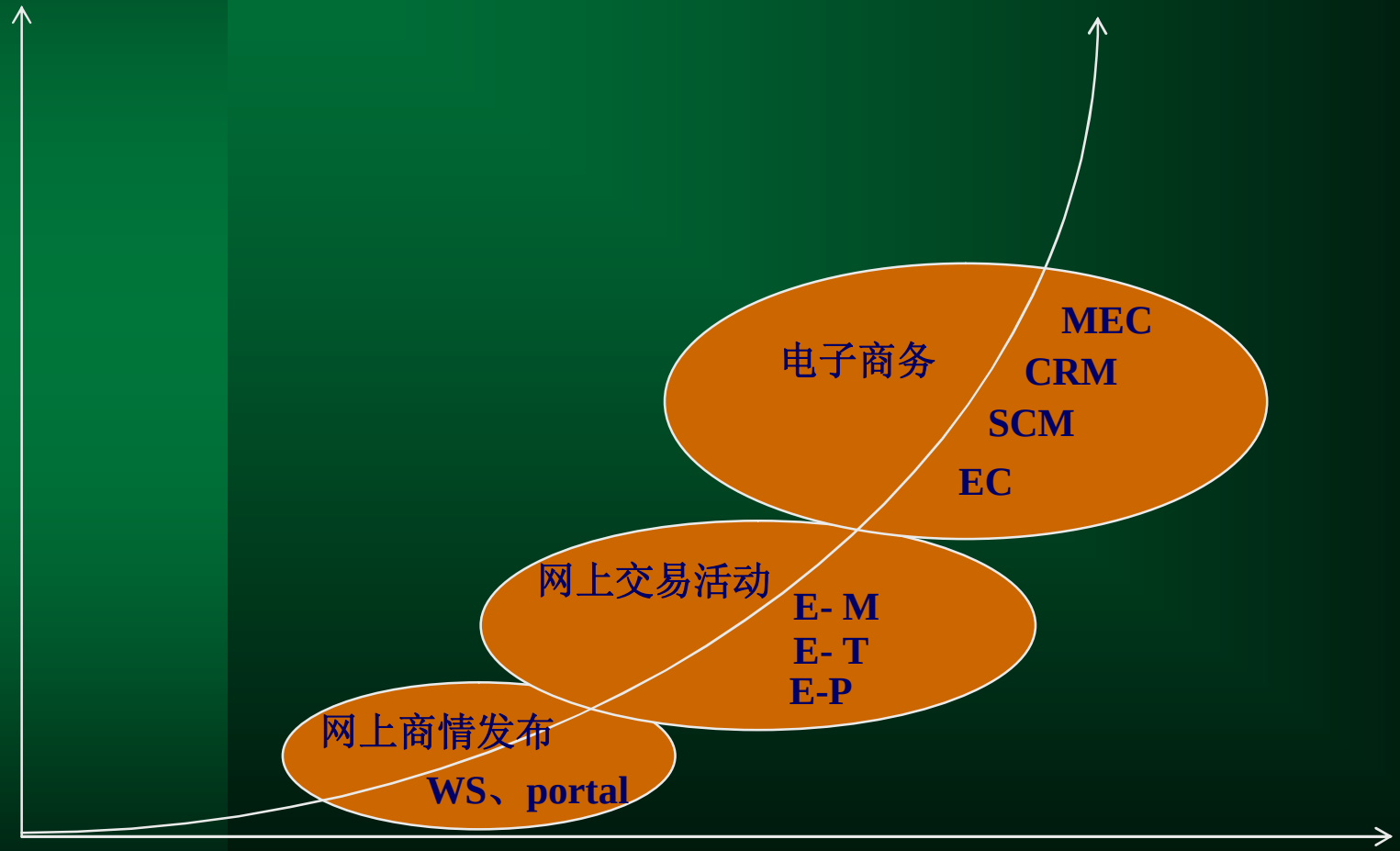
——管理领域信息化——



——制造领域信息化——



——营销领域信息化——



“制造业”数字化工程的前景

- 基于信息技术的制造业革命—“先进制造”
- DoD的IMTR计划为代表
- 数字化、集约化、网络化、虚拟化、智能化
- 数字化设计、现代供应链、知识管理
- 网络协同制造：基于CIMS的规划、研发、设计、制造、试验、装备、训练
- 虚拟制造：样机、装配、验证、检测、系统仿真、
- 企业资源管理：现代物流、金流与业务流的融合（ＯＡ、ＥＲＰ）
- 网络营销：ＥＣ、ＳＣＭ、ＣＲＭ、ＰＯＲＴＯＬ
- 数据中心建设：基于PDM、PLM、CIMS、ERP ,数据高度共享和深度挖掘
- B777：全程数字化、周期降低50%、成本降低25%
- JSF：US的四代战机、周期降低50%、成本降低50%
- 国防科工委：国防型号数字化示范工程

信息化正在对制造业进行强烈的融合

制造业信息安全将面临尖锐挑战

网络突发灾难带来巨大损失

- 电子威胁类
  - 2000年美国八大重要网站遭DDos攻击损失12亿
  - 2001年东京机场航管遭红色病毒侵入千人受阻
  - 2003年冲击波病毒在全球泛滥
  - - - - - -
- 内容威胁类
  - 2005年美国4000万张信用卡信息被窃出现大量卡敲诈
  - 2006年10亿网民的人年均垃圾邮件几千封
  - 当前“谍件”已被注入到80%的重要企业
  - 网络舆情爆发
- 物理威胁类
  - 2001年911事件造成“世贸中心”八百家企业信息系统毁灭而消亡
  - 2006年12.26“台湾海峡”地震导致6条国际通信电缆中断，周边影响严重（MSN、Google、Yahoo - - -）
  - 2008年大冰雪和四川大地震,电力和信道中断

网络威胁的新动向值得高度关注

- “零日攻击”现象出现（魔波蠕虫）
- 复合式病毒给防范增加难度
- 僵尸网成为DDos和垃圾邮件的源头
- 网络仿冒/劫持是在线窃信的重要途径
- 谍件泛滥是窃密/泄密的主要元凶
- 通过网页/邮件/P2P传播恶意代码的数量猛增
- 非法牟利动机明显增加和趋于嚣张
- 黑客地下产业链正在形成
- 僵尸源和木马源的跨国控制应该高度警惕
- 内部安全事件的增加引起高度重视

信息安全事件是“业务持续性管理(BCM)”的重要威胁

- 信息化促进企业(部门)的发展,也蕴育新的信息安全风险
- BCM从体系化、系统化、规范化的高度
  实施作业持续性管理的整体流程
- BCM是企业创利、信誉、责任、发展的前提，从企业生产链、供应链、客户关系、可用性全局出发
- BCM是政府使命、责任、执行力、公信力的前提，从部门业务流程、信息共享、部门协同、系统可用性全局出发
- “信息安全保障”是“BCM”的重要内核之一

业务持续性管理认证标准
(BS 25999)

BCM的六要素： 需求、战略、计划、演练、维护、评估

- **需求理解：** 威胁与资产、关键业务优先次序、容忍中断时间和最低服务水平
- **实施战略：** 控制策略、弹性机制、关键连续、依赖分散、备份替代、利害 相关
- **应急计划：** 响应、控制、恢复、沟通

- **演练：** 验证其可执行性和适应性
- **维护：** 变化、更新、
- **评估：** 评审、调整、改正

国家信息化领导小组第三次会议

《关于加强信息安全保障工作的意见》

—中办发[2003] 27号文—

- 坚持积极防御、综合防范
- 全面提高信息安全防护能力
- 重点保障信息网络和重要信息系统安全
- 创建安全健康的网络环境
- 保障和促进信息化发展、保护公众利益、维护国家安全
- 立足国情、以我为主、管理与技术并重、统筹规划、突出重点
- 发挥各界积极性、共同构筑国家信息安全保障体系

构造“信息安全保障体系”的目标

- 增强信息网络四种安全能力

1 创建信 息安全的基础支撑能力

安全 基础设施、技术与产业、人才与教育

2 提升信息安全防护与对抗能力

W.P.D.R.R.A

3 加强网络突发事件的快速反应能力

4 拥有安全管理的控制能力

- 保障信息及其服务具有六性

保密性、完整性、可用性、真实性、可核查性、可控性

构建企业信息安全保障体系

(一) 信息安全技术体系（ISTS）

(二) 信息安全管理体系（ISMS）

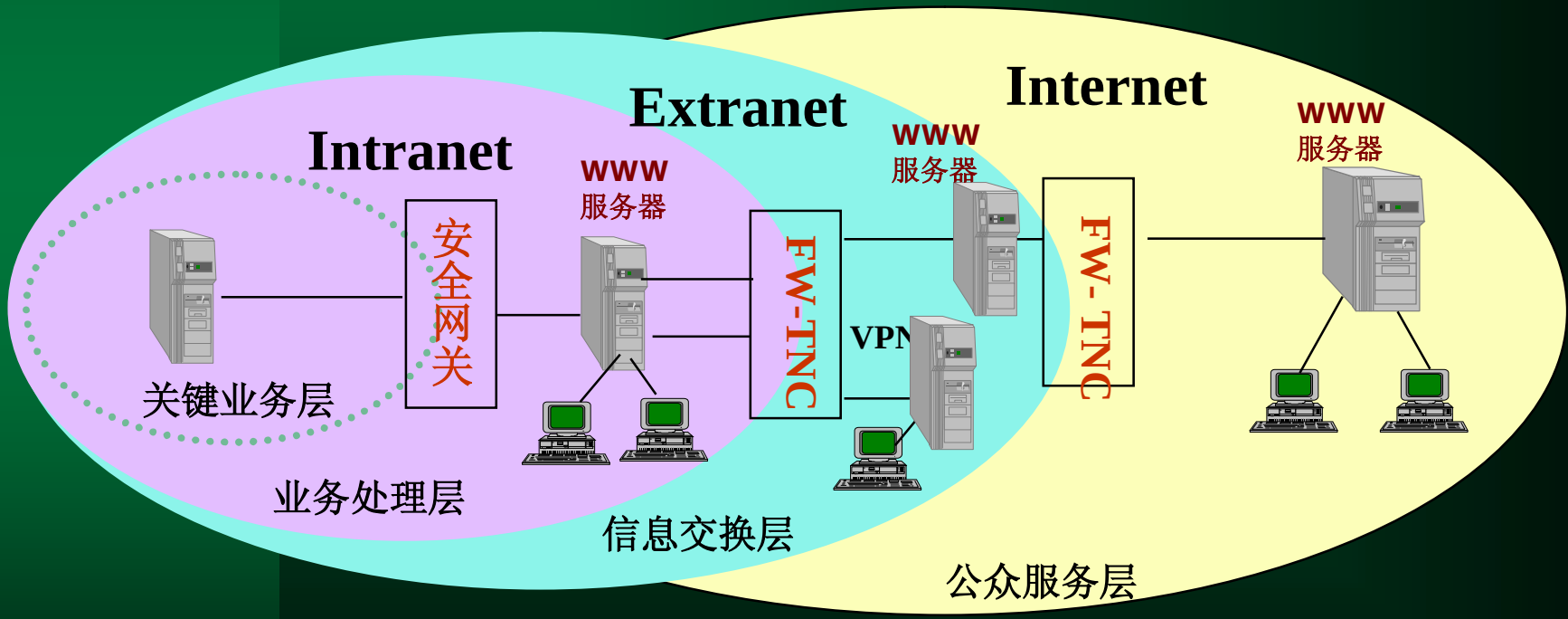
(一) 信息安全技术体系

(1) 建立网络安全纵深防御架构
(2) 启用动态防御技术机制
(3) 构建网络信任体系
(4) 强化内部安全审计
(5) 制订“应急预案”和推进“灾难恢复”
(6) 关注信息安全技术与产业的新动向

(1) 建立网络安全纵深防御架构

- 网络信息安全域的划分、等级保护、可信接入
- 内联网(Intranet)安全服务与控制策略
- 外联网(Extranet)安全服务与控制策略
- 互联网(Internet)安全服务与控制策略
- 公共干线的安全服务与控制策略（有线、无线、卫星）
- 计算环境的安全服务机制
- 多级设防与科学布署策略
- 全局安全测评、集成管理、联动控制与恢复

网络信息安全域划分与安全控制



纵深型防御技术的关注点

- 信息安全域的科学划分与等级保护

  内联网、外联网、互联网

- 信息安全域边界的安全控制

  逻辑隔离/物理隔离

- 信息安全机制的纵深多级布署

  多级配置/集成管理/设施联动

- 公共干线（TSP）的安全保障

  有线/无线/卫星

(2)启用动态防御技术机制

（WPDRRA)

- 基于时间“t”的动态过程防御
  - # Pt：入侵防护时间（Protection）
  - # Dt：入侵检测时间（Detection）
  - # Rt：入侵事件反应恢复时间（Response/Recovery）
- 要求Pt>Dt+Rt
- “资产”价值损失<资产拥有者承受能力
- 预警（Warning）要长备不懈
- 反击（Attack ）要有所准备

动态防御技术的关注点

- 风险评估与系统漏洞的预先发现（SCAN）
- 网络威胁检测、预警
- 信息系统边界防护(FW/UTM/NG)
- 系统监控、入侵检测诊断、防护（IDS/IPS/IPM）
- 应急预案与机制快速启动
- 备份、修复与容灾
- 虚拟资产的从新部署
- 动态拓扑结构的调整
- 积极防御机制的启动
  - 陷阱、隐蔽、追踪、取证
  - 侦探、预警、反击、制瘫

(3) 构建网络信任体系

- 身份认证

  口令/密码、动态口令/ToKen、 CA/PKI、物理识别

- 授权管理

  ACL、RBAC、DAC、MAC、能力表、AA/PMI

- 责任认定

  全局审计、审计保护、反向工程、恢复取证

数字认证与网络信任体系的建设（CA/ PKI）

- 适应开放型、大时空、无限边界
- 提供真实性、完整性、保密性、抗否认性
- 可以构建良好的信任环境
- 支持安全的交往/交换/交易多种业务对象
- PKI/CA在信息化中广泛应用

（4）强化内部审计

- **全局审计**

  网络级、数据库级、应用级、主机级（服务器、端机）
  介质级（磁、光、纸－－－）

- **审计信息的安全加固**

  保密性、完整性、防拷贝、可重现、防假冒

- **审计信息的证据有效性**

  法律上、管理上、技术上（恢复、反向工程）

- **审计点前移**

  事后----- ------> 事中----------> 事前
  （审计）　　（监控）　　（预警）

（5）应急予案与灾难恢复

- 信息安全事件监控予警
- 信息安全事件通报：定级（GB/Z 20982—2007）
- 启动应急予案
- 事件应急抑制：物理、网络、主机、应用、服务
- 事件应急根除
- 事件应急恢复：恢复、抢救、灾备、回退
- 应急审计评估：设施、数据、服务、审计、修订

“灾难恢复”是BCM关键之一，是“应急恢复”的最后一道防线

“信息系统灾难恢复规范”

(安标委 GB/T 20988—2007)

我国灾难恢复等级划分：六级、七要素

大致可以分为二类：数据类、应用类

- “第1级”：数据介质转移（异地存放、安全保管、定期更新）
- “第2级”：备用场地支持（异地介质存放、系统硬件网络可调）
- “第3级”：电子传送和部分设备支持（网络传送、、磁盘镜像复制）
- “第4级”：电子传送和完整设备支持（网络传送、网络与系统就绪）
- “第5级”：实时数据传送及完整设备支持（关键数据实时复制、网络系统就绪、人机切换）
- “第6级”：数据零丢失和远程（在线实时镜像、作业动态分配、实时 无缝切换）

灾难恢复建设的关注点

- 它是业务持续性保证的要素
- 重视等级保护与灾难恢复级别的选择
- 遵循灾难恢复的规范与标准
- 数据级灾备是容灾的基础和起点
- 灾难恢复的集约化建设
- 灾难恢复的社会化服务选择
- 自主建设的几大原则

(6) 关注信息安全技术与产业的新动向

- 由重“防外”向重“内控”迁移
- 由OSI“底层”防护向“应用层”集成防护过渡
- 由基于威胁“特征”向基于威胁“行为”防控转变
- 由“边界”防控向“源头”防控转移
- 由“静态”防御向“动态”防御发展
- 由“单要素”向“多要素”集成联动推进

(二)信息安全管理体制建设

- 国家文件多次指出：

  建立信息安全管理组织（网络信息安全协调小组）

  明确信息安全管理责任制（责任法制化）

  安全技术与安全管理要并重

- 信息安全标准化委员会正抓紧制订管理标准

  （WG7标准化组）

- 构建信息安全保障体系时一定要重视ISMS 的 建设

  （国信办开展了ISMS的试点）

信息安全管理体系(ISMS)

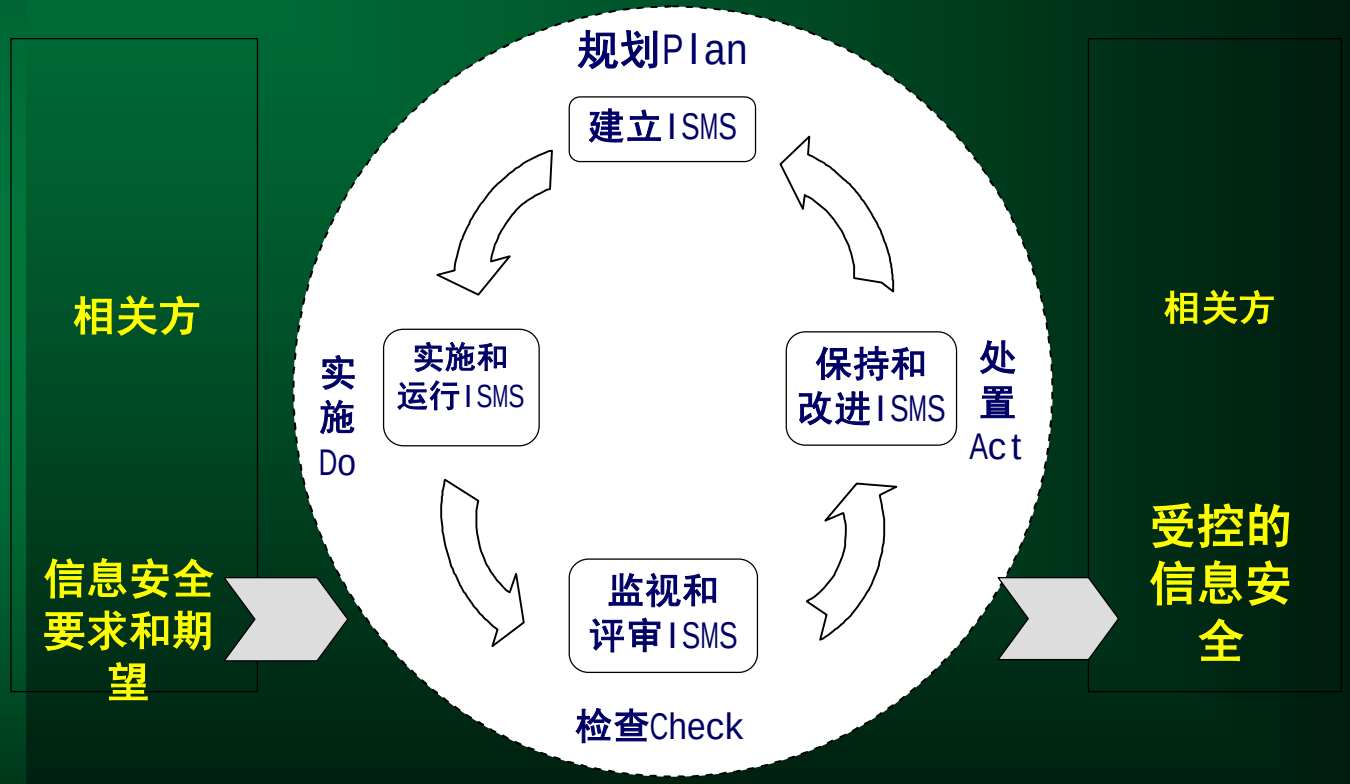
(ISO/IEC 27000 系列)

- 国际重要的信息安全管理标准
- 27001-2005：“信息安全管理体系(ISMS)要求”
  GB/T20269 - 2006
- 27002-2007：”信息安全管理实用规则“
  ISO/IEC 17799-2005 (GB/T - - - - - - - -)
  ISO/IEC 17799-2000（GB/T 19916-2005）
- 27003：ISMS 实施指南（起草）
- 27004：信息安全管理度量 （ISO 13335-2）
- 27005：信息安全风险管理
- 27006、27007、…….

应用于ISMS过程的PDCA模型

ISO/IEC 27001

PDCA循环是能使任何一项活动有效改进的工作程序



应用于ISMS过程的PDCA模型

信息安全管理实用规则

(ISO/IEC 27002-2007)

详细严格的安全管理控制，贯穿系统生命周期全过程和系统所有环节， 11个控制项目,39个控制目标,138个控制措施：

- 安全管理方针
- 信息安全组织
- 信息资产管理
- 人力资源安全
- 物理和环境安全
- 通信与操作管理
- 访问控制
- 信息系统获取
- 开发和维护
- 信息安全事件管理
- 业务持续性管理
- 符合性

谢 谢！