信息安全管理体系的研究与建立

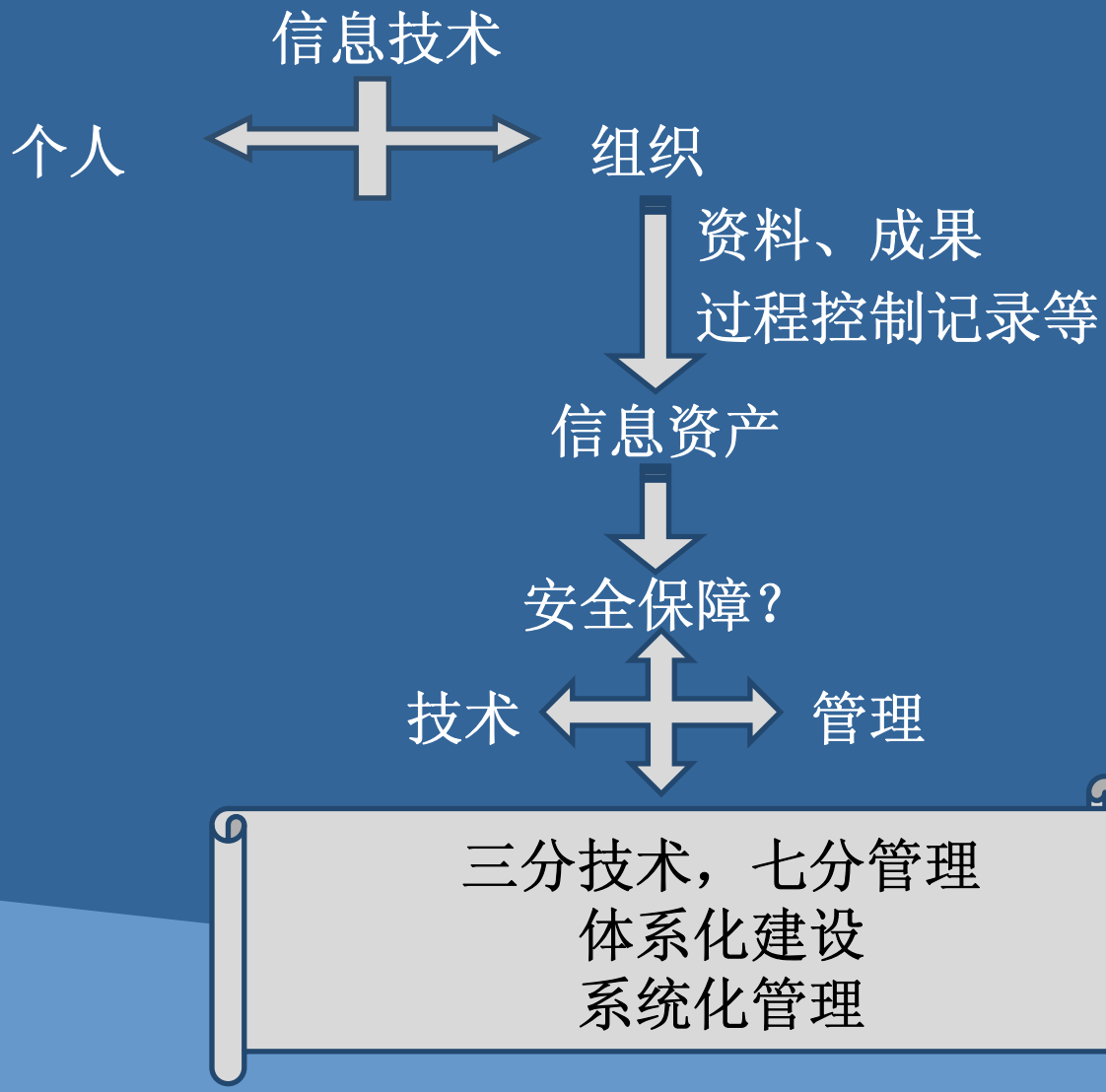
杨东娴

中国社会科学院计算机网络中心

主要内容

- 研究背景
- 体系设计
- 体系构建

信息安全与信息安全管理



信息安全管理现状

- 国际
  - 安全问题的思考切入点改变
  - 管理和技术脱节问题的认识
  - 信息安全管理重点的转移
- 国内
  - 管理：强化主管部门的管理力度
  - 技术：科研支持+技术产业化+学术交流
  - 法规制度

信息安全管理现状（续）

- 院内
  - 组织机构
  - 职责分工
  - 规章制度：入网管理、内容审核
  - 管理机制：全生命周期介入

需解决的问题

- 制度未完备
- 执行力度需增强
- 内部管理工作需加强
- 风险管理机制需建立
- 整体的信息安全防范意识需提高
- 全员参与意识与安全文化需建立

主要内容

- 研究背景
- 体系设计
- 体系构建

构建目标

- 摸清家底，全面掌握情况
- 建立常态化工作机制，持续改进
- 提高信息安全管理水平，保证适度安全

构建原则

- 先试点后推广
- 可行、适用、合规、有效
- 以业务为导向，以等级保护为判断点
- 以信息系统为核心，以资产为操作对象

构建依据

- 现行标准
  - 国际标准
  - 国内标准
- 管理循环模型
  - PDCA循环模型

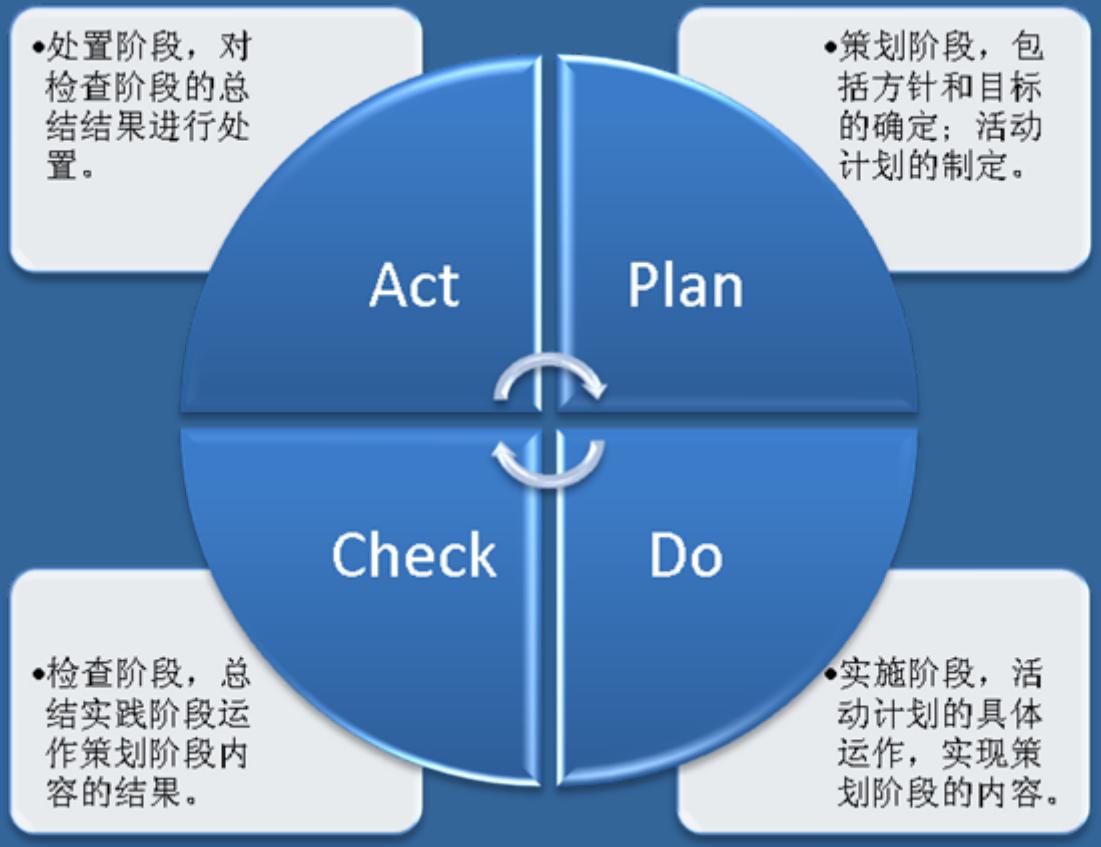
构建依据（续）

ISO/IEC27000	Information technology-Security techniques-Information security management systems-Overview and vocabulary （信息技术——安全技术——信息安全管理体系——概况与术语）
ISO/IEC 27001	Information technology-Security techniques-Information security management systems-Requirements （信息技术——安全技术——信息安全管理体系——要求）
ISO/IEC 27002	Information technology-Security techniques-Code of practice for information security management （信息技术——安全技术——信息安全管理实践规则）
ISO/IEC 27003	Information technology-Security techniques-Information security management systems implementation guidance （信息技术——安全技术——信息安全管理体系实施指南）
ISO/IEC 27004	Information technology-Security techniques-Information security management - Measurements （信息技术——安全技术——信息安全管理——度量）
ISO/IEC 27005	Information technology-Security techniques-Information security risk management （信息技术——安全技术——信息安全风险管理）

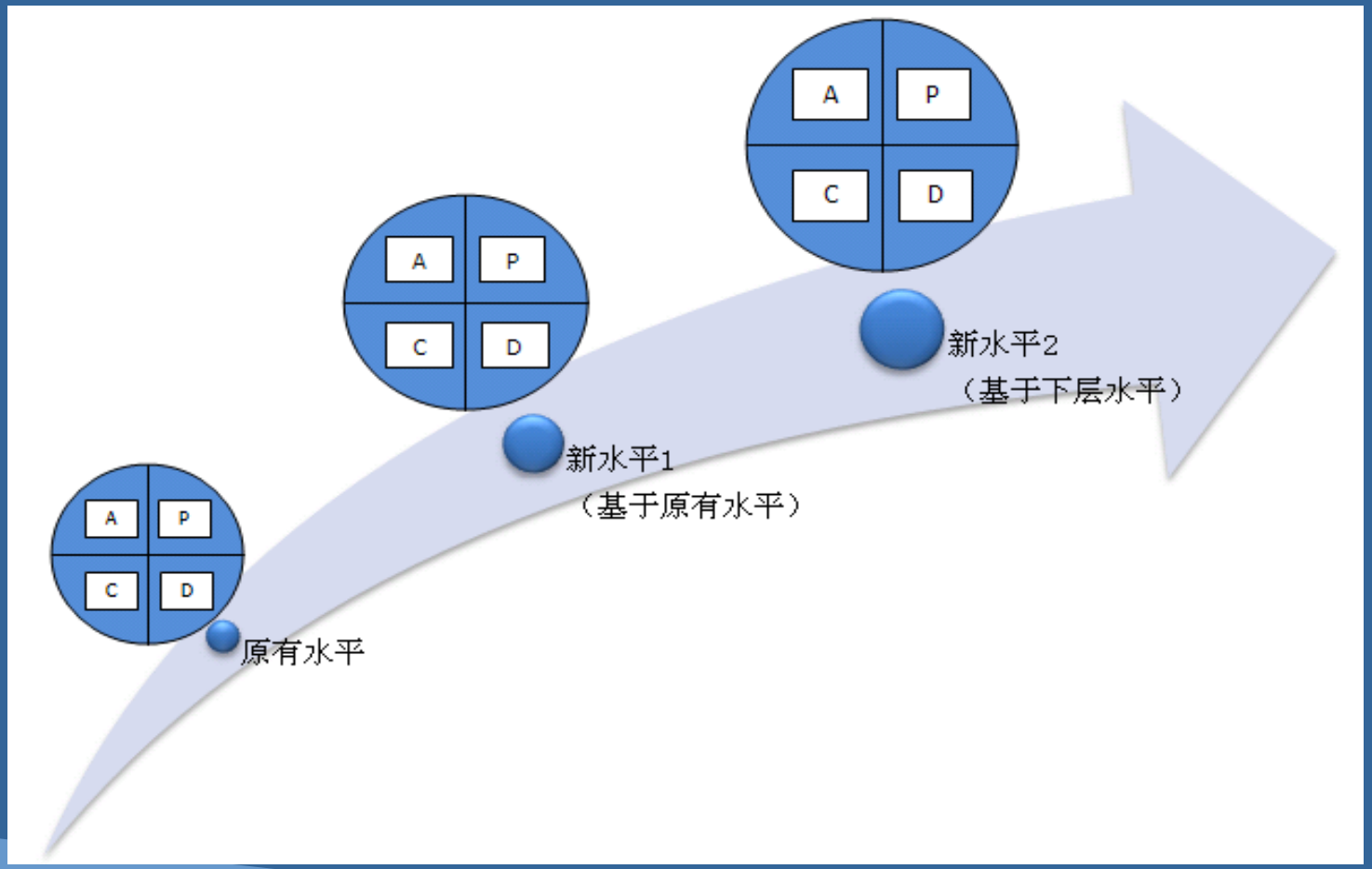
构建依据（续）

信息安全管理	GB/T 22080-2008	信息技术 安全技术 信息安全管理体系 要求 （为国际标准ISO/IEC 27001的等同转化）
	GB/T 22081-2008	信息技术 安全技术 信息安全管理使用规则 （为国际标准ISO/IEC 27002的等同转化）
等级保护	GB 17859-1999	计算机信息系统安全保护等级划分准则
	GB/T 22239-2008	信息安全技术 信息系统安全等级保护基本要求
	GB/T 22240-2008	信息安全技术 信息系统安全保护等级定级指南
	GB/T 24856-2009	信息安全技术 信息系统等级保护安全技术设计要求
应急响应	GB/T 20985-2007	信息技术 安全技术 信息安全事件管理指南
	GB/T 20986-2007	信息安全技术 信息安全事件分类分级
	GB/T 20988-2007	信息安全技术 信息系统灾难恢复规范
	GB/T 24363-2009	信息安全技术 信息安全应急响应计划规范
信息安全风险管理	GB/T 24364-2009	信息安全技术 信息安全风险管理指南
	GB/T 20984-2007	信息安全技术 信息安全风险评估规范

构建依据（续）


•处置阶段，对检查阶段的总结结果进行处置。
•策划阶段，包括方针和目标的确定；活动计划的制定。
Act
Plan
Check
Do
•检查阶段，总结实践阶段运作策划阶段内容的结果。
•实施阶段，活动计划的具体运作，实现策划阶段的内容。

构建依据（续）



安全域设计

<table>
<tr><td colspan="6">信息安全方针
(Information Security Poligy)</td></tr>
<tr><td colspan="6">信息安全组织
(Organization of Information Security)</td></tr>
<tr><td colspan="6">资产管理
(Asset Management)</td></tr>
<tr><td colspan="6">信息安全教育和培训
(Information Security Education and Training)</td></tr>
<tr><td>服务外包安全
(External Parties Security)</td><td>人力资源安全
(Human Resource Security)</td><td>物理和环境安全
(Physical and Environmental Security)</td><td>通讯和操作安全
(Communications and Operations Management)</td><td colspan="2" rowspan="2">信息系统获取开发和维护
(Information Systems Acquisition、Development and Maintenance)</td></tr>
<tr><td colspan="4">访问控制
(Acess Control)</td></tr>
<tr><td colspan="6">检查/监督/审计
(Review、Monitoring、Audit)</td></tr>
<tr><td colspan="6">信息安全事件管理
(Information Securty Incident Management)</td></tr>
<tr><td colspan="6">业务连续性管理
(Business Continuity Management)</td></tr>
<tr><td colspan="6">符合性
(Compliance)</td></tr>
</table>

主要内容

- 研究背景
- 体系设计
- 体系构建

前期准备阶段

- 目的
  - 项目前期的准备工作
- 主要工作
  - 成立ISMS建设项目组，明确责任人。
  - 确定ISMS项目的项目范围，明确实施对象。
  - 召开项目启动会并进行前期培训。
  - 确定ISMS项目的总体实施方案。

运行分析阶段

- 目的
  - 了解情况
  - 确定试点的构建范围和边界
- 主要工作
  - 明确工作范围。
  - 收集信息：组织愿景+文档+组织架构+环境+业务流程+资产明细。
  - 初步确定信息系统的处置优先级。

现场调研阶段

- 目的
  - 获取需求
  - 差距分析
- 主要工作
  - 现场调研。
  - 确定信息系统的等级保护级别。
  - 收集各类与信息系统相关的管理资料。
  - 现状分析和差距分析。

风险评估阶段

- 目的
  - 风险的识别、处置和管理
- 主要工作
  - 确定风险评估方法和工作计划。
  - 识别和评价威胁和脆弱性。
  - 识别和评价现有控制措施的有效性。
  - 分析风险的大小。
  - 进行风险处置。

体系编制阶段

- 目的
  - 建立完整的体系文件
- 主要工作
  - 编制ISMS体系文件。
  - 编制适用性声明（SOA）。

试运行阶段

- 目的
  - 检验ISMS的全面性、适用性和有效性
  - 适度调整，提高ISMS的契合度

谢谢

请指正