测试点4-1

什么是信息安全管理中的PDCA模型?

PDCA（Plan、Do、Check、Act)

规划（Plan）通过风险评估，了解安全需求， 制订解决方案;

实施（Do）将解决方案付诸实施； - 检查（Check）监视评审方案的有效性;

处置（Act）对发现的问题予以解决，产生新 的需求则再次进入规划阶段。

我国的信息安全法律法规体系是如何构成的?

信息安全法律法规是指国家和相关职能部门为维护信息安全，预防信息犯罪 的法律规范的总称。涉及网络与信息系统安全、信息内容安全、信息安全系统与产品、保密及密码管理、计算机病毒与危害性程序防治、金融等特定领域的信息安全、信息安全犯罪制裁等多个领域 ，初步形成了我国信息安全的法律体系。

还包括有通用性法律法规，惩戒信息犯罪的法律，针对信息网络安全的特别规定

有人说西方的网络环境是开放自由的，公民在网络空间中的行为不会受到管理和监控，这种观点是正确的吗？请查阅相关资料，谈谈自己的看法。

不正确，棱镜门事件，脸书facebook用户个人信息泄露。棱镜门是美国政府监听美国公民的手段，它通过此实施控制公民的日常生活。即使西方的自由，也只不过是表面的自由，公民的自由也会存在被暗中管理和控制。

测试点4-2

请查阅《中华人民共和国网络安全法》，回答以下问题:

网络安全法是如何规范个人信息收集行为的?

第二十二条：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第三十七条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。

第四十一条：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

网络安全法是如何斩断信息买卖利益链的?

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

网络安全法是如何防范个人信息泄露的?

　第四十三条：个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

网络安全法是如何对网络诈骗溯源追责?

第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

测试点4-3

GB17895-1999《计算机信息系统安全保护等级划分准则》中划分了哪几种 安全等级?

第一级 用户自主保护级：提供用户和数据隔离功能。

第二级 系统审计保护级：实施粒度更细的自主访问控制，它通过登录规程、审计安全性 相关事件和隔离资源，使用户对自己的行为负责。

第三级 安全标记保护级：具有系统审计保护的功能。

第四级 结构化保护级：建立在一个明确定义的形式化安全策略模型之上，要求将第三级 系统中的访问控制扩展到所有主体与客体。

第五级 访问验证保护级：满足访问监控器需求，由访问监控器仲裁主体对客体的全部访问。

GB/T 22239-2019 《网络安全等级保护基本要求》中分别对哪几类信息系统做出了专门规定?

安全通用，云计算安全，移动互联安全，物联网安全，工业控制系统安全。

概述等级保护的工作流程。

定级、备案、安全建设、等级测评、监督检查

1.定级：确认定级对象, 参考《定级指 南》等初步确认等级,组织专家评审,主管单位审核,公安机关备案审查。

2.备案： 持定级报告和 备案表等材料 到公安机关网 安部门进行备 案。

3.安全建设：以《基本要求》 中对应等级的 要求为标准,对 定级对象当前 不满足要求的 进行建设整改。

4.等级测评：委托具备测评 资质的测评机 构对定级对象 进行等级测评, 形成正式的测 评报告。

5.监督检查：向当地公安机 关网安部门提 交测评报告,配 合完成对网络 安全等级保护 实施情况的检 查

假定有一个由银行提供代水电代收费服务的信息系统，如果该系统受到破坏 ，将导致个人或企业无法通过银行网点缴纳相关费用，水电公司的收费业务 只能在其处理能力有限营业厅进行，导致业务能力大幅度下降，依据等级保 护的定级规则，思考该系统应属于几级保护的对象?

严重损害，第三级

测试点4-4

作为一名从事信息安全专业的人员，应该如何从自身做起，共同营造清朗的网络环境?

1.树立良好的道德意识，做有道德，有底线的信息安全专业人员

2.增强法律意识，不利用信息安全技术做违法犯罪的行为，勿以恶小而为之

3.学无止境，不断学习信息安全相关知识，从自我做起，锻炼自我

4.积极宣传信息安全知识，和他人共同营造清朗的网络环境