# 安全需求总览

## 保密性需求

保密性需求本质上是为了解决敏感数据泄露和被未授权实体访问的问题。数据的敏感性分类常被用来确定保密性需求的级别。保密性需求还需要考虑数据的整个生命周期，包括从数据的产生到最后的应用结束所面临的各种威胁。

## 完整性需求

完整性需求主要是为了解决未经授权的修改问题，确保系统或软件按照预期的功能工作。不仅要确保系统的完整性（指对系统或软件进行修改的保护），同时还包括数据的完整性（对系统或软件所处理数据的保护），以及系统和数据的完备性和一致性。

## 可用性需求

可用性需求主要用于协助授权用户防范 DoS 攻击，当然，不安全的编码结构，如悬挂指针、内存分配不当或无限循环结构，也都会影响可用性。

## 可认证需求

可认证需求就是要验证并确保那些提出认证申请的实体的合法性和有效性。其中，实体可能是一个人、一个过程或一个硬件设备。

## 授权需求

授权需求是在身份认证的基础上，为了确认一个经过认证的实体对于请求的资源所需要的访问权限、优先级及可执行的动作而进行的权限分配方面的需求。可认证性回答的是 “实体是否是他所声称的身份”，可授权性回答的是 “实体能做什么”。授权分级。

## 可审计性需求

可记账性需求帮助建立用户操作的历史记录，为每项活动提供一个完整的、可审计的轨迹。如果软件行为被适当地记录和跟踪，那么审计不仅可以作为一种检测控制手段帮助计算机调查取证，同时也可以用于错误和异常故障诊断。

## 合规性需求

使用 等保，GDPR等按条例通过。