《信息安全保障》重点知识点串讲

一、信息安全保障基础

1. 信息安全定义：ISO 定义，通过技术和管理的手段防护信息系统不破坏、篡改等，掌握不同定义（数据安全、信息安全、通信安全、信息系统安全、网络安全、网络空间安全）的使用场景。
2. 信息问题分类：狭义（技术）和广义（业务）问题，根源包括内因和外因。
3. 信息安全特征：系统、动态、无边界、非传统。
4. 信息安全属性：保密性、完整性和可用性。
5. 信息安全视角：国家、企业、个人。
6. 信息安全发展：通信安全、计算机安全、信息系统安全、信息安全保障、网络空间安全。掌握每一个阶段的内容和特点。
7. 网络空间安全：学科、应用和物理范围上扩展了；**防御、情报和威慑**三位一体的安全；威胁情报和态势感知。

二、信息安全框架模型

1. PPDR 模型

1）PPDR：策略、保护、检测和响应。
2）思想：填充安全间隙，安全在时间上连续性。
3）公式：Pt>攻击时间>Dt+Rt, Et<=0；

2. IATF 模型

1）思想：深度防御。
2）三要素：人、技术、操作。
3）四个方面：本地计算环境、网络边界、网络基础设施、支撑性基础设施。

3. 保障评估框架

1）内容：安全保障对象的全生命周期中通过**人、技术、管理**和**工程**实现保密、完整和可用，最终服务于业务使命。
2）流程：**ISPP->ISST->建设->评估**（TCML1-5,MCML1-5,ECML1-5）。
3）ISPP：标准化信息系统安全需求；ISST：标准化信息系统安全设计方案。

4. 商业应用架构（SABSA）

1）出发：业务安全和业务风险为出发点，为组织架构建设和安全提供方法和流程。
2）内容：背景（业务）、概念（架构）、逻辑（设计）、物理（工程）、组件（实施）、运营（运维）。
3）阶段：规划、设计、实施、管理和测量（**PDCA,计划、实施、检查、改进**）。

三、信息安全工作流程

1. 需求：来源要全面（合规、业务、风险评估），建议使用 ISPP 的方法。
2. 设计：建议使用 ISST 的方法。
3. 工程：建议使用 SW-CMM\CMMI\ISO/IEC 21827 **SSE-CMM（分为 1-5 级）**方法。
4. 测评：产品 CC 标准（ISO/IEC 15408,GB/T 18336）EAL1-7；信息系统等级保护测评 1-5；工程服务商 **1-5**（SSE-CMM）；人员测评（NISP/CISM/CISP 等）。
5. 运维：主要方法是风险管理。
6. 废弃。

四、安全保障新领域

1. 云计算安全：IaaS\PaaS\SaaS。核心问题是开源工具。
2. 物联网安全：感知、传输、支撑、应用。核心问题是感知和传输安全问题。
3. 移动互联网安全：核心问题是系统和芯片。
4. 大数据安全：海量、高速、多变、多样性，GDPR 作为关注。大数据自身的安全和大数

据平台的安全。

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请一定进一步结合官方的教材进行理解和掌握全面，以免产生以偏概全的问题。

（END）