**第三章 信息安全工程能力成熟度模型**

**1．SSE-CMM是什么？它的优势和用途是什么？**

**2．SSE-CMM中的过程域有哪几类，每类过程域的特点是什么？**

**3．域维中的基本实施、过程域和过程类是什么？**

**4．能力维中通用实施、公共特征以及能力级别的关系是什么？**

**5．SSE-CMM的模型使用场合主要有哪些？**

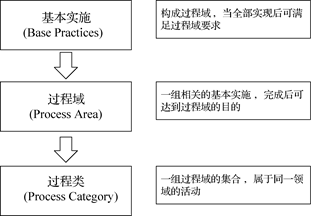
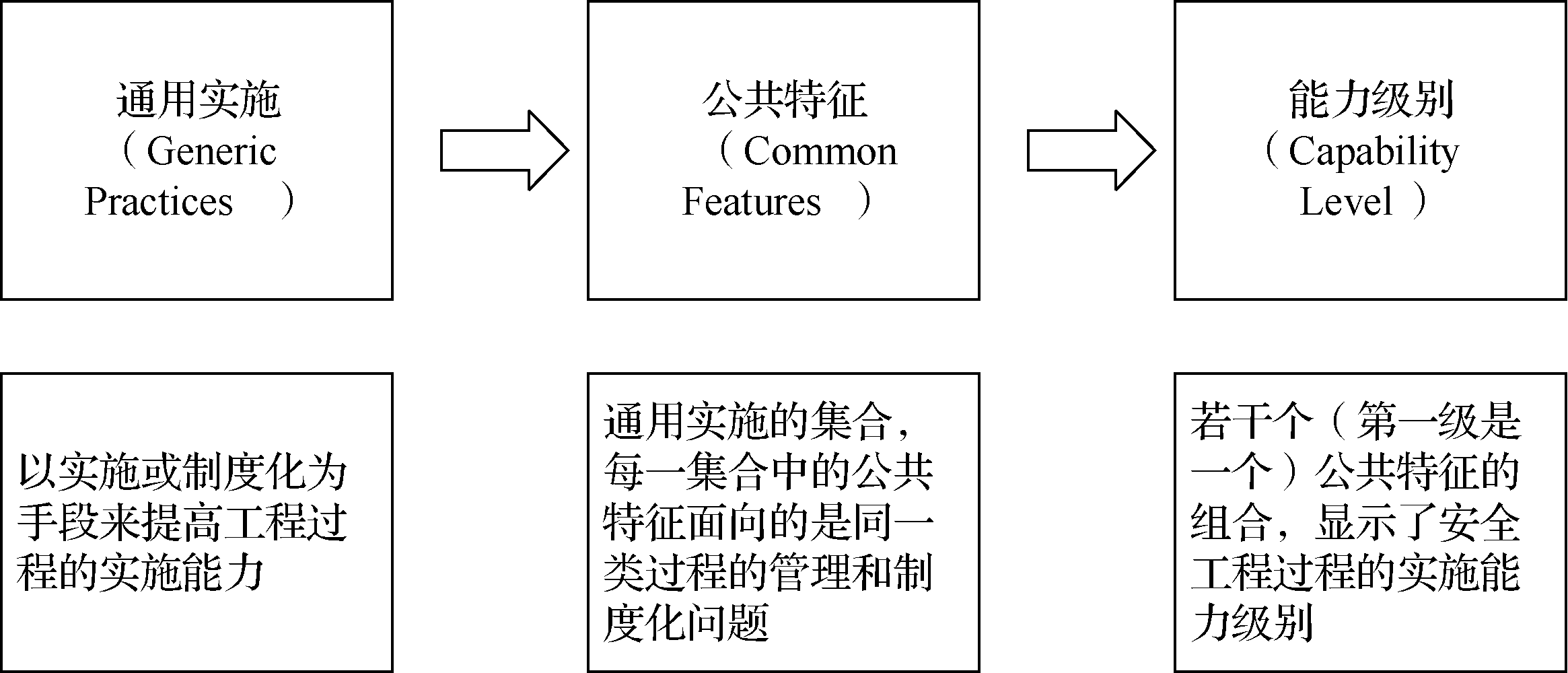
**6．请简要描述组织如何对SSE-CMM中的过程域进行测量。**

**7．IDEAL方法模型分为哪几个阶段？每个阶段有哪些内容？**

**8．请简述一下SSE-CMM的能力评估方法SSAM。**

**9．SSE-CMM与ISSE的区别有哪些？**

**10．相比较SSE-CMM而言，DSMM模型而言有哪些新的特点？**

1. （1）系统安全工程能力成熟模型（SystemsSecurity Engineering Capability Maturity Model，SSE-CMM），一个专门应用于系统工程的能力成熟模型（CMM）的构思，其目的是建立和完善一套成熟的、可度量的安全工程过程。（2）SSE-CMM优势：改进安全工程实施的现状，以达到提高安全系统、安全产品和安全工程服务的质量和可用性并降低成本的目的。SSE-CMM的应用方式如下：①作为工程机构的工具来评估其安全工程实施活动，并实现对这些工程实施的改进。②作为安全工程评估机构（如系统认证机构、产品评估机构）的工作基础，基于机构的能力为被评估机构建立起信任度（作为系统或产品安全保证的要素）。③为客户建立起用以评估提供商的安全工程能力的标准机制。当前市场中的信息安全产品主要分为两种，一种是已评估的产品，一种是未评估的产品。由于产品的评估耗时耗力且价格昂贵，所以评估周期漫长导致进入市场时需求已经发生新的变化。而对于未评估的产品，用户只能根据产品说明书和与其他产品对比来决定是否购买。
2. （1）三类：安全工程过程域、组织过程域和项目过程域。（2）安全工程过程域分为3个基本类别的领域：风险过程、工程过程和保证过程。对最简单的层次而言，风险过程要识别内含于产品、系统开发过程中的危险因素，并将其按危险性的等级进行排列；工程过程则要对上述危险带来的问题采取解决措施；保证过程要确保安全性的解决措施有效，并将这种确信传递给客户；项目过程域的目标之一是确保项目的质量，这不但要考虑系统的质量，而且还要考虑用于构造系统的过程域的质量。另外，这个过程必须严格坚持并贯彻于 SSE-CMM的整个生命周期。项目过程域的另一目标是对项目的技术工作进行有效的管理，这涉及对技术工作的计划和监控；组织过程域包括三方面的内容：为安全工程提供支持、指导产品开发方向、安全工程过程的标准化。
3. 
4. 
5. SSE-CMM模型有3个主要用途：用于安全工程过程的改进、对安全工程承包单位实施能力的评估、帮助客户获得信任保证。①安全工程过程的改进：可以使一个安全工程组织对其安全工程能力的水平有一个认识，以便设计得到改进的安全工程过程，提高其安全工程过程能力。②安全工程承包单位实施能力的评估：允许一个客户组织了解其提供商的安全工程过程能力。③信任度评估：凭借证据对所采用工程的成熟性做出支持性声明，提高了产品、系统和服务的可信性。
6. 以下步骤来考察一个组织如何对SSE-CMM中的过程域进行测量。①根据业务内容，从PA01-PA22中选择一个适合机构业务或任务的一个过程域。②查看该过程域的描述、目标及所包含的基本实施（BP）。③查看机构中是否有在执行该过程域包含的所有基本实施（BP）。④查看该过程域的目标是否得到了满足，若对应的基本实施（BP）都被执行，则该过程域的目标完成。⑤若过程域的目标已经满足，则在相应的公共特征1.1“执行基本实践”列上做标记。⑥查看公共特征2.1“计划执行”中的描述和所包含的通用实施（GP）。⑦对照公共特征2.1“计划执行”中的通用实施（GP），查看机构是否正在计划执行所选择的过程域。⑧如果步骤 7得到满足，在公共特征2.1“计划执行”列做上标记，如未满足，则跳至步骤10。⑨对照第二级中的其他每一个公共特征，分别重复步骤6～8。⑩对其他每一个过程域，重复步骤2～9。
7. ①初始化（Initiating）：为安全工程过程的成功改进奠定基础。②诊断（Diagnosing）：判断当前的工程过程能力现状。③建立（Establishing）：建立详细的行动计划，为实现目标做出规划。④执行（Acting）：根据计划展开行动。⑤学习（Learning）：吸取经验，提升过程能力。
8. SSE-CMM的能力评估方法SSAM旨在为系统安全工程界提供一种开放的可理解的方案，供准备实施和正在实施SSE-CMM评估的人员使用。据在SSE-CMM中详述的标准获得的实际实施的基线或基准，SSAM可用于评价产品开发者、服务提供者、系统集成者、系统管理者和安全专家。尽管SSAM的基本概念适用于其他评估，但它是专为支持SSE-CMM而设计的。SSAM包含了为实现对组织机构的系统安全工程过程能力和成熟度的评定所需的信息和方向。

|  |  |  |
| --- | --- | --- |
|  | ISSE | SSE-CMM |
| 来源 | 系统工程 | 能力成熟度模型 |
| 思路 | 以时间维来描述信息安全工程过程 | 以域维和能力维描述信息安全工程的能力成熟度 |
| 作用 | 在生命周期中对系统的安全风险等问题不断做出审查、验证，并找到折衷、平衡的风险解决方案，进而对系统做出调整 | 改进安全工程实施的现状，提高安全系统、可信任产品、安全工程的服务质量和可用性，并降低成本 |
| 过程结构 | 系统工程 | 风险、工程、信任度 |
| 体系结构 | 贯穿于系统工程的全过程，在特定系统开发的每个阶段都进行集成 | 组织可以以任何方式创建符合他们业务目标的过程和组织结构 |
| 缺陷 | 缺乏针对信息安全的可信保证要求，不适合反映时间过程不明显的领域 | 很难判断己定的过程域是否足够，如何添加过程域也未明确 |

1. 数据安全能力成熟模型是以数据安全为中心思想，结合大数据时代这一特征而提出的。它是将能力成熟度模型的分析方法借鉴到数据安全领域，基于数据的生命周期，结合组织中各个维度的安全能力，从而构成一个三维的大数据安全能力成熟度模型（Data Security Maturity Module，DSMM）。