**第二章 信息系统安全工程过程**

**1．ISSE是什么？主要包括哪些过程？**

**2．ISSE的指导思想是什么？**

**3．ISSE的基本功能有哪些？每个功能具有哪些作用？**

**4．请简要概述ISSE的实施框架。**

**5．信息系统的安全需求是如何发掘的？**

**6．从哪些方面定义信息安全系统？**

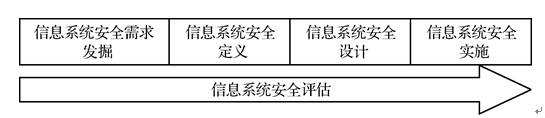
**7．信息安全系统的设计要经历哪几个过程以及每个过程需要做什么？**

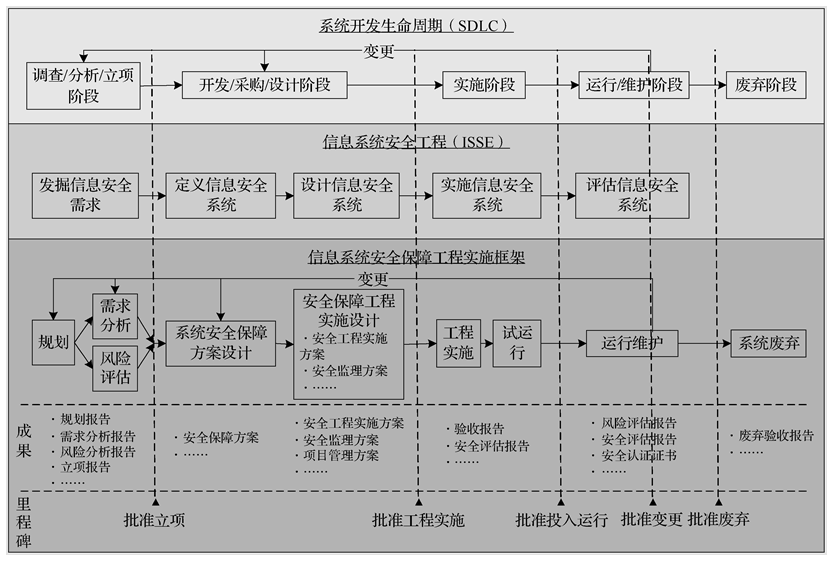
**8．实施信息安全时需要考虑哪些问题？**

**9．信息安全系统评估在ISSE过程中各个阶段的作用有哪些？**

**10．请简述ISSE是在上机管理系统中的应用。**

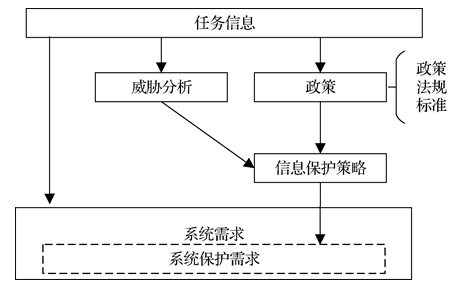
1. （1）信息系统安全工程（ISSE）作为信息系统安全建设的方法论，是发掘用户信息保护需求，然后以经济、精确和简明的方法来设计和制造信息系统的一门技巧和科学。（2）主要分为发掘信息保护需求、确定系统安全要求、设计系统安全体系结构、开展详细安全设计、实施系统安全和评估信息保护有效性这几个阶段。



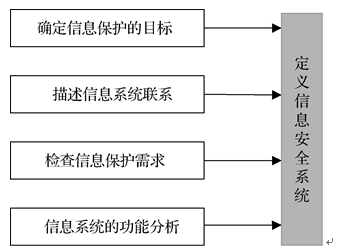
1. （1）以满足用户安全需求为目的。（2）以系统风险分析为基础。（3）以系统工程的方法论为指导。（4）以技术、运行、人作为要素。（5）安全技术以纵深防御为支撑（技术）。（6）以生命期支持保证运行安全（运行）。（7）安全管理以安全实践为基础（人）。（8）安全质量以测评认证为依据。（9）质量保证以动态安全原理（PDCA）为方法。
2. ISSE具有以下6个基本功能。①安全规划与控制：系统和安全项目的管理与规划活动，开始于一个机构从业务角度来承担对应的工程。如果安全规划做得足够好，那么就能为系统将安全需求转化成有效的设计和实现提供坚实的基础。规划和准备活动为建立要求的可跟踪性、基准程序和客户确认提供了平台。②确定安全需求：系统特有的需求和定义一般是在两个级别上给出：从用户角度给出高级操作的安全要求定义；从系统开发者或集成者的工程观点出发，提出更正式的安全要求的规范式定义。③支持安全设计：通过安全设计，一个被选择的系统体系结构可以被形式化，然后转换为稳定的、可生产的和有好的经济效益的系统设计。对信息系统而言，这种转换通常包括软件开发和软件设计，还可能包括信息数据库或知识库的安全设计。④分析安全操作：它将影响信息系统产品，特别是产品安全生产过程和产品本身的安全要求的解决方案。通过这一功能的反复应用与安全设计支持功能相结合，将确认“过程”安全解决方案。安全操作概念的分析和定义是系统工程和ISSE过程的集成部分，是对安全认证和认可（C/A）的关键输入。⑤支持安全生命周期：SPO（系统项目办公室）将一直监督系统的整个生命期各阶段的计划，包括开发、生产、现场工作、维护、培训和处理等。在操作和维护期间，对过程设计、操作确认等都可以用充分准备的生命周期支持计划及其实现来完成。⑥管理安全风险：在系统工程过程中，风险是对达到属于技术性能、成本和进度方面的目的和目标的不确定性的一种量度。风险等级用事件和事件结果的概率来分类。
3. 

调查/分析/立项阶段：该阶段是发掘信息安全需求的阶段。开发/采购/设计阶段：该阶段是定义和设计信息安全系统的阶段。实施阶段：该阶段是对信息安全系统进行工程实施和试运行过程的阶段。运行/维护阶段：该阶段是在系统运行过程中评估信息系统有效性的阶段。废弃阶段：该阶段是系统的生命周期终结，需要完成系统废弃验收报告，决策者可以基于相应结果和相关的法律法规、政策标准批准进行废弃并进行相应废弃处理工作。

1. 首先要了解相关的业务需求，确定信息和任务之间的关系以及其重要性。界定相关法律和法规的要求，明确设计限制，如电子政务的有关要求、国家安全管理机构的相关规定、相应的安全标准以及国际、国家的有关安全标准等；以及本行业、本部门的相关规定和标准。整个过程大致分为了解信息保护需求、掌握信息系统威胁以及考虑信息安全策略三个部分。



1. 一般信息安全系统定义分为以下几个部分：确定信息保护的目标、描述信息系统联系、检查信息保护需求以及信息系统的功能分析。



1. ①功能分配：当系统的一系列功能确定后，对每一个具体的功能，应该制定相应的信息保护功能。这些信息保护功能相互协作形成一个信息保护系统体系架构，用户保护整个信息系统的功能安全。整个功能分配过程如下。（1）确定安全系统的组件或要素；（2）将安全功能分配给这些要素，并描述这些要素间的关系。

②信息保护预设计：在信息保护预设计阶段，ISSE工程师应分析设计约束和均衡取舍，完成初步的系统安全设计，并考虑生命周期的支持，具体包括以下内容。（1）根据之前分析系统安全体系结构的结果，对已经定义好的安全功能进行检查和修改；（2）选择相应的安全机制类型，验证并保证是否满足所有的安全需求；（3）加入系统工程过程，对信息保护预设计进行审查，包括认证/认可（C/A）、管理决策和风险分析等。

③信息保护详细设计：在本活动中，信息系统安全工程师将进一步完善设计方案，细化安全规范，确保对安全体系结构的遵循，实施均衡取舍研究，主要包括以下内容。（1）检查、细化并改进预设计阶段的成果；（2）对解决方案提供细节设计资料以支持系统层和配置层的设计；（3）检查关键设计的原理和合理性；（4）设计信息保护测试与评估程序；（5）实施并追踪信息保护的保障机制；（6）检验配置项层设计与上层方案的一致性；（7）提供各种测试数据；（8）检查和更新信息保护的风险与威胁计划；（9）加入系统工程过程，并支持认证/认可（C/A）和管理决策，提出风险分析结果。

1. ①采购系统部件：系统部件的采购决定了是自行生产部件还是通过购买来获取部件，通常这需要以市场中的产品的好坏、能否满足相应的需求为依据。在做相应的决定之前，应该对各种影响因素进行相应的考虑，比如：安全性、成本、易用性、风险等。在购买时，应该确定备选的商业现货（COTS）和政府现货（GOTS）等安全产品。在采购部件的过程中，具体应该注意如下几点因素。（1）确保能够满足当前所有的安全需求；（2）考察现有的多个产品，从中选出最满足当前系统部件需求的产品；（3）考虑到未来技术发展的因素，怎样将新的技术融入当前的系统当中。

②信息安全系统的构造：信息安全系统的构造是对信息系统的保护设计进行实现，包括对安全部件进行部署和集成。系统在整个构造的过程中会受到诸多因素的影响，而这些因素决定了信息安全系统的正确与否，具体考虑如下。（1）部件的集成过程是否遵循相应的安全规范；（2）部件的配置参数能否满足所需的安全服务；（3）系统建造的流程是否依据了相应的设计文档。

③信息安全系统的测试：这个阶段的工作主要是检验信息安全系统的实现效果，包括功能的可用性、安全的有效性等，具体的工作如下。（1）根据详细的安全设计对实现进行验证；（2）所有的接口均需要测试，系统和设计工程师将撰写测试流程；（3）通过集成测试将验证子系统或系统的性能，确保能够防御此前的威胁评估中确定的威胁；（4）验证系统的确能在集成和测试时，重要的一项工作是记录下安装、操作、维护和支持的流程；（5）加入系统工程过程，并支持认证/认可（C/A）和管理决策，提出风险分析结果。

1. 针对每个过程，其评估信息有效性的任务如下。①信息安全需求发掘：需要表示过程的概貌，综述信息模型，描述任务或业务的信息攻击威胁。针对信息威胁建立安全服务，确定安全服务对客户的相对重要性。得到客户对本阶段活动结论的认同，作为判断系统安全有效性的基础。②信息安全系统定义：确保所选择的解决方案组满足任务或业务的安全需求。调整系统的边界，提出安全上下文、向客户提供并展示安全背景环境、安全CONOPS以及系统安全要求，并获得客户的认同。保证项目的安全风险是用户可以接受的。③信息安全系统设计：开展正式的风险分析，确保所选择的安全机制能够提供所需的安全服务，并向客户解释安全体系结构如何满足安全要求。执行互依赖分析，比较安全机制的强度，审查所选择的安全服务和机制是否能够对抗信息威胁。一旦完成设计，风险评估的结果，尤其是风险减缓需求和残余风险，都将文档化并与客户共享以便得到其认可。④信息安全系统实施：实施并更新风险分析，制定风险减缓战略。标识风险可能对任务带来的影响，并通知客户和认可员及认证员。
2. ISSE中的各过程：信息系统安全需求发掘、信息系统安全定义、信息系统安全设计、信息系统安全实施，分别对应上机管理系统中①上机管理系统安全需求的发掘②上机管理系统安全的定义③上机管理系统安全的设计④上机管理系统安全的实施。