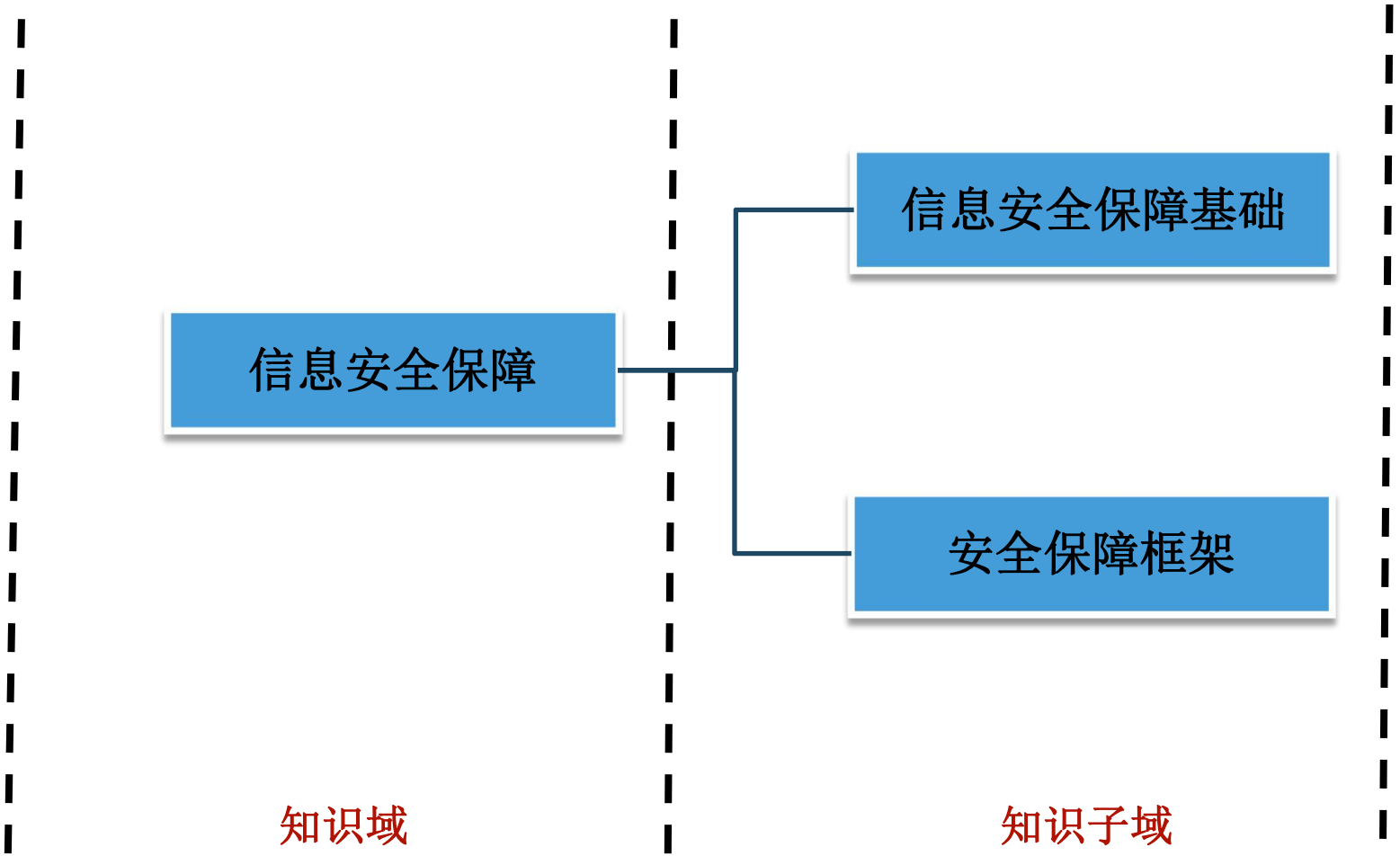
CISP-DSG 信息安全保障

版本：1.0

讲师姓名　　机构名称

课程内容



知识子域：信息安全保障基础

- 信息安全概念
  - 了解信息安全的定义及信息安全问题侠义、广义两层概念与区别；；
  - 理解信息安全问题的根源（内因和外因）；
  - 理解信息安全的系统性、动态性、无边界、非传统等特征；
  - 了解威胁情报、态势感知的基本概念及对信息安全的作用。

信息安全的定义

- ISO对信息安全的定义
  - “为数据处理系统建立和采取技术、管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而受到破坏、更改、泄露”
- 其他相关定义
  - 美国法典中的定义
  - 欧盟的定义

信息安全问题

- 狭义的信息安全概念
  - 狭建立在以IT技术为主的安全范畴
- 广义的信息安全问题
  - 一个跨学科领域的安全问题
  - 安全的根本目的是保证组织业务可持续性运行
  - 信息安全应该建立在整个生命周期中所关联的人、事、物的基础上，综合考虑人、技术、管理和过程控制，使得信息安全不是一个局部而是一个整体
  - 安全要考虑成本因素
  - 信息系统不仅仅是业务的支撑，而是业务的命脉

信息安全问题的根源及特征

- 信息安全问题的根源
  - 内因：信息系统复杂性导致漏洞的存在不可避免
  - 外因：环境因素、人为因素
- 信息安全的特征
  - 系统性
  - 动态性
  - 无边界
  - 非传统

威胁情报与态势感知

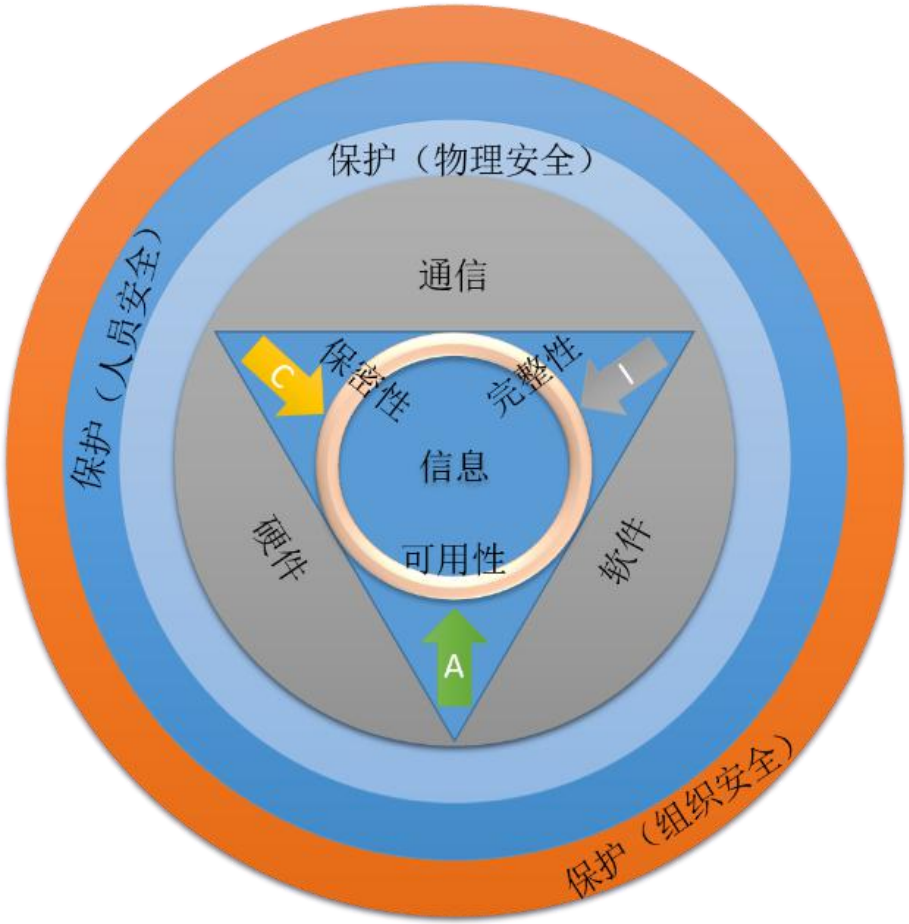
- 威胁情报
  - 为管理人员提供行动和制定决策的依据
  - 建立在大量的数据搜集和处理的基础上，通过对搜集数据的分析和评估，从而形成相应的结论
  - 威胁情报成为信息安全保障中的关键性能力
- 态势感知
  - 建立在威胁情报的基础上
  - 利用大数据和高性能计算为支撑，综合网络威胁相关的形式化及非形式化数据进行分析，并形成对未来网络威胁状态进行预判以便调整安全策略

知识子域：信息安全保障基础

- 信息安全属性
  - 理解信息安全属性的概念及CIA三元组（保密性、完整性、可用性）；
  - 了解真实性、不可否认性、可问责性、可靠性等其他不可缺少的信息安全属性。
- 信息安全视角
  - 了解国家视角对信息安全的关注点（网络战、关键基础设施保护、法律建设与标准化）及相关概念；
  - 了解企业视角对信息安全的关注点（业务连续性管理、资产保护、合规性）及相关概念；
  - 了解个人视角对信息安全的关注点（隐私保护、个人资产保护、社会工程学）及相关概念。

信息安全属性

- 基本属性
  - 保密性
  - 完整性
  - 可用性
- 其他属性
  - 真实性
  - 可问责性
  - 不可否认性
  - 可靠性



国家视角

- 网络战
  - “一个民族国家为了造成损害或破坏而渗透另一个国家的计算机或网络的行动”
  - 网络战其作为国家整体军事战略的一个组成部分已经成为趋势

国家视角

- 国家关键基础设施保护
  - 2016年11月通过的《网络安全法》第三章第二节第三十一条定义了我国关键基础设施，“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的基础设施”为关键基础设施。

国家视角

- 法律建设与标准化
  - 由互联网的开放、自由和共有的脆弱性，使国家安全、社会公共利益以及个人权利在网络活动中面临着来自各方面的威胁，国家需要在技术允许的范围内保持适当的安全要求。
  - 所谓适度安全是指安全保护的立法的范围要和应用的重要性相一致，不要花费过多的成本，限制信息系统的可用性。
  - 信息安全风险具有“不可逆”的特点，需要信息安全法律采取以预防为主的法律原则。但是由于信息安全威胁的全局性特点，其法律原则更应当采取积极主动的预防原则。

企业视角

- 业务连续性
  - 业务数据对组织的重要性使得组织必须关注业务连续性
- 资产保护
  - 有什么
  - 用来做什么
  - 需要保护他们吗
- 合规性
  - 法律法规的合规
  - 标准的合规性

个人视角

- 从个人角度而言，这不仅仅是一个技术问题，还是一个社会问题、法律问题以及道德问题。
  - 隐私保护
  - 社会工程学
  - 个人资产安全
- 个人信息资产问题思考
  - 哪些信息资产被恶意利用后会形成人身的损害？
  - 哪些信息资产被恶意利用后会形成财务的损失？
  - 哪些信息资产被恶意利用后会形成法律责任？

知识子域：信息安全保障基础

- 信息安全发展阶段
  - 了解通信安全阶段的核心安全需求、主要技术措施；
  - 了解计算机安全阶段信息安全需求、主要技术措施及阶段的标志；
  - 了解信息系统安全阶段的安全需求、主要技术措施及阶段的标志；
  - 了解信息安全保障阶段与系统安全阶段的区别，信息安全保障的概念及我国信息安全保障工作的总体要求、主要原则；
  - 了解网络空间的概念，理解网络空间安全对国家安全的重要性。

通信安全

- 20世纪，40年代-70年代
- 主要关注传输过程中的数据保护
- 安全威胁：搭线窃听、密码学分析
- 核心思想：通过密码技术解决通信保密，保证数据的保密性和完整性
- 安全措施：加密

影响现代通信安全因素越来越多，针对移动通信的伪基站、对通信链路的破坏、干扰等因素

计算机安全

- 20世纪，70-90年代
- 主要关注于数据处理和存储时的数据保护
- 安全威胁：非法访问、恶意代码、脆弱口令等
- 核心思想：预防、检测和减小计算机系统（包括软件和硬件）用户（授权和未授权用户）执行的未授权活动所造成的后果。
- 安全措施：通过操作系统的访问控制技术来防止非授权用户的访问

信息系统安全

- 20世纪，90年代后
- 主要关注信息系统整体安全
- 安全威胁：网络入侵、病毒破坏、信息对抗等
- 核心思想：重点在于保护比“数据”更精炼的“信息”
- 安全措施：防火墙、防病毒、漏洞扫描、入侵检测、PKI、VPN等

把信息系统安全从技术扩展到管理，从静态扩展到动态，通过技术、管理、工程等措施的综合融合至信息化中，形成对信息、信息系统乃至业务使命的保障

信息安全保障

- 1996年，DoDD 5-3600.1首次提出了信息安全保障
- 关注信息、信息系统对组织业务及使命的保障
- 信息安全概念延伸，实现全面安全
- 我国信息安全保障工作
  - 总体要求：积极防御，综合防范
  - 主要原则：技术与管理并重，正确处理安全与发展的关系

网络空间安全

- 互联网已经将传统的虚拟世界与物理世界相互连接，形成网络空间
- 新技术领域融合带来新的安全风险
  - 工业控制系统
  - “云大移物智”
- 核心思想：强调“威慑”概念

将防御、威慑和利用结合成三位一体的网络空间安全保障

知识子域：信息安全保障基础

- 信息安全保障新领域
  - 了解工业控制系统中SCADA、DCS、PLC等基本概念，理解工业控制系统的重要性，面临的安全威胁及安全防护的基本思路；
  - 了解云计算所面临的安全风险及云计算安全框架；了解虚拟化安全的基本概念；
  - 了解物联网基本概念、技术架构及相应的安全问题；
  - 了解大数据的概念，大数据应用及大数据平台安全的基本概念；
  - 了解移动互联网面临的安全问题及安全策略；
  - 了解智慧的世界的概念。

工业控制系统基本架构

- 工业控制系统基本结构
  - 分布式控制系统（DCS）
  - 数据采集与监控系统（SCADA）
  - 可编程逻辑控制器（PLC）
- 工业控制系统体系结构

工业控制系统安全威胁

- 缺乏足够安全防护
- 安全可控性不高
- 缺乏安全管理标准和技术

由于TCP/IP协议和以太网的在工业控制系统中逐步扩大应用范围，工业控制系统的结构与一般信息系统逐渐趋同，安全问题也越发严峻

工业控制系统安全架构

- 管理控制
  - 一是风险评价，二是规划，三是系统和服务采购，四是认证、认可和安全评价
- 操作控制
  - 人员安全、物理和环境保护、意外防范计划、配置管理、维护、系统和信息完整性、媒体保护、事件响应、意识和培训
- 技术控制
  - 识别和认证、访问控制、审计和追责、系统和通信保护

云计算的安全风险

- 数据管理和访问失控的风险
  - 数据存储位置对用户失控
  - 云计算服务商对数据权限高于用户
  - 用户不能有效监管云计算厂商内部人员对数据的非授权访问
- 数据管理责任风险
  - 不适用“谁主管谁负责 谁运营谁负责”
- 数据保护的风险
  - 缺乏统一标准，数据存储格式不同
  - 存储介质由云服务商控制，用户对数据的操作需要通过云服务商执行，用户无法有效掌控自己数据

云计算安全架构

- 云计算安全是个交叉领域，覆盖物理安全到应用安全
- 云计算安全覆盖角色
  - 云用户、云提供者、云承载者、云审计者和云经纪人
- 云计算安全服务体系三层架构
  - 安全云基础设施
  - 云安全基础服务
  - 云安全应用服务

虚拟化安全

- 虚拟化是云计算的支撑技术，把硬件资源虚拟化，构成一个资源词从而提供云服务的各项特性
- 虚拟化安全
  - 云计算中核心的安全问题
  - 确保虚拟化多租户之间的有效隔离

物联网基本概念

- 什么是物联网
  - “信息社会的基础设施”
  - 物联网的核心和基础仍然是互联网
  - 其用户端延伸和扩展到了任何物品与物品之间
- 物联网技术架构
  - 感知
  - 传输
  - 支撑
  - 应用

物联网安全威胁及安全架构

- 感知层安全
  - 网关节点被控制，拒绝服务
  - 接入节点标识、识别、认证和控制
- 传输层安全
  - 拒绝服务、欺骗
- 支撑层安全
  - 来自终端的虚假数据识别和处理、可用性保护、人为干预
- 应用层安全
  - 隐私保护、知识产权保护、取证、数据销毁

大数据安全

- 大数据的概念
  - 大数据是指传统数据架构无法有效处理的新数据集
- 大数据的价值
  - 趋势分析
- 大数据安全
  - 数据的生命周期安全
  - 技术平台安全

移动互联网安全问题及策略

- 移动互联网安全问题
  - 系统安全问题
  - 移动应用安全问题
  - 个人隐私保护问题
- 安全策略
  - 政策管控
  - 应用分发管控
  - 加强隐私保护要求

知识子域：信息安全保障框架

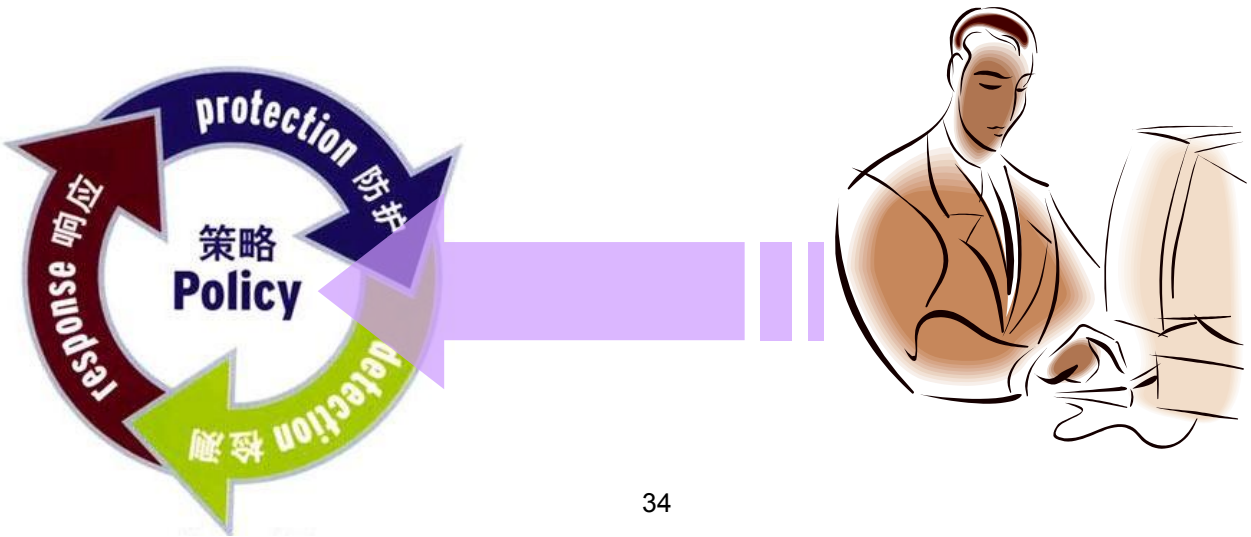
- 基于时间的PDR与PPDR模型
  - 理解基于时间的PDR模型的核心思想及出发点；
  - 理解PPDR模型与PDR模型的本质区别；
  - 了解基于时间判断系统安全性的方式；

基于时间的PDR与PPDR模型

- PDR模型思想
  - 承认漏洞，正视威胁，采取适度防护、加强检测工作、落实响应、建立对威胁的防护来保障系统的安全
- 出发点：基于时间的可证明的安全模型
  - 任何安全防护措施都是基于时间的，超过该时间段，这种防护措施是可能被攻破的
  - 当Pt>Dt+Rt，系统是安全的
- 局限性：Pt、Dt、Rt很难准确定义

基于时间的PDR与PPDR模型

- PPDR模型核心思想
  - 所有的防护、检测、响应都是依据安全策略实施
- 全新定义：及时的检测和响应就是安全
  - 如果Pt ＜ Dt ＋ Rt 那么，Et=（Dt ＋ Rt）－ Pt
- PPDR模型则更强调控制和对抗、考虑了管理的因素，强调安全管理的持续性、安全策略的动态性等



基于时间的PDR与PPDR模型

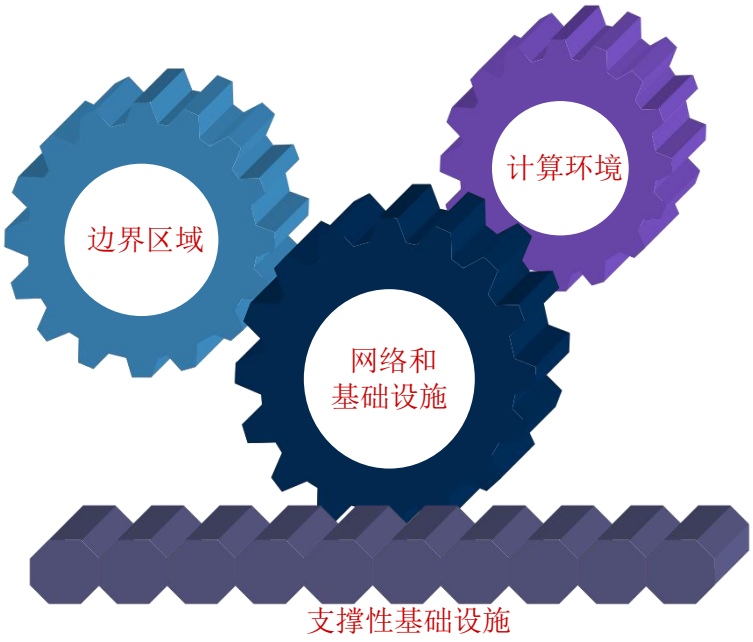
- P2DR模型中的数学法则
  - 假设S系统的防护、检测和反应的时间分别是
    - Pt（防护时间、有效防御攻击的时间）
    - Dt（检测时间、发起攻击到检测到的时间）
    - Rt（反应时间、检测到攻击到处理完成时间）
  - 假设系统被对手成功攻击后的时间为
    - Et（暴露时间）
  - 则该系统防护、检测和反应的时间关系如下：
    - 如果Pt＞Dt＋Rt，那么S是安全的；
    - 如果Pt＜Dt＋Rt，那么Et＝（Dt＋Rt）－Pt。

知识子域：信息安全保障框架

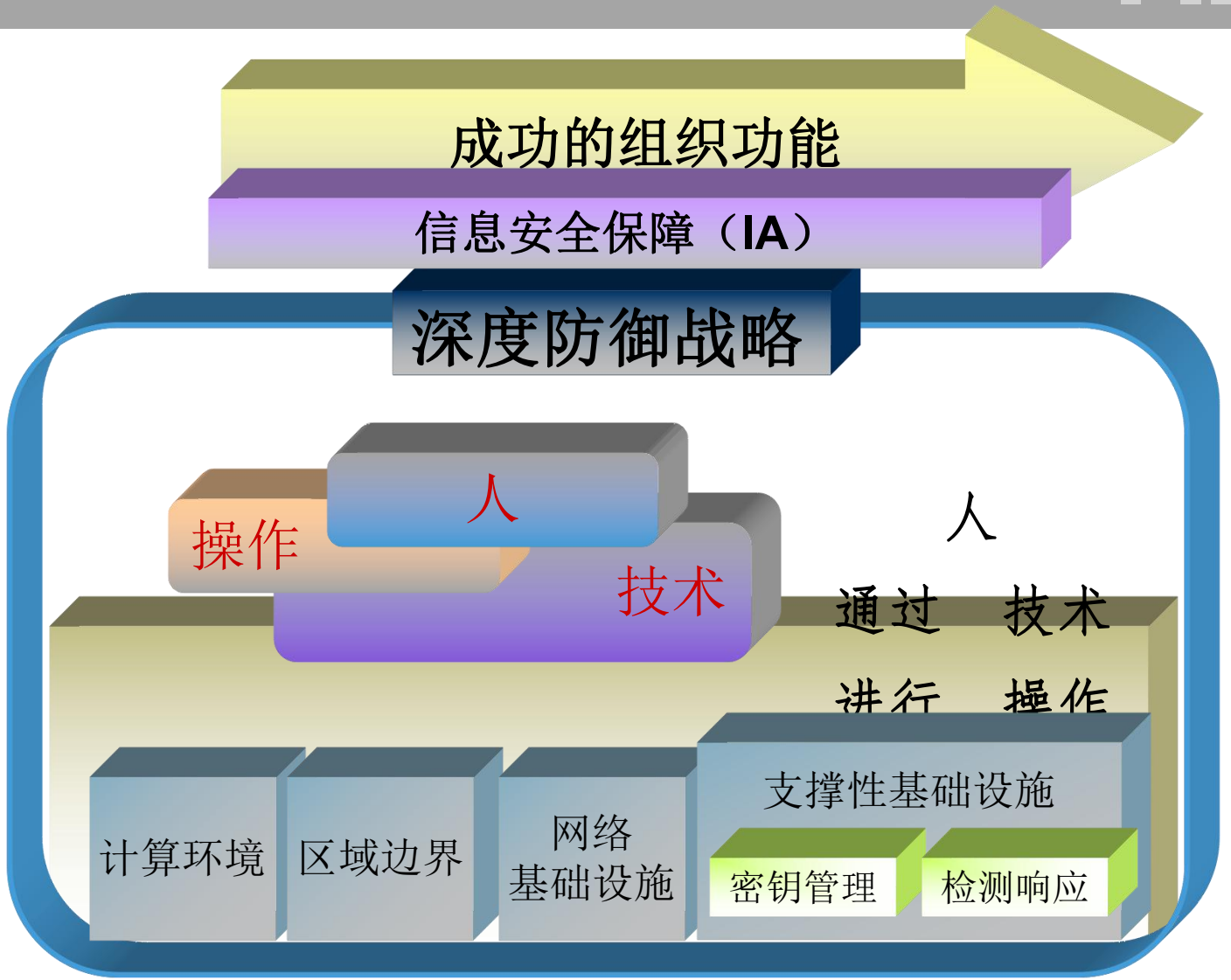
- 信息安全保障技术框架
  - 理解信息安全保障技术框架（IATF）的“深度防御”核心思想、三个核心要素及四个焦点领域；
  - 了解保护区域边界的原则和技术实现方式；
  - 了解保护计算环境的原则和技术实现方式；
  - 了解保护网络基础设施的原则和技术实现方式；
  - 了解支撑性基础设施建设的概念及技术实现；

信息保障技术框架（IATF）

- 信息保障技术框架（IATF）
  - 美国国家安全局（NSA）制定，为保护美国政府和工业界的信息与信息技术设施提供技术指南
- 核心思想：“深度防御”
- 三个要素：人、技术、操作
- 四个焦点领域
  - 保护网络和基础设施
  - 保护区域边界
  - 保护计算环境
  - 支持性基础设施



信息保障技术框架


成功的组织功能
信息安全保障（IA）
深度防御战略
人
操作
技术
人
通过
技术
进行
操作
计算环境
区域边界
网络
基础设施
支撑性基础设施
密钥管理
检测响应

信息保障技术框架-核心要素

- **人（People）：**
  - 信息保障体系的核心，是第一位的要素，同时也是最脆弱的。
  - 基于这样的认识，安全管理在安全保障体系中愈显重要，包括：
    - 意识培训、组织管理、技术管理、操作管理
    - ……
- **技术（Technology）：**
  - 技术是实现信息保障的重要手段。
  - 动态的技术体系：
    - 防护、检测、响应、恢复
- **操作（Operation）：**
  - 也叫运行，构成安全保障的主动防御体系。
  - 是将各方面技术紧密结合在一起的主动的过程，包括
    - 风险评估、安全监控、安全审计
    - 跟踪告警、入侵检测、响应恢复

信息保障技术框架-保护计算环境

- 目标：
  - 使用信息保障技术确保数据在进人、离开或驻留客户机和服务器时具有保密性、完整性和可用性
- 方法：
  - 使用安全的操作系统，
  - 使用安全的应用程序
  - 主机入侵检测
  - 防病毒系统
  - 主机脆弱性扫描
  - 文件完整性保护
  - ……

信息保障技术框架-保护区域边界

- 区域边界：区域的网络设备与其它网络设备的接入点被称为“区域边界”。
- 目标：对进出某区域（物理区域或逻辑区域）的数据流进行有效的控制与监视。
- 方法：
  - 病毒、恶意代码防御
  - 防火墙
  - 人侵检测
  - 远程访问
  - 多级别安全
  - ……

信息保障技术框架–保护网络和基础设施

- 目标：网络和支持它的基础设施必须
  - 防止数据非法泄露
  - 防止受到拒绝服务的攻击
  - 防止受到保护的信息在发送过程中的时延、误传或未发送
- 方法：
  - 骨干网可用性
  - 无线网络安全框架
  - 系统高度互联和虚拟专用网
  - ……

信息保障技术框架-支撑性基础设施

- 目标：为安全保障服务提供一套相互关联的活动与基础设施
- 密钥管理基础设施（KMI）
  - 提供一种通用的联合处理方式，以便安全地创建、分发和管理公钥证书和传统的对称密钥，使它们能够为网络、区域和计算环境提供安全服务
- 检测和响应基础设施
  - 能够迅速检测并响应入侵行为，需要入侵检测与监视软件等技术解决方案以及训练有素的专业人员（通常指计算机应急响应小级（CERT））的支持。

信息保障技术框架-安全原则与特点

- 安全原则
  - 保护多个位置
  - 分层防御
  - 安全强健性
- IATF特点
  - 全方位防御、纵深防御将系统风险降到最低
  - 信息安全不纯粹是技术问题，而是一项复杂的系统工程
  - 提出“人”这一要素的重要性，人即管理

知识子域：信息安全保障框架

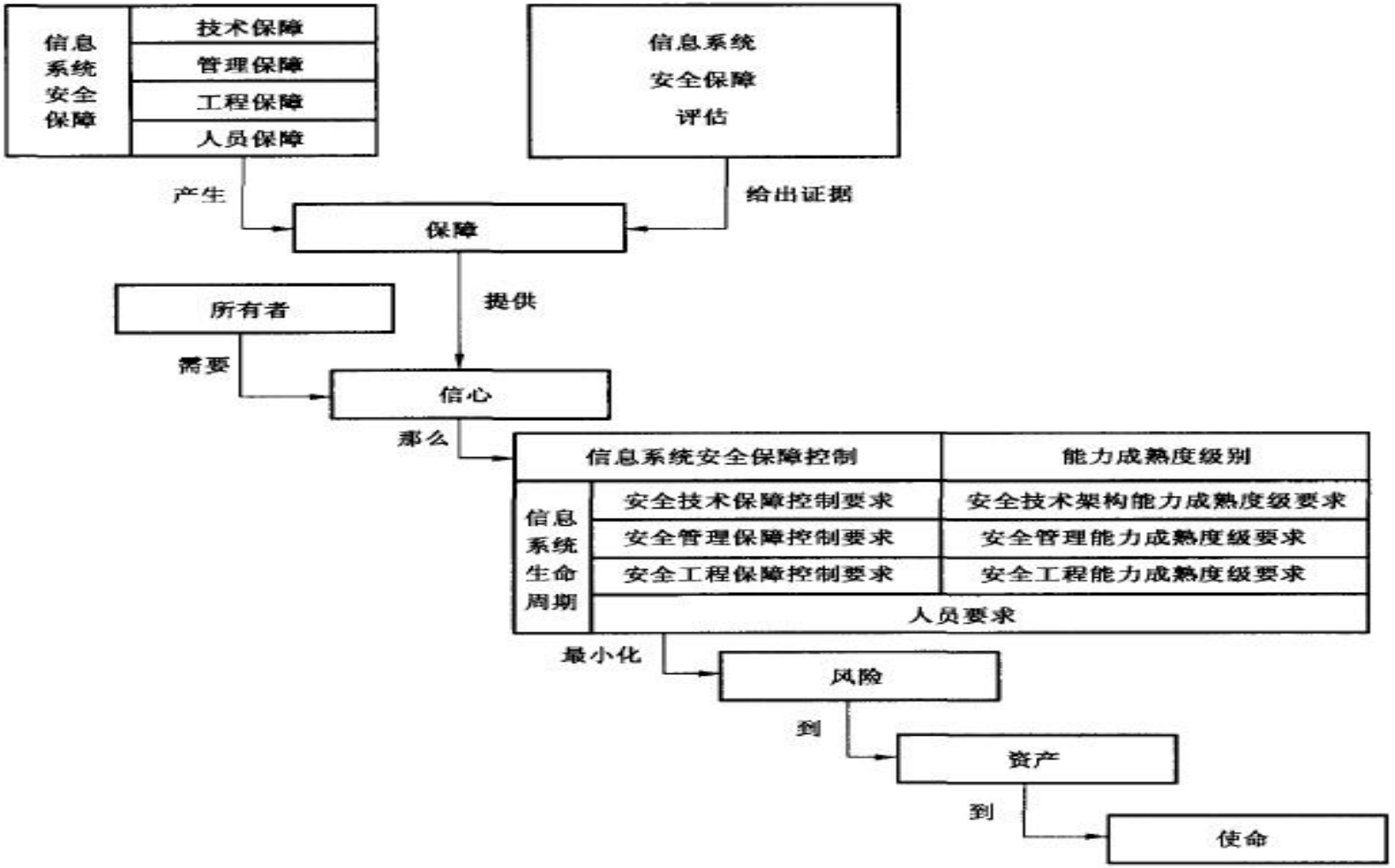
- 信息系统安全保障评估框架
  - 理解信息系统保障相关概念及信息安全保障的核心目标；
  - 了解信息系统保障评估的相关概念和关系；
  - 理解信息系统安全保障评估模型主要特点，生命周期、保障要素等概念。

信息系统安全保障评估框架-基本概念

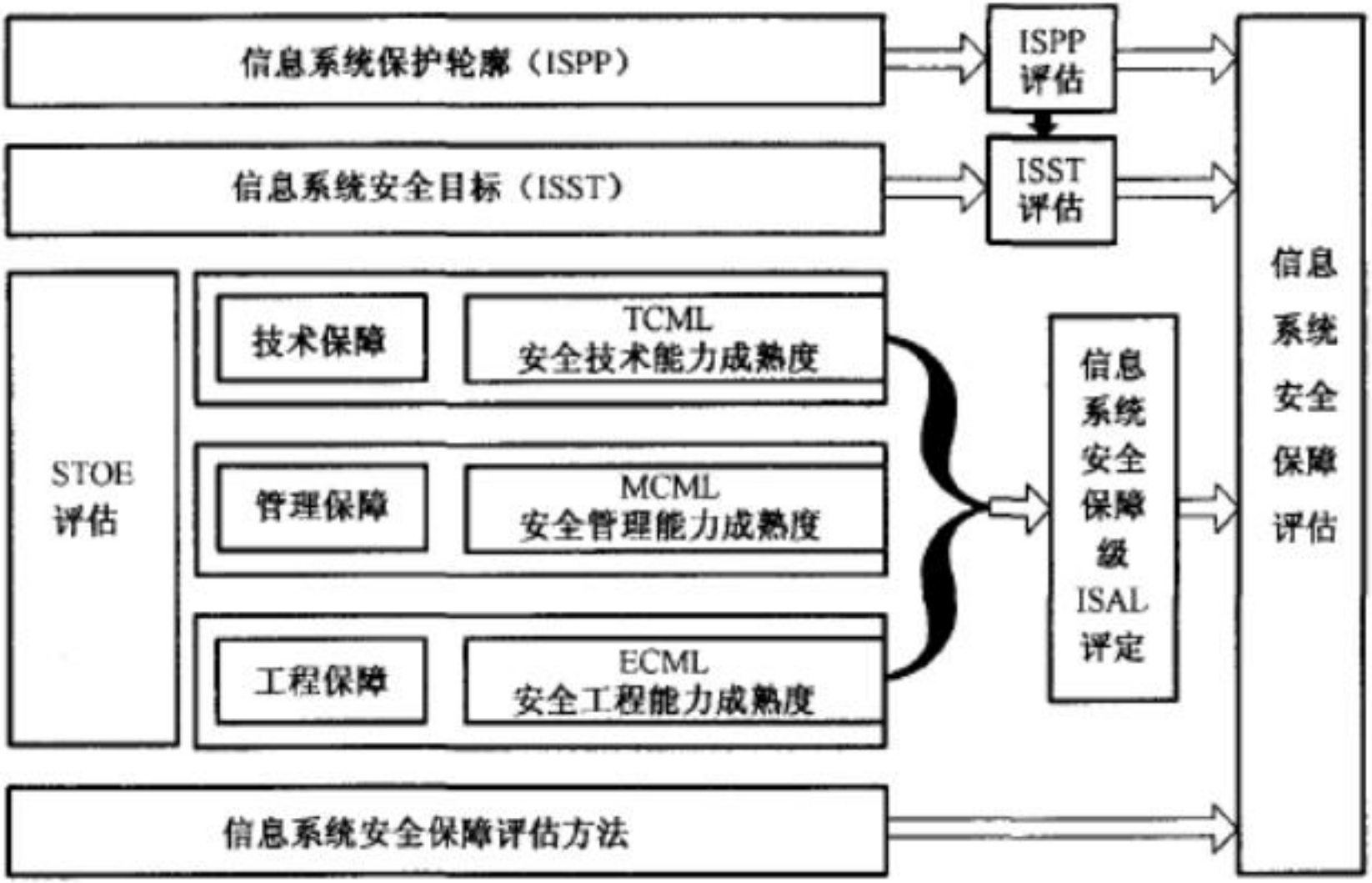
- 信息系统
  - 用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、机构人员和组件的总和。
- 信息系统安全风险
  - 是具体的风险，产生风险的因素主要有信息系统自身存在的漏洞和来自系统外部的威胁。信息系统运行环境存在特定威胁动机的威胁源。
- 信息系统安全保障
  - 在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出信息安全保障要求，确保信息系统的保密性、完整性和可用性，把安全风险到可接受的程度，从而保障系统能够顺利实现组织机构的使命。

信息系统安全保障评估框架-概念和关系

- 信息系统安全保障评估概念和关系



信息系统安全保障评估框架-评估的描述



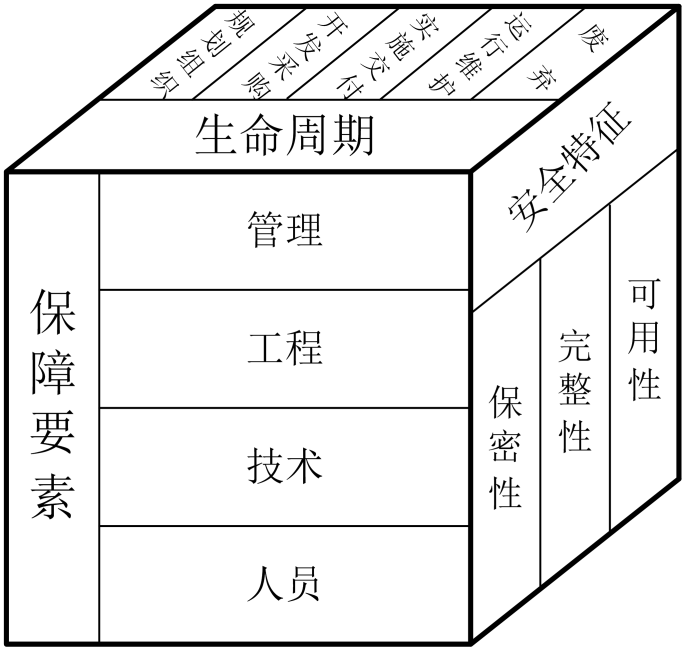
信息系统安全保障评估框架

- 信息系统保护轮廓（ISPP）
  - 根据组织机构使命和所处的运行环境，从组织机构的策略和风险的实际情况出发，对具体信息系统安全保障需求和能力进行具体描述。
  - 表达一类产品或系统的安全目的和要求。
  - ISPP是从信息系统的所有者（用户）的角度规范化、结构化的描述信息系统安全保障需求。
- 信息系统安全目标（ISST）
  - 根据信息系统保护轮廓（ISPP）编制的信息系统安全保障方案。
  - 某一特定产品或系统的安全需求。
  - ISST从信息系统安全保障的建设方（厂商）的角度制定的信息系统安全保障方案。

信息系统安全保障评估框架-评估模型

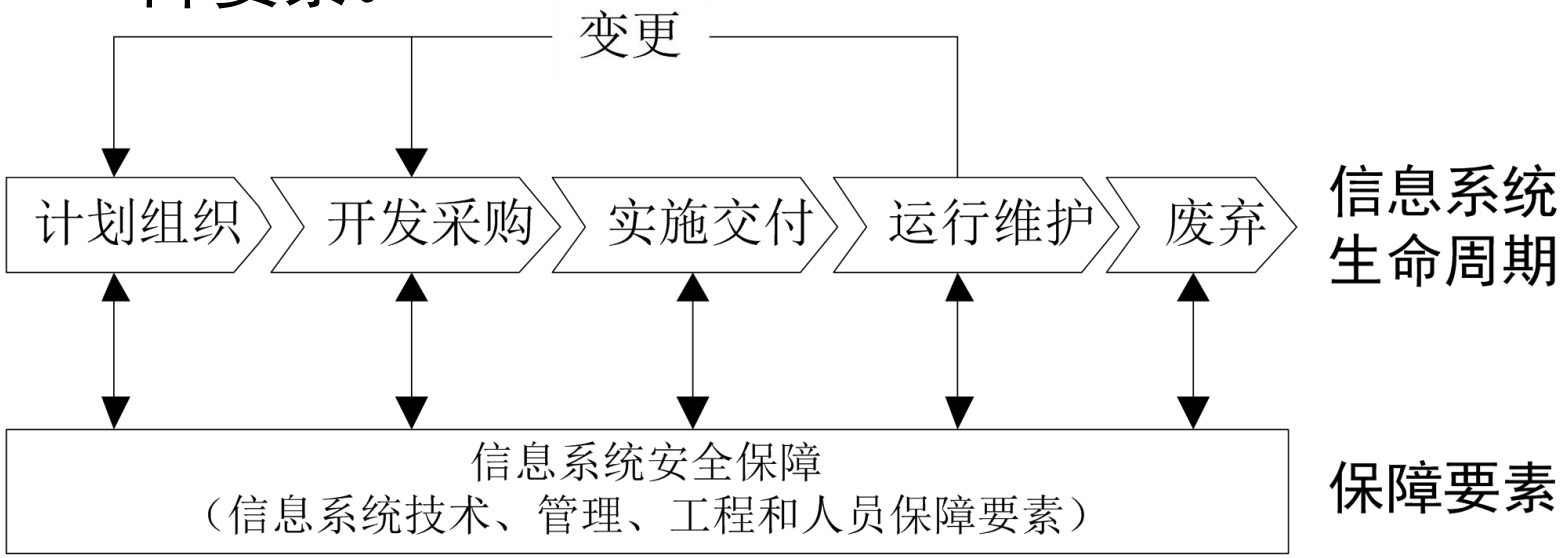
- 模型特点
  - 将风险和策略作为信息系统安全保障的基础和核心
  - 强调安全贯彻信息系统生命周期
  - 强调综合保障的观念

以风险和策略为基础，在整个信息系统的生命周期中实施技术、管理、工程和人员保障要素。通过信息系统安全保障实现信息安全的安全特征：信息的保密性、完整性和可用性特征，从而达到保障组织机构执行其使命的根本目的



信息系统安全保障评估框架

- 基于信息系统生命周期的信息安全保障
  - 信息系统的生命周期层面和保障要素层面不是相互孤立的，而是相互关联、密不可分的。
  - 在信息系统生命周期中的任何时间点上，都需要综合信息系统安全保障的技术、管理、工程和人员保障要素。



信息系统安全保障评估框架

- 信息安全保障要素–信息安全技术
  - 密码技术
  - 访问控制技术
  - 审计和监控技术
  - 网络安全技术
  - 操作系统技术
  - 数据库安全技术
  - 安全漏洞与恶意代码
  - 软件安全开发
- 信息安全保障要素–信息安全管理
  - 信息安全管理体系
  - 风险管理

信息系统安全保障评估框架

- 信息安全保障要素–信息安全工程
  - 信息安全工程涉及系统和应用的开发、集成、操作、管理、维护和进化以及产品的开发、交付和升级。
- 信息安全保障要素–信息安全人才
  - 信息安全保障诸要素中，人是最关键、也是最活跃的要素。网络攻防对抗，最终较量的是攻防两端的人，而不是设备。

信息系统安全保障评估框架

- 信息安全保障解决方案
  - 以风险评估和法规要求得出的安全需求为依据
    - 考虑系统的业务功能和价值
    - 考虑系统风险哪些是必须处置的，哪些是可接受的
  - 贴合实际具有可实施性
    - 可接受的成本
    - 合理的进度
    - 技术可实现性
    - 组织管理和文化的可接受性

知识子域：信息安全保障框架

企业安全架构

- 了解企业安全架构的概念；
- 了解舍伍德商业应用安全架构模型构成及生命周期。

企业安全架构

- 什么是企业安全架构
  - 企业架构的一个子集，它定义了信息安全战略，包括各层级的解决方案、流程和规程，以及它们与整个企业的战略、战术和运营链接的方式。
  - 开发企业安全架构的主要原因是确保安全工作以一个标准化的和节省成本的方式与业务实践相结合。
- 常见企业安全架构
  - 舍伍德的商业应用安全架构（Sherwood Applied Business Security Architecture，SABSA）
  - Zachman框架
  - 开放群组架构框架（The Open Group Architecture Framework，TOGAF）

企业安全架构

- 企业安全架构
  - 企业架构的一个子集
  - 定义了信息安全战略、包括分层级的解决方案、流程和规程
  - 确保安全工作以一个标准化和节省承办的方式与业务实践想结合
- 常见企业安全架构
  - 舍伍德商业应用安全架构（SABSA）
  - Zachman框架
  - 开放群组架构框架（TOGAF）

舍伍德的商业应用安全架构

- 分层的模型，包括六个层级

	资产（什么）	动机（为什么）	过程（如何）	人（谁）	地点（何地）	时间（何时）
背景层	业务	业务风险模型	业务过程模型	业务组织和关系	业务地理布局	业务时间依赖性
概念层	业务属性配置文件	控制目标	安全战略和架构分层	安全实体模型和信任框架	安全域模型	安全有效期和截止时间
逻辑层	业务信息模型	安全策略	安全服务	实体概要和特权配置文件	安全域定义和关系	安全过程循环
物理层	业务数据模型	安全规则、实践和规程	安全机制	用户、应用程序和用户接口	平台和网络基础设施	控制结构执行
组件层	数据结构细节	安全标准	安全产品和工具	标识、功能、行为和访问控制列表（ACL）	过程、节点、地址和协议	安全步骤计时和顺序
运营层	业务连续性保障	运营风险管理	安全服务管理和支持	应用程序和用户管理与支持	站点、网络和平台的安全	安全运营日程表

SABSA模型架构

- 背景层（业务视图）
  - 业务视图说明所有架构必须满足业务要求。了解该系统的业务需求驱动，选择合适的架构。
  - 业务视图被称为背景环境的安全架构。这是安全系统必须设计、建造和经营的业务范围内的描述。
- 概念层（架构视图）
  - 架构是整体的概念，可满足企业的业务需求。也被称为概念性的安全架构。
  - 定义在较低层次的抽象逻辑和物理元素的选择和组织上，确定指导原则和基本概念。
- 逻辑层（设计视图）
  - 设计是架构的具体反映，设计过程通常被称为系统工程，涉及整个系统的架构元素的识别和规范。
  - 逻辑的安全架构应该反映和代表所有概念性的安全架构中的主要安全战略。

SABSA模型架构

- 物理层（建设视图）
  - 设计是产生一套描述了系统的逻辑抽象，这些都需要形成一个物理的安全体系结构模型，该模型应描述实际的技术模式和指定的各种系统组件的详细设计。
  - 如需要描述提供服务的服务器的物理安全机制和逻辑安全服务等。
- 组件层（实施者视图）
  - 这层的模型也被称为组件安全架构。
- 运营层（服务和管理视图）
  - 当建设完成后，需要进行运维管理。
  - 保持各项服务的正常运作，保持良好的工作秩序和监测，以及按要求执行。
  - 也被称为服务管理安全架构。关注的焦点是安全性相关的部分。

总结

- 信息安全保障基础
  - 基本概念
  - 信息安全发展阶段
  - 信息安全保障新领域
- 信息安全保障框架
  - PPDR
  - IATF
  - 信息系统安全保障评估框架
  - 舍伍德的商业应用安全架构

CISP

谢谢，请提问题！