1. TCB 在 TCSEC 中的定义是一个计算机系统中的保护机制的全体，它们共同负责实施一个安全策略，包括硬件，固件和软件；一个TCB由在一个产品或系统上共同实施一个统一的安全策略的一个或多个组件构成。

TCB主要包括哪些部份：

①固件和硬件 ②与安全策略相关的文件 ③负责安全管理的人员 ④安全核 ⑤具有特权的进程和命令 ⑥

2. 最小特权原则是系统仅授予用户执行任务中所需最少的权限，以确保可能发生的事故，错误、网络部件的篡改等原因造成的损失最小。

3. LKM机制是可加载内核模块，即在内核中动态加载代码的能力。系统可调用 create_module，init_module，query_module 以及 delete module 等分别用于创建，初始化，查寻和删除模块。

4. 三个方面：① 云存储平台安全机制 ② 云存储管控安全机制 ③ 云存储应用安全机制

5. 可信计算的安全基本思想是：① 首先在计算机系统中建立一个信任根，信任根的可信性由物理安全、技术安全与管理安全共同确保 ② 再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用。一级测量认证一级，一级信任一级，再把这种信任扩展到整个计算机系统，从而确保计算机系统的可信。