**(9) RBAC模型是否可以实现中国墙模型？请说明理由。**

RBAC可以实现中国墙模型，RBAC将授权针对工作角色而不是直接针对用户，实现了用户与权限的逻辑分离，这样可以大大降低访问控制管理的复杂性，同时，角色的划分还有利于职责分离的实施。可以满足中国墙模型的两条规则，用户想获得怎样的权限必须在其获得对应的工作角色之后才能获得，可以解决利益冲突。

**（10）请自学NIST《Framework for Improving Critical Infrastructure Cybersecurity （v1.0）》附录A Framework Core中表“Table 2：Framework Core”的相关内容，选择其中一个分类（Category），例如“Access Control (PR.AC):”，用中文简要介绍其所有子类（Subcategory）的内容。**

Access Control（PR.AC）中包含了5个子类

PR.AC-1：被授权的设备和用户的身份标识和证书是被管理的。

PR.AC-2：对资产的物理存取是管理和保护的。

PR.AC-3：远程访问是托管的

PR.AC-4：Access权限是被管理的，包含“最小特权”和“分离”的原理

PR.AC-5：网络的完整性是受保护的适当的，包含了网络的隔离性。

**（11）简要阐述三纵三横两个中心的信息安全技术防护框架。**

在工作流程相对固定的重要信息系统中，信息系统主要由操作应用、共享服务和网络通信三个环节组成。如果信息系统中每一个使用者都是在安全管理支持下经过认证和授权的，其操作都是符合规定的，网络上也不会被窃听和插入，那么就不会产生攻击性的事故，就能够保证整个信息系统的安全，这便构成了工作流程相对固定的生产系统内的信息安全保护框架。在技术层面上将信息系统安全保护分为以下五个环节作为保护重点：应用环境 、应用区域边界 、网络和通信传输 、安全管理中心 、密码管理中心

**（12）如何理解可信计算的概念，可信计算和传统的信息安全保护机制的不同点是什么？**

可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性。签注[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5)是一个2048位的RSA公共和私有密钥对，它在芯片出厂时随机生成并且不能改变。这个私有密钥永远在芯片里，而公共密钥用来认证及加密发送到该芯片的敏感数据。

可信计算是在硬件平台上引入安全芯片（可信平台模块）来提高终端系统地安全性，也就是在每个终端平台上植入一个信任根，让护士从bios到操作系统内核再到应用层构建信任关系，当终端收到攻击时能够实现自我保护、自我管理和恢复；而传统的信息安全保护机制是通过授权给相应角色以相应工作从而得到该部分的权限，并没有从计算机的硬件平台出发。

**（13）什么是可信计算基（TCB）？**

在一个安全操作系统中，与安全相关的部分的全体被定义为可信计算基，即TCB，它由计算机系统中所有安全保护机制构成的。

GB 17859 定义可信计算基为：计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。

可信计算基是安全操作系统自身安全性的基石。为了确保安全操作系统自身的安全性，就需要确保TCB 的设计遵循一些原则。高安全级别的操作系统要求TCB 独立于系统的其它部分，要求TCB 中不含有和安全无关的内容，并且要求TCB 的设计具有引用监视器的特性，使TCB 的安全性可以被比较严格的分析和测试。

**（14) 管理安全要求主要有哪些？并请选其中之一进行举例说明。**

管理安全要求主要有：

1、管理层的支持；

2、定义安全要求；

3、保证人员安全；

4、员工的安全意识和培训；

5、变更管理。

举例说明：如果不能获得管理层的支持，那么工作无法开展，责任授权不明晰出现问题时不能找到合适的人选去解决，所需各类资源如经费实验设备等无法获得，如果需要其他部门的协助也不能够及时协商。

**(15) 调研有关用户帐户、口令管理的各种方法,以及帐户/口令泄露的案例; 并尝试设计一个你认为是安全、合用的口令策略。**

1.密码长度12位以上

2.同时包含数字字母下划线或其他特殊字符

3.系统强制定期修改口令

**(16) 对于下面的访问控制矩阵，请写出其相应的访问控制列表和能力表。**

访问控制列表：

acl(文件1)={ (进程1，{读,写,拥有} ) }

acl(文件2)={ (进程2，{读,写,拥有} ) }

acl(进程1)={ (进程1，{读,写,执行,拥有} ) }

acl(进程2)={ (进程2，{读,写,执行,拥有})}

能力表：

cap(进程1)={ (文件1，{读,写,拥有})，(进程1，{读,写,执行,拥有} ) }

cap(进程2)={ (文件2，{读,写,拥有})，(进程2，{读,写,执行,拥有})}

**(17) 请简要阐述一下安全保障的作用，及其分类。**

作用：

安全保障是对实体满足安全需求的信心，依赖于应用保障技术提供的专门证据。

安全保障是通过使用多种多样的安全保障技术而获得，这些安全保障技术提供证据来说明系统的实现和运行能够满足安全策略中定义的安全需求。

分类：策略保障、设计保障、实现保障、运维保障

**(18) GB 17859将计算机信息系统安全保护能力分为哪几个等级？并选择其中之一，简要介绍其主要安全功能要求。**

等级：

第一级: 用户自主保护级

第二级: 系统审计保护级

第三级: 安全标记保护级

第四级: 结构化保护级

（本级的计算机信息系统可信计算基建立于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自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。）

第五级: 访问验证保护级

**(19) GB/T 18336（CC）将安全等级分为哪几个评估保证级？并选择其中之一，简要介绍其主要的安全保障（保证）能力要求。**

等级：

EAL1：功能测试：

EAL2：结构测试

通过利用功能和接口的规范、指导性文档和TOE的高层设计，对安全功能进行分析来提供保证，以理解安全行为。

EAL3：系统地测试和检查

EAL4：系统地设计、测试和复查

EAL5：半形式化设计和测试

EAL6：半形式化验证的设计和测试

EAL7：形式化验证的设计和测试