定义授权和授予授权需要数据清单、对数据需求仔细分析以及每个用户权利中公开的数据文档。高度敏感信息通常与非敏感信息混合在一起。企业数据模型对于识别和定位敏感数据至关重要。

即使数据无意暴露，利用数据脱敏也可以保护数据。某些数据法规需要加密，这是落地脱敏的极端情况。解密密钥授权可以是用户授权过程的一部分。授权访问解密密钥的用户可以看到未加密的数据，而其他人只能看到随机字符。

关系数据库视图可用于强制执行数据安全级别。视图可以基于数据值限制对某些行的访问，或对某些列的限制访问，从而限制对机密/受监管字段的访问。

2）监控用户身份验证和访问行为。

报告访问是合规性审计的基本要求。监视身份验证和访问行为提供了有关谁正在连接和访问信息资产的信息。监控还有助于发现值得调查的异常、意外或可疑的交易。通过这种方式，弥补了数据安全规划、设计和实现方面的缺陷。

要根据业务和法规要求进行仔细分析，以决定需要监控什么、监控多长时间以及决定在警报发生时要采取哪些行动。监控涉及多种活动，可具体到某些数据集、用户或角色。监控可用于验证数据完整性、配置或核心元数据。监控可在系统内实现，也可以跨依赖的异构系统实现。监控可以专注于特定权限，如下载大量数据或在非工作时间访问数据的能力。

监控可自动或手动执行，也可通过自动化和监督相结合的方式来执行。自动监控确实会给底层系统带来开销，并可能影响系统性能。活动的定期快照有助于理解趋势和对标比较。可能需要迭代配置变更来获得适当监控的最佳参数。

敏感或异常数据库事务的自动记录应该是任何数据库部署的一部分。缺乏自动化监控意味着严重的风险：

1）监管风险（Regulatory Risk）。数据库审计机制薄弱的组织将越来越多地发现他们与政府的监管要求相悖。金融服务领域的萨班斯－奥克斯利法案（SOX）和医疗保健部门的医疗保健信息可移植性和责任法案（HIPAA）只是两个典型的美国政府法规，其中有明确的数据库审计要求。

2）检测和恢复风险（Detection and Recovery Risk）。审计机制代表最后一道防线。如果攻击者绕过其他防御，则审计数据可以在事后识别是否存在违规行为。审计数据还可作为系统修复指南或将违规关联到特定用户。

3）管理和审计职责风险（Administrative and Audit Duties Risk）。具有数据库服务器管理访问权限的用户（无论该访问权限是合法还是恶意获得的），都可以关闭审计以隐藏欺诈活动。在理想的情况下，审计职责应独立于 DBA 和数据库服务器平台支持人员。

4）依赖于不适当的本地审计工具的风险（Risk of Reliance on Inadequate Native Audit Tools）。数据库软件平台通常集成基本审计功能，但它们往往受到很多限制或部署的阻碍。当用户通过 Web 应用程序（如 SAP、Oracle 电子商务套件或 PeopleSoft）访问数据库时，该机审计机制无法识别特定的用户身份，且所有用户活动都与 Web 应用程序账户名称相关联。因此，当该机审计日志显示欺诈性数据库事务时，缺乏指向对此负责的用户链接。

为了降低风险，可以部署实施基于网络的审计设备。虽然这可以解决与单机审计工具相关的大