

# 主要内容

---

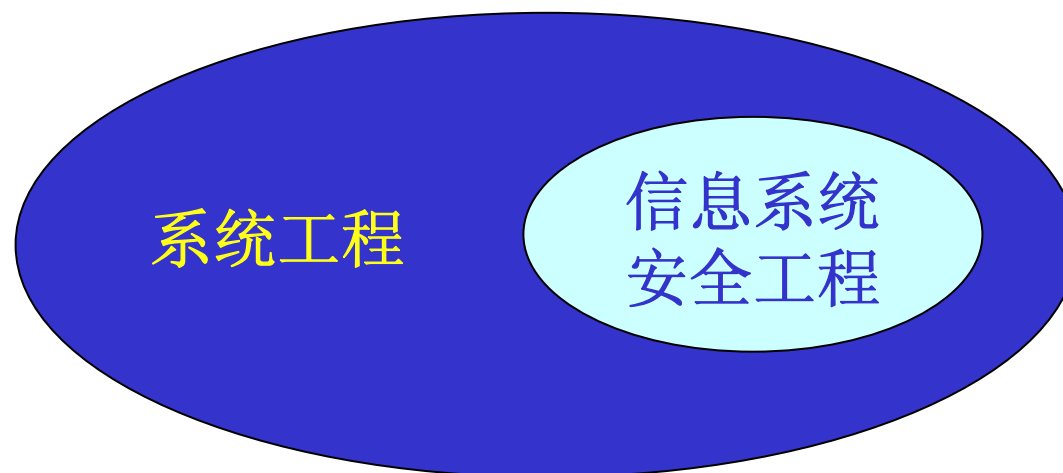
## ■ 系统工程

## ■ 信息系统安全工程 (ISSE)

- 信息系统安全工程 (ISSE) 过程概述
- 信息系统安全工程 (ISSE) 过程
  - 发掘信息保护需求
  - 定义信息保护系统
  - 设计信息保护系统
  - 实施信息保护系统
  - 评估信息保护系统的有效性

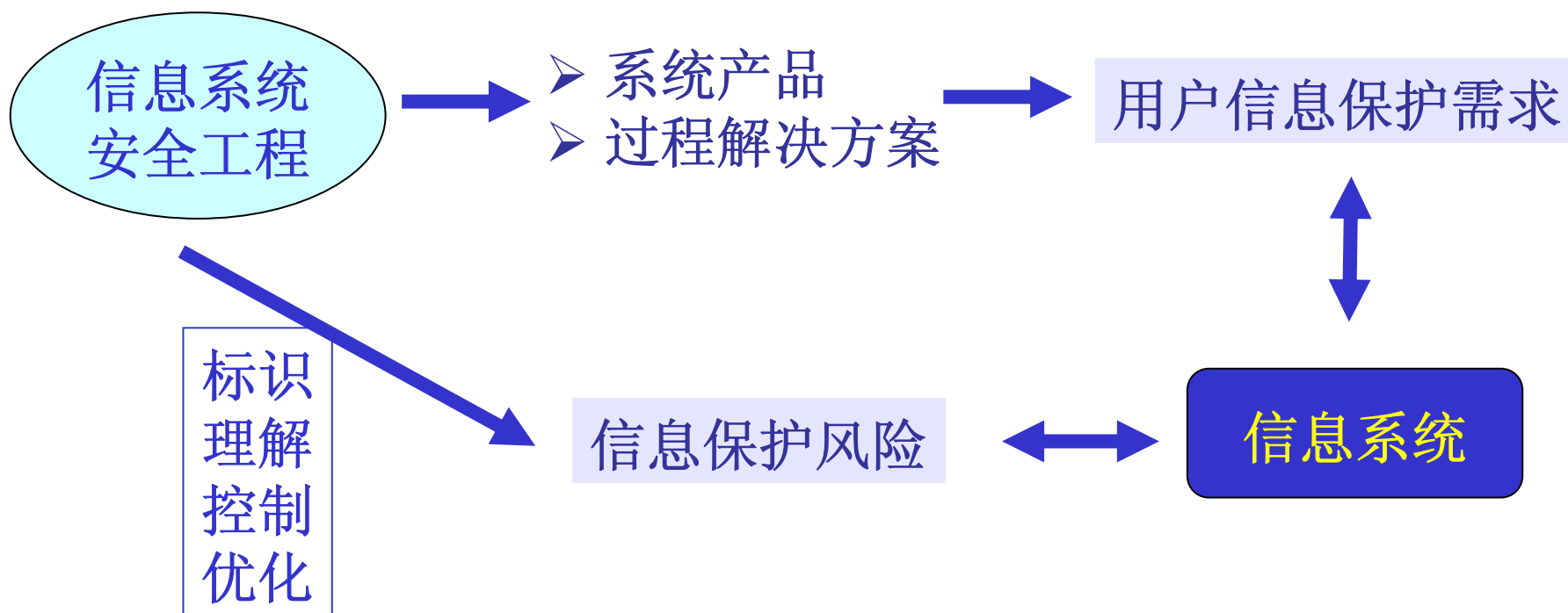
# ISSE 信息系统安全工程

---



通过实施系统工程过程来满足信息保护的需求

# ISSE的作用



# ISSE与SE

---

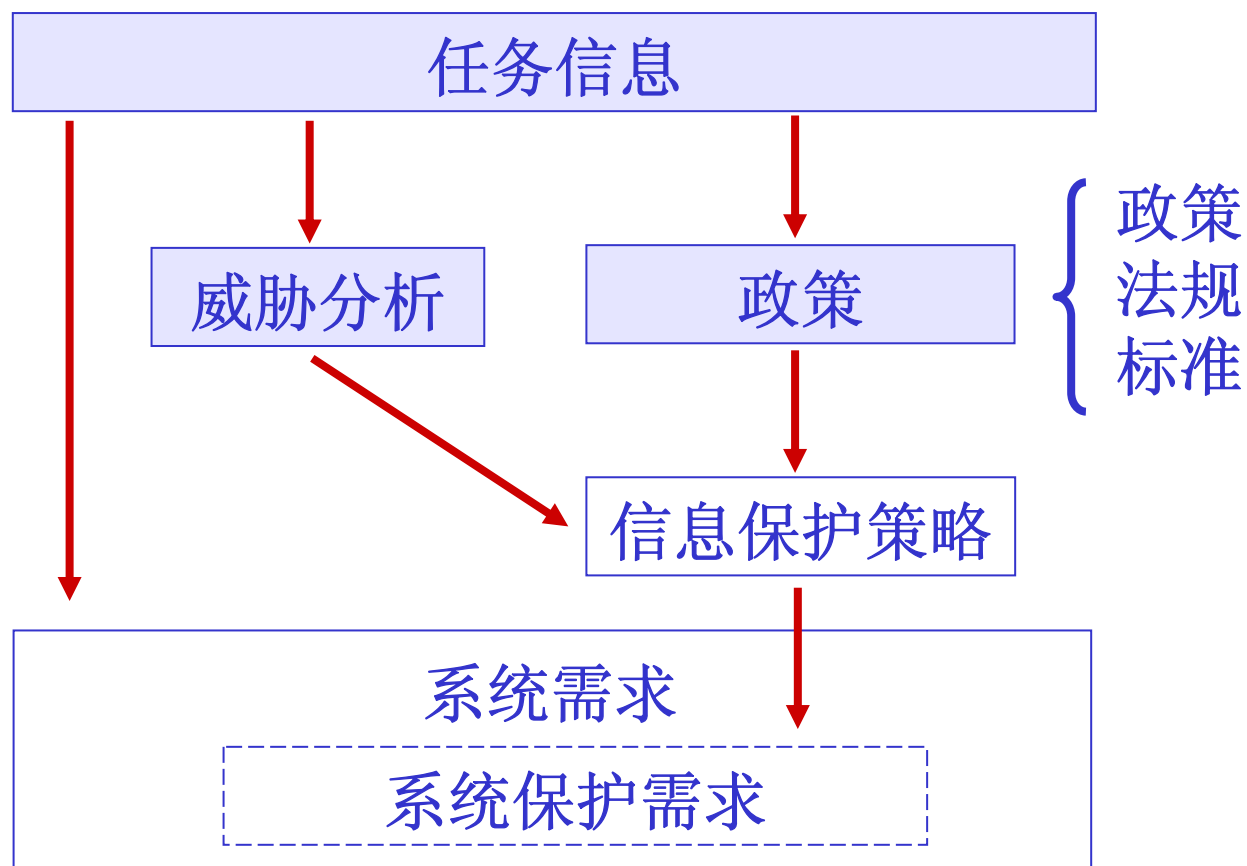
- ISSE过程是SE过程的子过程
- 对系统而言，要同步考虑
  - 即在相应的阶段同时考虑信息保护的目标、需求、功能、体系结构、设计、测试与实施，是信息保护得以优化

# 信息系统安全工程（ISSE）过程

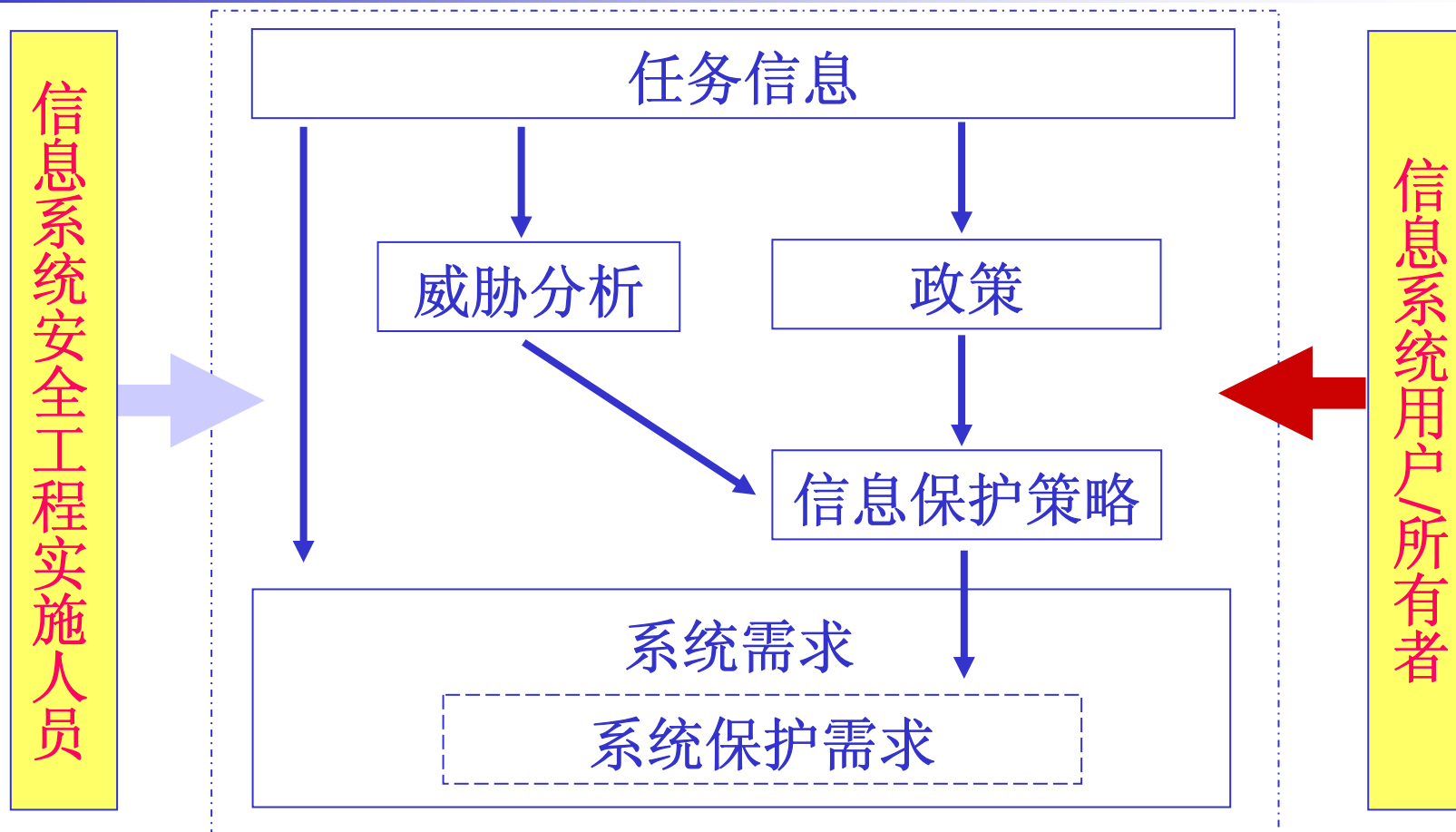
---

- 发掘信息保护需求
- 定义信息保护系统
- 设计信息保护系统
- 实施信息保护系统
- 评估信息保护系统的有效性

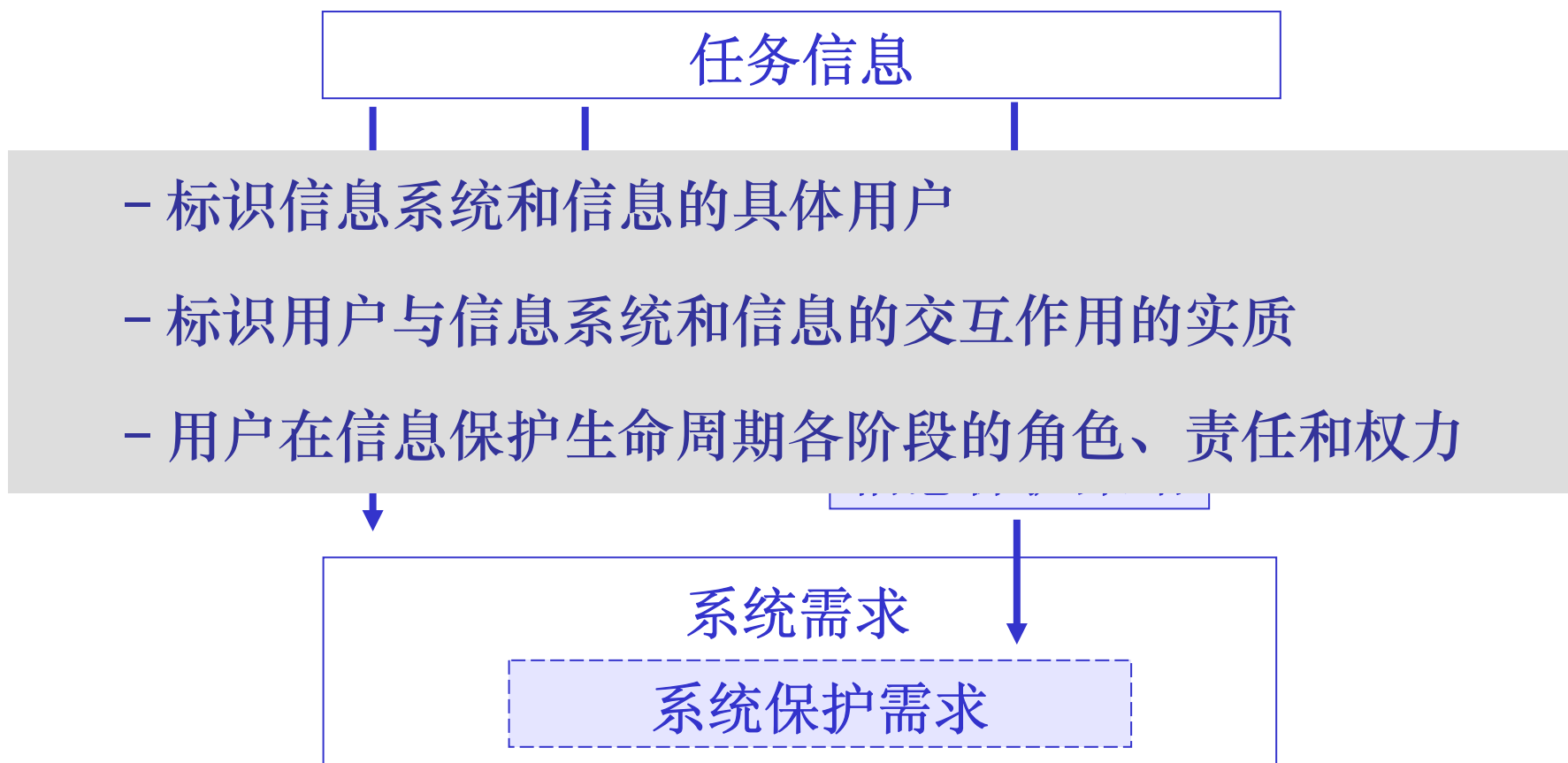
# 发掘信息保护需求过程



# 发掘信息保护需求主体



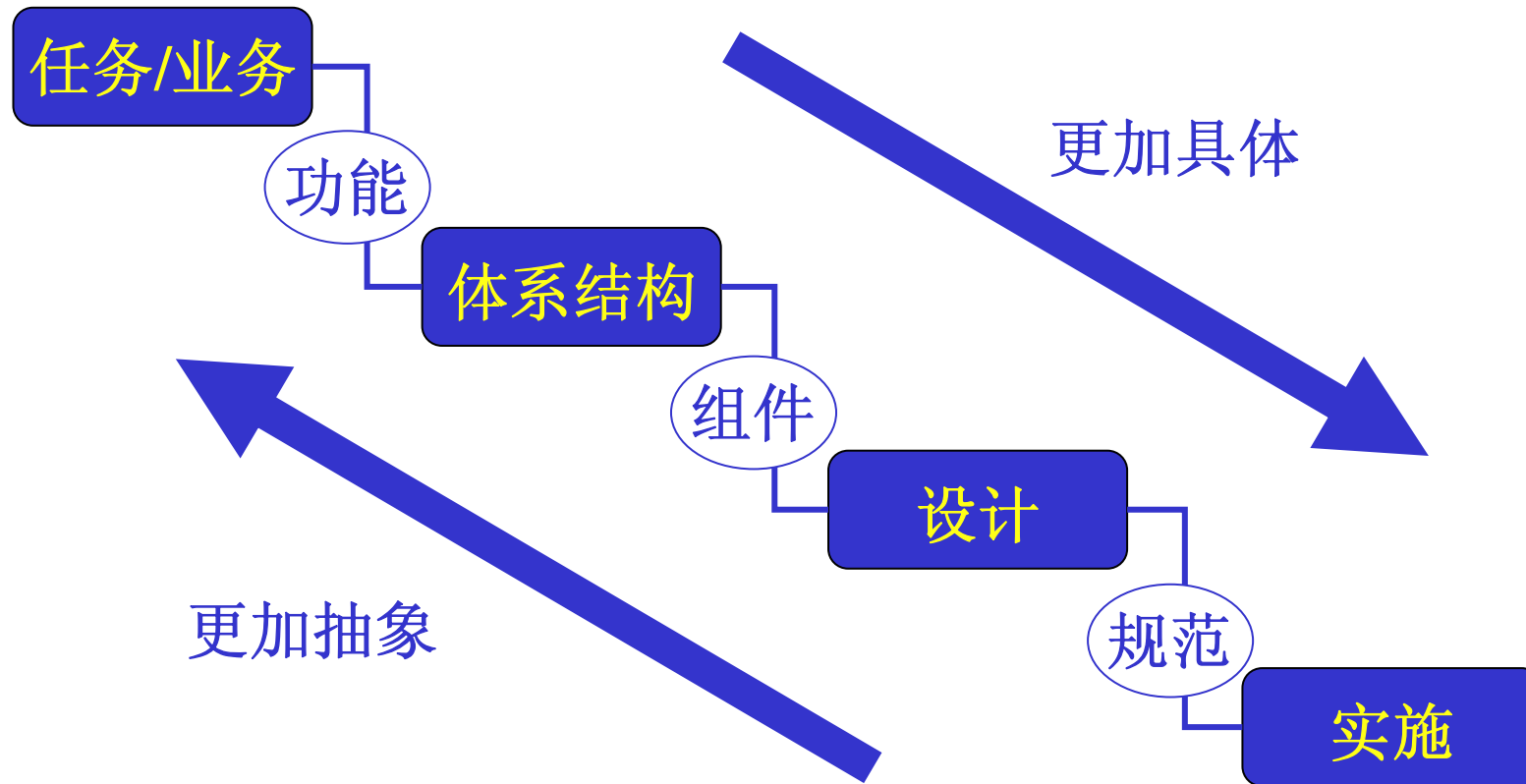
# 任务信息——保护需求



？当无法使用信息系统或信息，尤其是丧失保密性，完整性，可用性，不可否认性时，可能会带来那些问题？



# 分层需求图



# 例

---

## - 信息和信息系统在支持系统任务方面的角色描述

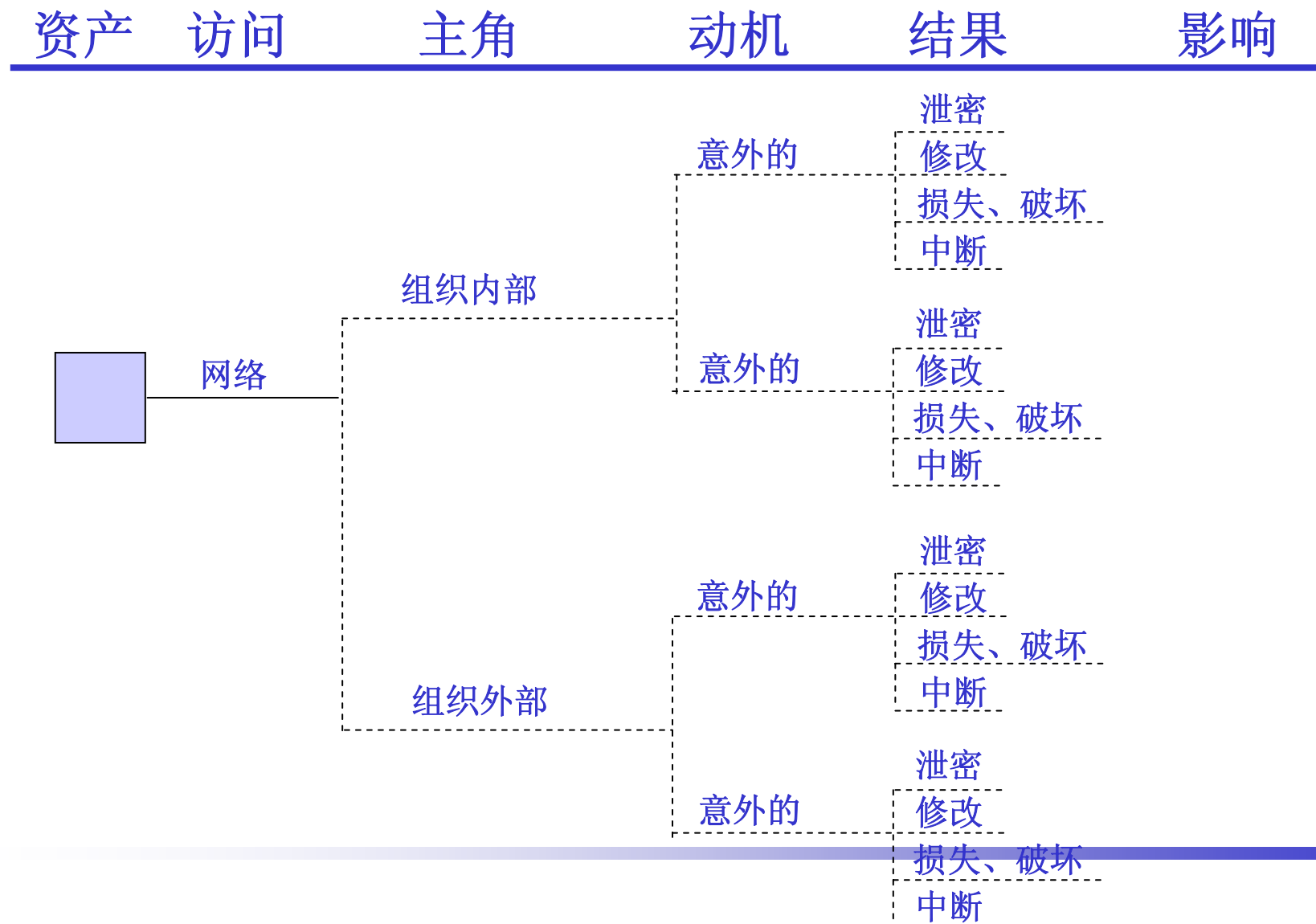
- 需要查阅、更新、删除、初始化或者处理的信息属于何种类型（涉密信息、金融信息、产权信息、个人隐私信息等）？
- 谁有权查阅、更新、删除、初始化和处理信息记录？
- 授权用户如何履行其职责？
- 授权用户使用何种工具（文档、硬件、软件、固件和规程）履行其责任？
- 系统中是否有不可否认性需求？
- .....

# 威胁分析

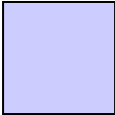
---

- “威胁”是指可能造成某个结果的事件或对系统造成危害的潜在事实
- 系统威胁的描述涉及
  - 信息类型
  - 信息的合法用户及用户的信息
  - 对威胁主体的考察
    - 动机
    - 能力
    - 意图
    - 途径
    - 可能性
    - 后果（对机构人物/业务的影响）

# 威胁分析方法示例：使用网络方式访问的人 (OCTAVE)



# 威胁分析方法示例：系统问题(OCTAVE)

资产	主角	结果	影响
	软件故障	泄密	
		修改	
		损失、破坏	
	恶意代码	中断	
		泄密	
		修改	
	系统崩溃	损失、破坏	
		中断	
		泄密	
	硬件故障	修改	
		损失、破坏	
		中断	
		泄密	
		修改	
		损失、破坏	

# 信息安全策略 -- policy

---

- 策略指：“以正式形式出现的，经**管理层同意和批准**的，规定了组织行为方向和行为自由程度的途径”，或者说策略是管理层对某个主题有关意见的一种陈述形式。
- 信息安全策略是一组**规则**，这组规则描述了一个组织要实现的**信息安全目标**和实现这些信息安全目标的**途径**。
  - 从管理角度看，信息安全策略是组织关于信息安全的文件，**是一个组织关于信息安全的基本指导规则**。它通常由组织最高管理层批准，在整个组织内发布其目标在于减少信息安全事故的发生，将信息安全事故的影响与损失减低到最小

# 信息安全策略提供：

---

- 信息保护的内容和目标
- 信息保护的职责落实
- 实时信息保护的方法
- 事故的处理

# 本阶段的主要活动

---

- 帮助用户对自己的信息管理过程进行建模
- 帮助用户定义信息威胁
- 帮助用户确立信息保护需求的优先次序
- 准备信息保护策略
- 获得用户许可

确保任务需求中包含了信息保护需求，系统功能中包含了信息保护功能，系统中包含信息保护体系结构和机制



# 发掘信息保护需求--子任务

---

- 任务-01.1 分析机构的任务
- 任务-01.2 判断信息对机构任务的关系和重要性
- 任务-01.3 确定法律和法规的要求
- 任务-01.4 确定威胁的类别
- 任务-01.5 判断影响
- 任务-01.6 确定安全服务
- 任务-01.7 记录信息保护需求
- 任务-01.8 记录安全管理角色和责任

# 发掘信息保护需求--子任务（续）

---

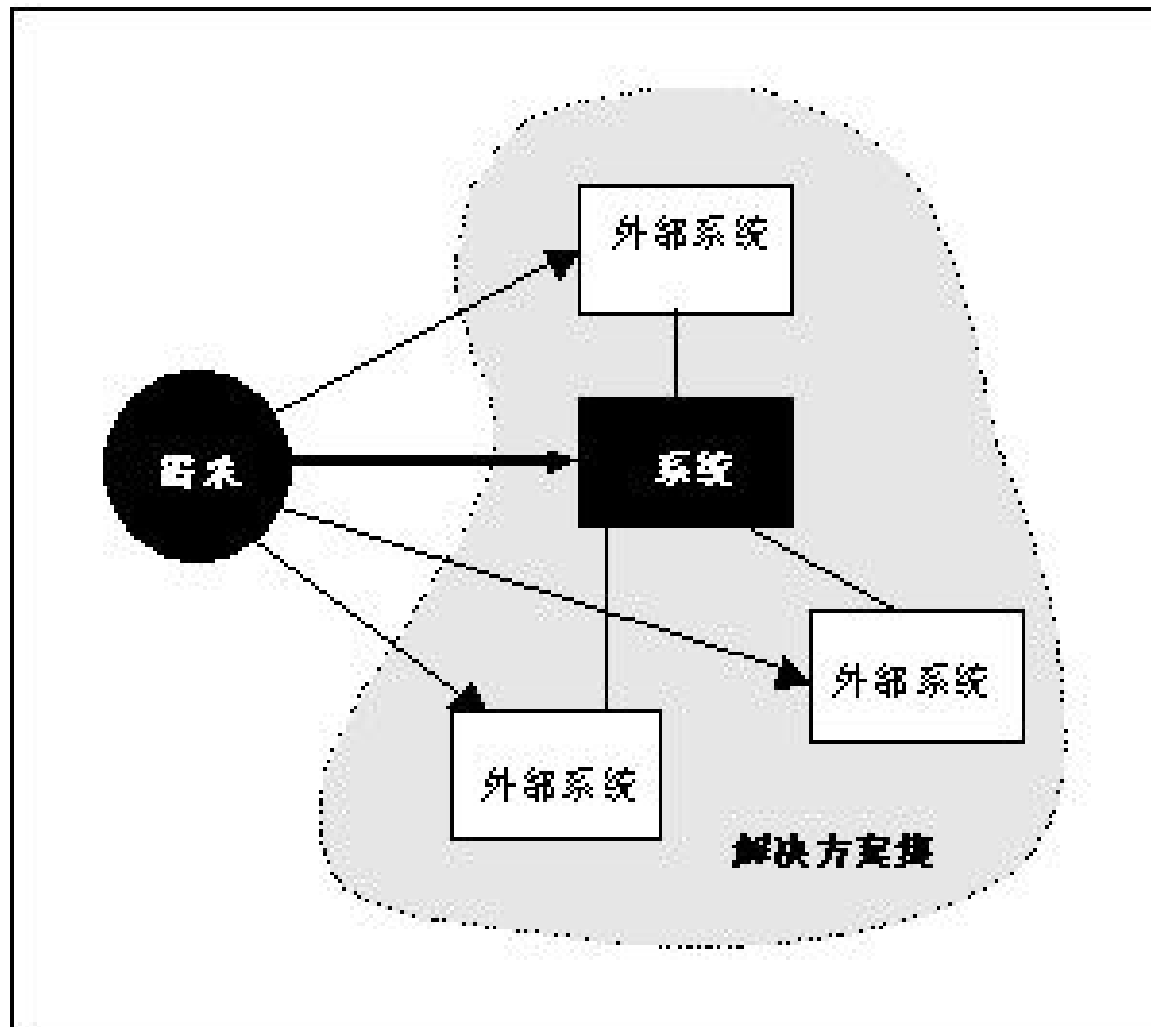
- 任务-01.9 标识设计约束
- 任务-01.10 评估信息保护的有效性
  - 子任务-01.10.1 向客户提供/展示文档化的信息保护需求
  - 子任务-01.10.1 得到客户对信息保护需求的认同
- 任务-01.11 支持系统的认证和认可（C&A）
  - 子任务-01.11.1 标识指派的批准官员（DAA）/认可员
  - 子任务-01.11.2 标识认证专家（CA）/认证员
  - 子任务-01.11.3 确定可适用的C&A和采办过程
  - 子任务-01.11.4 确保认可员和认证员对信息保护需求的认同

# 信息系统安全工程（ISSE）过程

---

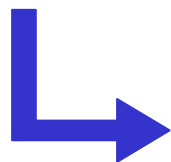
- 发掘信息保护需求
- 定义信息保护系统
- 设计信息保护系统
- 实施信息保护系统
- 评估信息保护系统的有效性

# 将需求分配解决方案集中

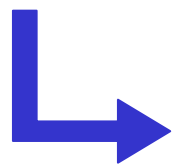


# 定义信息保护系统

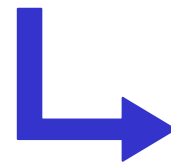
需求



目的/目标



要求



功能分析

ISSE将定义信息保护系统将要做什么，信息保护系统执行其功能的情况如何，以及信息保护系统的内部和外部接口

- 信息保护目标
- 系统背景/环境
- 信息保护需求/要求
- 功能分析

# 定义信息保护系统 -- 子任务

---

- 任务-02.1 定义系统安全背景环境
  - 子任务-02.1.1 定义系统边界及与SE的接口
  - 子任务-02.1.2 记录目标系统和外部系统的安全分配
  - 子任务-02.1.3 标识目标系统与外部系统之间的数据流以及与这些数据流有关的保护要求
- 任务-02.2 定义安全运行概念（CONOPS）
- 任务-02.3 制定系统安全要求基线
  - 子任务-02.3.1 定义系统安全要求
  - 子任务-02.3.2 定义系统安全操作模式
  - 子任务-02.3.3 定义系统安全性能测度
- 任务-02.4 审查设计约束

# 定义信息保护系统 -- 子任务（续）

---

## - 任务-02.5 评估信息保护的有效性

- 子任务-02.5.1 向客户提供并展示安全背景环境、安全CONOPS及系统安全要求
- 子任务-02.5.2 得到客户对系统安全背景环境、CONOPS及保护要求的认同

## - 任务-02.6 支持系统的认证和认可（C&A）

- 子任务-02.6.1 确保认可员和认证员对系统安全背景环境、CONOPS及保护要求的认同

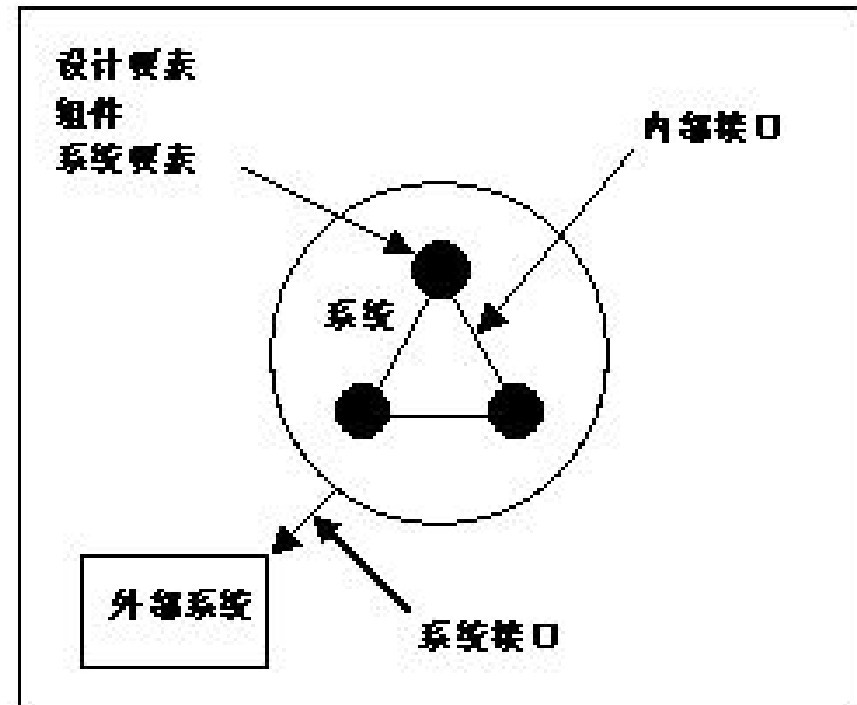
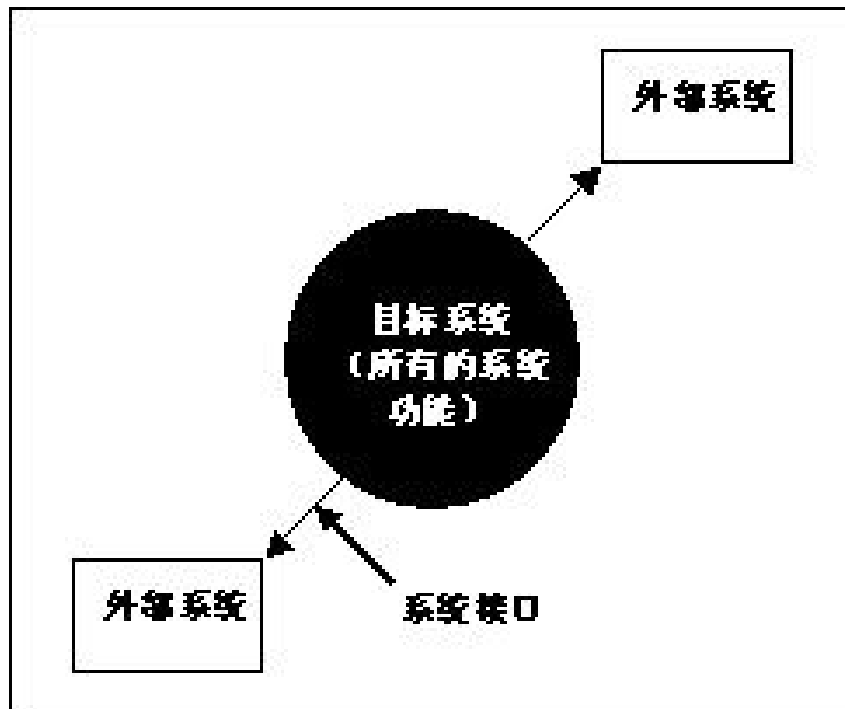
# 信息系统安全工程（ISSE）过程

---

- 发掘信息保护需求
- 定义信息保护系统
- 设计信息保护系统
- 实施信息保护系统
- 评估信息保护系统的有效性



# 定义与设计的区别



“定义系统要求”与“设计系统体系结构”

# 步骤

---



# 设计信息保护系统

---

## ■ ISSE将构造系统的体系结构，详细说明信息保护系统的设计方案

- 精练、验证并检查安全要求与威胁评估的技术原理
- 确保一系列的底层要求能够满足系统级的要求
- 支持系统级体系结构、配置项和接口定义
- 支持长研制周期和前期的采购决策
- 定义信息保护的检验和认证的步骤及战略

# 设计信息保护系统（续）

---

- 考虑信息保护的操作和生命周期支持问题
- 继续跟踪、精炼信息保护相关的采办和工程管理计划及战略
- 继续进行面向具体系统的信息保护风险审查和评估
- 支持认证和认可过程
- 加入系统工程过程

# 设计信息保护系统 -- 子任务

---

## - 任务-03.1 实施功能分析和功能分配

- 子任务-03.1.1 分析待建系统的体系结构
- 子任务-03.1.2 在体系结构中分配安全服务
- 子任务-03.1.3 选择安全机制的类型
- 子任务-03.1.4 提交安全体系结构设计，以供评估
- 子任务-03.1.5 修改安全体系结构
- 子任务-03.1.6 选择安全体系结构

## - 任务-03.2 评估信息保护的有效性

- 子任务-03.2.1 确保所选择的安全机制能够提供所需的安全服务
- 子任务-03.2.2 向客户解释安全体系结构如何满足安全要求
- 子任务-03.2.3 制定风险目标
- 子任务-03.2.4 得到客户对安全体系结构的认同

# 设计信息保护系统 -- 子任务（续）

---

## - 任务-03.3 支持系统的认证和认可（C&A）

- 子任务-03.3.1 准备并提交最终的体系结构文档，用于风险分析
- 子任务-03.3.2 与认可员和认证员一起协商风险分析的结果

# 开展详细的安全设计 -- 子任务

---

- 任务-04.1 确保对安全体系结构的遵循
- 任务-04.2 实施均衡取舍（trade-off）研究
- 任务-04.3 定义系统安全设计要素
  - 子任务-04.3.1 向系统安全设计要素中分配安全机制
  - 子任务-04.3.2 确定备选的商业现货（COTS）/政府现货（GOTS）安全产品
  - 子任务-04.3.3 确定需要定制的安全产品
  - 子任务-04.3.4 检验设计要素和系统接口（内部及外部）
  - 子任务-03.3.5 制定规范

# 开展详细的安全设计 -- 子任务（续）

---

## – 任务-04.4 评估信息保护的有效性

- 子任务-04.4.1 对详细设计进行风险分析
- 子任务-04.4.2 确保所选择的安全设计能够提供所需的安全服务
- 子任务-04.4.3 向客户解释安全设计如何满足安全要求
- 子任务-04.4.4 向客户解释并记录设计中存在的任何残余风险
- 子任务-04.4.5 得到客户对详细安全设计的认同

## – 任务-04.5 支持系统的认证和认可（C&A）

- 子任务-04.5.1 准备并提交详细设计文档，用于风险分析
- 子任务-04.5.2 与认可员和认证员一起协商风险分析的结果



# 信息系统安全工程（ISSE）过程

---

- 发掘信息保护需求
- 定义信息保护系统
- 设计信息保护系统
- 实施信息保护系统
- 评估信息保护系统的有效性

# 实施信息保护系统

---

- 购买
- 建设、集成
- 测试、认证

# 实施信息保护系统 – 子任务

---

## – 任务-05.1 支持对安全的实现和集成

- 子任务-05.1.1 参与安全实现的规划
- 子任务-05.1.2 检验安全工具和机制的互操作性
- 子任务-05.1.3 根据安全设计对实现进行验证
- 子任务-05.1.4 根据所选择的安全准则，验证安全组件是否已经得到评估
- 子任务-05.1.5 参与系统组件的集成，确保其满足了系统安全规范，且未改变组件的规范
- 子任务-05.1.6 参与系统组件的配置，确保安全特性已经激活，且安全参数已得到正确设置，能够提供所需的安全服务
- 子任务-05.1.7 确保系统和组件的配置已得到纪录，并实施了配置管理

# 实施信息保护系统 – 子任务（续）

---

## – 任务-05.2 支持测试和评估

- 子任务-05.2.1 建立测试和评估战略（包括示范、观察、分析和测试）
- 子任务-05.2.2 评审可用的测试和评估证据（例如来自于 CCEP、NIAP、内部测试的数据）
- 子任务-05.2.3 对测试和评估流程的开发提供支持
- 子任务-05.2.4 对测试和评估活动提供支持

## – 任务-05.3 评估信息保护的有效性

- 子任务-05.3.1 监督以确保安全设计的正确实现
- 子任务-05.3.2 实施并更新风险分析
- 子任务-05.3.3 定义风险及其可能对使命带来的影响，并通知客户和认可员及认证员

# 实施信息保护系统 – 子任务（续）

---

## – 任务-05.4 支持系统的认证和认可（C&A）

- 子任务-05.4.1 确保所需的C&A文档能满足客户和认可员及认证员的要求
- 子任务-05.4.2 为C&A过程提供文档记录和分析

## – 任务-05.5 支持安全培训

# 信息系统安全工程（ISSE）过程

---

- 发掘信息保护需求
- 定义信息保护系统
- 设计信息保护系统
- 实施信息保护系统
- 评估信息保护系统的有效性

# 评估信息保护系统的有效性 – 子任务

---

- 要在多项活动中评估信息保护的有效性：发掘信息保护需求、定义系统安全要求、定义系统安全体系结构、开展详细的安全设计以及实现系统安全。“评估信息保护的有效性”中的各项任务 and 子任务已经列入上述的活动中。

# 其它任务——规划技术工作

---

- 任务-07.1 估计项目范围
- 任务-07.2 确定资源及其可用性
- 任务-07.3 确定角色和责任
- 任务-07.4 估计项目成本
- 任务-07.5 制定项目进度
- 任务-07.6 标识技术活动



# 其它任务——规划技术工作（续）

---

- 任务-07.7 标识可交付项
- 任务-07.8 定义管理接口
- 任务-07.9 准备技术管理规划
- 任务-07.10 审查项目计划
- 任务-07.11 得到客户的认同

# 其它任务—管理技术工作

---

- 任务-08.1 指导技术工作
- 任务-08.2 跟踪项目资源
- 任务-08.3 跟踪技术参数
- 任务-08.4 监督技术活动的进展
- 任务-08.5 确保可交付项的质量
- 任务-08.6 管理配置要素
- 任务-08.7 审查项目绩效
- 任务-08.8 报告项目状态

# SE与ISSE过程的对应

SE 活动	ISSE 活动
<p><b>发掘需求</b></p> <p>系统工程师要帮助客户理解并记录用来支持其业务或使命的信息管理的需求，信息需求说明可以在信息管理模型（IMM）中记录。</p>	<p><b>发掘信息保护需求</b></p> <p>信息系统安全工程师要帮助客户理解用来支持其业务或使命的信息保护的需求。信息保护需求说明可以在信息保护策略（IPP）中记录。</p>
<p><b>定义系统要求</b></p> <p>系统工程师要向系统中分配已经确定的需求。应标识出系统的环境，并说明系统功能对该环境的分配。要写出概要性的系统运行概念（CONOPS），描述待建系统的运行情况。要建立起系统的基线要求。</p>	<p><b>定义系统安全要求</b></p> <p>信息系统安全工程师要将信息保护需求分配到系统中。系统安全的背景环境、概要性的系统安全 CONOPS 以及基线安全要求均应得到确定。</p>

# SE与ISSE过程的对应

SE 活动	ISSE 活动
<p><b>设计系统体系结构</b></p> <p>系统工程师应该分析待建系统的体系结构，完成功能的分析和分配，同时分配系统的要求，并选择相关机制。系统工程师还应确定系统中的组件或要素，将功能分配给这些要素，并描述这些要素间的关系。</p>	<p><b>设计系统安全体系结构</b></p> <p>信息系统安全工程师要与系统工程师合作，一起分析待建系统的体系结构，完成功能的分析和分配，同时分配安全服务，并选择安全机制。信息系统安全工程师还应确定安全系统的组件或要素，将安全功能分配给这些要素，并描述这些要素间的关系。</p>
<p><b>开展详细设计</b></p> <p>系统工程师应分析系统的设计约束和均衡取舍，完成详细的系统设计，并考虑生命周期的支持。系统工程师应将所有的系统要求跟踪至系统组件，直至无一遗漏。最终的详细设计结果应反映出组件和接口规范，为系统实现时的采办工作提供充分的信息。</p>	<p><b>开展详细的安全设计</b></p> <p>信息系统安全工程师应分析设计约束和均衡取舍，完成详细的系统和安全设计，并考虑生命周期的支持。信息系统安全工程师应将所有的系统安全要求跟踪至系统组件，直至无一遗漏。最终的详细安全设计结果应反映出组件和接口规范，为系统实现时的采办工作提供充分的信息。</p>

# SE与ISSE过程的对应

SE 活动	ISSE 活动
<p><b>实现系统</b></p> <p>系统工程师将系统从规范变为现实，该阶段的主要活动包括采办、集成、配置、测试、记录和培训。系统的各组件要接受测试和评估，以确保它们能够满足规范。成功的测试之后，各组件——硬件、软件、固件——要进行集成和正确的配置，并作为一个系统接受整体测试。</p>	<p><b>实现系统安全</b></p> <p>信息系统安全工程师要参与到对所有的系统问题进行的多学科检查之中，并向 C&amp;A 过程活动提供输入，例如检验系统是否已经针对先前的威胁评估结果实施了保护；跟踪系统实现和测试活动中的信息保护保障机制；向系统的生命周期支持计划、运行流程以及维护培训材料提供输入。</p>
<p><b>评估有效性</b></p> <p>各项活动的结果要接受评估，以确保系统能够满足用户的需求，系统在一个预期环境中实现了期望的功能，并达到了一个需要的质量标准。系统工程师要检查系统对任务需求的满足程度。</p>	<p><b>评估信息保护的有效性</b></p> <p>信息系统安全工程师要关注信息保护的有效性——系统是否能够为其使命所需的信息提供保密性、完整性、可用性、鉴别和不可否认性。</p>

# ISSE应用情况

---

- 确定信息保护需求
- 在一个可接受的信息保护风险下满足信息保护的需求
- 根据需求，构建一个功能上的信息保护体系结构
- 根据物理体系结构和逻辑体系结构分配信息保护的具体功能
- 设计信息系统，用于实现信息保护的体系结构
- 从整个系统的成本、规划运行的适宜性和有效性综合，在信息保护风险与其他ISSE问题之间进行权衡

# ISSE应用情况（续）

---

- 参与对其他信息保护和系统工程学科的综合应用
- 将ISSE过程与系统工程与采办工程相结合
- 以验证信息保护设计方案并确认信息保护的需求为目的，对系统进行测试
- 根据用户需要对整个过程进行扩充和剪裁，为用户提供系统部署后的进一步测试

