数据库中控制特定用户数据可见性的技术分析

1. 引言：现代数据库中细粒度数据可见性控制的必要性

在当今的数字环境中，数据安全和隐私的重要性日益凸显。随着数据量的持续增长和数据敏感性的提高，组织面临着越来越严格的监管合规要求，例如通用数据保护条例（GDPR）、健康保险流通与责任法案（HIPAA）以及支付卡行业数据安全标准（PCI DSS）等 [1]。传统的对象级权限控制方法在满足细粒度数据可见性需求方面存在局限性。这些传统方法通常侧重于控制用户对数据库对象（如表或视图）的访问权限，而无法精确地控制用户在这些对象中可以看到哪些特定的数据行或列。为了应对这些挑战，并确保只有授权用户才能访问其需要的数据，数据库系统需要提供更精细的控制机制，以最大限度地降低数据泄露和违规风险。

本报告旨在深入分析主流数据库系统（包括 Oracle、PostgreSQL、SQL Server 和 MySQL）中用于控制特定用户数据可见性的各种技术。这些技术主要包括基于角色的访问控制（RBAC）、行级安全性（RLS）、列级权限以及数据脱敏。通过对这些技术的详细探讨，本报告旨在为数据库管理员、安全架构师和高级数据库开发人员提供全面的理解，以便他们能够有效地实施安全且符合法规的数据访问策略。

2. 数据库访问控制的核心原则：身份验证与授权

数据库安全的基础在于两个核心原则：身份验证和授权 [4]。

身份验证是验证尝试访问数据库的用户身份的过程。这通常通过多种方法实现，包括密码、安全令牌、生物识别扫描以及多因素身份验证（MFA）[1]。强大的身份验证机制至关重要，因为它是确保只有经过验证的用户才能进入系统的第一道防线 [1]。然而，仅凭身份验证不足以保护数据 [4]。

授权是在用户身份验证成功后，确定该用户被允许执行哪些操作以及可以访问哪些数据的过程 [4]。授权是身份验证之外的另一层安全保障，它根据预定义的策略来判断用户是否应该被允许访问特定的数据或执行他们尝试进行的事务 [4]。授权的核心原则之一是最小权限原则，即仅授予用户执行其工作职责所需的最低限度的访问权限 [4]。

身份验证和授权相互配合，共同确保数据库的安全性 [4]。身份验证确认了用户的身份，而授权则规定了该用户在系统中可以执行的操作和可以查看的数据范围。没有授权，即使是经过身份验证的用户也可能访问到他们不应该查看的敏感数据 [4]。因此，对于实现强大的数据可见性控制而言，有效的授权策略至关重要，这些策略需要超越简单的表级权限，以实现对数据更精细的控制 [4]。

3. 基础访问控制模型

为了实现数据可见性控制，各种数据库系统采用了不同的访问控制模型。以下是几种常见

的基础模型：

- 基于角色的访问控制 **(RBAC)**：RBAC 是一种广泛使用的访问控制技术，它提供了一种灵活且可扩展的方法来管理系统内的用户权限 [1]。在 RBAC 中，访问权限被分配给角色，而不是直接分配给个人用户 [9]。然后，根据用户的职位职责和要求，将用户分配给特定的角色 [9]。这种方法简化了用户权限的管理，因为它允许管理员定义具有相关权限的角色，并将用户分配给这些角色 [9]。RBAC 具有多项优势，包括提高安全性、简化管理以及更好地遵守安全策略和法规 [9]。通过实施 RBAC，组织可以确保用户仅能访问执行其工作职责所需的资源，从而降低未经授权访问或数据泄露的风险 [9]。此外，RBAC 使组织能够轻松适应人员和职位角色的变化 [9]。当用户的职位职责发生变化时，可以更新其角色，相关的权限将自动调整 [9]。这简化了管理用户访问权限的过程，并减少了管理开销 [9]。总而言之，RBAC 是一种适用于各种规模组织的有效访问控制技术 [4]。然而，对于控制表中特定数据的可见性，RBAC 可能不够精细 [10]。例如，虽然 RBAC 可以允许“销售”角色的所有用户访问“客户”表，但它本身并不能限制销售人员仅查看分配给他们特定区域的客户。这种更精细的控制通常需要行级安全性等技术来实现。
- 自主访问控制 **(DAC)**：DAC 是一种允许用户控制自己拥有的资源权限和访问权限的访问控制技术 [4]。在 DAC 中，资源所有者决定谁可以访问他们的资源以及可以执行哪些操作 [4]。通过 DAC，用户可以自行决定授予或撤销对其资源的访问权限，使其成为一种灵活的访问控制方法 [9]。这允许用户根据其特定需求和要求定制其资源的权限 [9]。DAC 的主要优点之一是它赋予用户对其自身数据和资源的更多控制权 [9]。这在用户协作并需要共享资源，同时仍然保持对其访问权限的控制的情况下尤其有用 [9]。然而，DAC 的一个挑战是它可能导致复杂且分散的访问控制系统 [9]。由于多个用户控制着自己的资源，因此可能难以强制执行一致的安全策略并确保资源得到充分保护 [9]。为了应对这些挑战，组织可以实施额外的访问控制技术，例如 RBAC 或 MAC，以补充 DAC 并提供更全面的安全框架 [9]。总的来说，自主访问控制是一种有价值的访问控制技术，它允许用户控制自己的资源，提供灵活性并赋予用户权力，但也需要仔细的管理和监督以确保适当的安全措施到位 [9]。
- 强制访问控制 **(MAC)**：MAC 是一种由中央机构根据安全许可级别来管理访问权限的访问控制模型 [1]。它是一种非自主模型，意味着最终用户无法控制任何提供权限的设置 [10]。MAC 通常与信息保密性（如 Bell-LaPadula 模型）和信息完整性（如 Biba 模型）相关联 [10]。在 MAC 中，系统中的每个资源（如文件或数据库记录）都被分配了一个安全标签，并且只有具有相应安全许可级别的用户才能访问这些资源 [1]。MAC 广泛应用于对信息安全要求极高的环境，例如政府和军事领域 [1]。在这种模型下，访问决策不是由数据所有者或用户自行决定的，而是由中央策略强制执行的，从而提供了非常强的安全性 [10]。然而，MAC 的严格性也使其在商业应用中不如其他模型灵活。
- 基于属性的访问控制 **(ABAC)**：ABAC 是一种更精细的访问控制方法，它根据用户的属性、资源的属性以及环境的属性来授予访问权限 [1]。在这种动态方法中，系统会对用户的属性（例如角色、部门、安全级别）、资源的属性（例如数据敏感度、创建者）以及环境的属性（例如时间、位置）进行比较评估，以做出访问决策 [1]。ABAC 提供了比 RBAC

更精确的控制[1]，因为它能够基于更广泛的因素来定义访问策略[4]。例如，可以制定策略，允许特定角色的用户在特定时间范围内，从特定位置访问具有特定敏感度标签的数据[4]。ABAC 的灵活性和精细度使其成为复杂安全需求的理想选择。

4. 行级安全性 **(RLS)** 用于数据可见性控制

行级安全性（RLS）是一种允许数据库管理员定义策略以控制特定用户角色如何显示和操作数据表中特定行的安全特性。RLS 本质上是您可以应用于 PostgreSQL 数据库表的附加过滤器[11]。当用户尝试对表执行操作时，此过滤器将在查询条件或其他过滤之前应用，并根据您的安全策略缩小或拒绝数据[11]。

- **Oracle** 行级安全性
  - 虚拟私有数据库 **(VPD)**：Oracle 虚拟私有数据库 (VPD) 通过基于用户上下文动态地向 SQL 查询添加 WHERE 子句来控制行级数据的访问[12]。VPD 策略通常使用 PL/SQL 函数定义[14]。这种方法的主要优点是它对应用程序透明，并且安全逻辑集中化[14]。当用户运行查询时，VPD 会自动应用相应的过滤器，确保用户只能看到他们有权访问的数据行。例如，一个销售代表可能只能看到分配给他们的客户数据。然而，VPD 的一个潜在缺点是谓词评估可能会带来性能开销[14]。因此，在设计和实施 VPD 策略时，需要仔细考虑其复杂性和对性能的潜在影响。Oracle Analytics Server 为语义模型物理层中的每个数据库提供了一个虚拟私有数据库 (VPD) 数据源属性。启用虚拟私有数据库 (VPD) 选项后，可以防止用户之间共享查询缓存，因为每个用户只需要检索他们有权查询的数据[20]。在物理数据库的高级属性中选择“虚拟私有数据库”字段可确保 Oracle Analytics 查询引擎保护每个用户的缓存条目[20]。Oracle Analytics 查询引擎会将安全敏感变量列表与每个潜在的缓存命中进行匹配[20]。只有包含并匹配所有安全敏感变量的缓存条目才会发生缓存命中[20]。
  - 标签安全性 **(OLS)**：Oracle 标签安全性 (OLS) 通过为数据行和用户分配基于敏感度级别的安全标签来提供行级安全性[21]。标签由级别、部门和组组成[21]。OLS 会自动比较数据标签和用户权限，以确定访问权限[21]。当没有自然数据指示访问要求时，OLS 非常有用[21]。例如，在具有分层安全要求的环境中，可以将高度敏感的数据标记为“高度敏感”，而不太敏感的数据标记为“敏感”。然后，OLS 确保只有具有相应权限级别的用户才能访问这些数据[21]。LBACSYS 账户管理 Oracle 标签安全策略，通过集中管理这些策略并降低未经授权修改的风险，从而提供额外的安全层[21]。Oracle 标签安全性还为行级安全性提供了预定义的 PL/SQL 包[21]。
- **PostgreSQL** 行级安全性：PostgreSQL 的行级安全性 (RLS) 通过使用 ALTER TABLE ENABLE ROW LEVEL SECURITY 命令在表上启用[11]。然后，使用带有 USING 和 WITH CHECK 子句的 CREATE POLICY 命令创建策略[11]。策略可以是允许性的（使用 OR 组合）或限制性的（使用 AND 组合）[22]。策略可以特定于命令和角色[22]。例如，可以创建一个策略，允许只有特定部门的成员才能查看该部门的数据行。PostgreSQL 的 RLS 功能为控制行级数据访问提供了一种灵活而强大的机制。然而，在涉及多个受 RLS 保护的表的复杂连接场景中，性能优化需要特别注意[19]。要启用 PostgreSQL 中的行级安全

性 (RLS)，需要执行以下步骤：首先，使用命令 ALTER TABLE your_table_name ENABLE ROW LEVEL SECURITY; 在表上启用行级安全性 [22]。其次，创建行安全策略 [22]。您可以使用 CREATE POLICY 命令来执行此操作 [22]。策略可以使用 USING 子句定义条件，以确定哪些行对指定角色可见 [22]。对于 INSERT 和 UPDATE 命令，您可以使用 WITH CHECK 子句添加一个额外的条件，以确保新行或修改后的行满足特定要求 [22]。

- **SQL Server** 行级安全性：SQL Server 行级安全性 (RLS) 通过使用安全谓词（内联表值函数）和安全策略来实现 [29]。RLS 支持两种类型的安全谓词：筛选谓词（用于 SELECT、UPDATE 和 DELETE 操作的静默筛选）和阻止谓词（用于显式阻止违反谓词的 INSERT、UPDATE 和 DELETE 操作）[29]。安全策略将谓词绑定到表 [29]。例如，可以创建一个安全策略，使用一个函数来检查用户的 ID 是否与订单表中的 CustomerID 匹配，从而确保用户只能看到他们自己的订单。与视图类似，RLS 的性能取决于谓词的复杂性和索引的使用情况 [36]。要实现 SQL Server 中的行级安全性 (RLS)，需要执行以下步骤：首先，创建将需要数据访问权限的指定用户 [30]。其次，在 SQL 中创建一个内联表值函数 [30]。此函数将包含要实施 RLS 的表的筛选谓词 [30]。最后一步是为该表创建一个安全策略，并将上述内联表值函数提供给它 [30]。
- **MySQL** 行级安全性：MySQL 在 8.0 版本中引入了行级安全性 (RLS) [42]。MySQL 中的 RLS 通常通过使用视图和函数进行行过滤来实现 [42]。可以创建带有基于 CURRENT_USER() 或其他上下文的 WHERE 子句的视图 [43]。还可以创建函数以返回策略的筛选条件 [42]。RLS 提供了基于条件或用户属性的细粒度访问控制 [42]。例如，可以创建一个视图，只显示当前用户拥有的任务。由于 MySQL 中的 RLS 主要通过视图的抽象层实现，因此与直接表访问相比，可能会引入一些性能开销 [43]。要使用视图实现 MySQL 中的行级访问控制，可以创建一个视图，该视图仅包含要向用户显示的列，然后向用户提供视图名称而不是表名称 [43]。这可以防止用户查看或修改视图中未包含的列中的数据 [43]。对于更复杂的情况，可能需要创建一个授权映射以进行连接，或者使用像 Satori 这样的产品来简化访问控制 [43]。

5. 列级权限用于细粒度访问

列级权限允许数据库管理员限制用户对表中特定列的访问，从而实现比行级安全性更细粒度的控制。

- **PostgreSQL** 列级权限：PostgreSQL 允许使用 GRANT 命令授予对特定列的 SELECT、INSERT、UPDATE 和 REFERENCES 权限 [46]。可以使用 REVOKE 命令撤销这些权限 [46]。此外，还可以使用视图来限制列的可见性 [48]。需要注意的是，当用户的列访问受到限制时，使用 SELECT * 可能会导致错误 [47]。例如，可以授予一个“支持代理”角色对“客户”表的“customer_name”和“email”列的 SELECT 权限，但拒绝访问“credit_card_number”列。要授予 PostgreSQL 中特定列的权限，可以使用 GRANT 命令 [46]。例如，要授予角色 joe 对表 accounts 中 name 列的 SELECT 权限，可以使用命令 GRANT SELECT (name) ON accounts TO joe; [46]。可以使用类似的语法授予 INSERT、UPDATE 和 REFERENCES 权限 [46]。要撤销权限，可以使用 REVOKE 命令，例

如 REVOKE SELECT (name) ON accounts FROM joe; [46]。

- **SQL Server** 列级权限：SQL Server 允许使用 GRANT 命令授予对特定列的 SELECT、UPDATE 和 REFERENCES 权限 [57]。可以使用 DENY 命令拒绝权限 [57]。除了传统的权限控制，SQL Server 还提供了列级加密（使用 Always Encrypted [61]）和动态数据脱敏（用于在查询结果中屏蔽列数据 [64]）。例如，可以使用 GRANT SELECT (name, email) ON customers TO SupportRole 来允许支持代理查看客户姓名和电子邮件。对于“credit_card_number”列，可以使用 Always Encrypted 来保护数据在存储和传输过程中的安全。要授予 SQL Server 中特定列的权限，可以使用 GRANT 语句 [57]。例如，要授予用户 exampleuser 对 mydata.table 中 column1 和 column2 的 SELECT 权限，可以使用命令 GRANT SELECT ON mydata.table (column1, column2) TO exampleuser; GO [57]。可以使用 DENY 语句拒绝权限，例如 DENY SELECT ON mydata.table (column3) TO exampleuser; GO [57]。
- **MySQL** 列级权限：MySQL 允许使用 GRANT 命令授予对特定列的 SELECT、INSERT、UPDATE 和 REFERENCES 权限 [75]。可以使用 REVOKE 命令撤销这些权限 [75]。与 PostgreSQL 和 SQL Server 类似，可以使用视图来限制列的可见性 [80]。此外，MySQL 还提供了企业版数据脱敏功能（MySQL Enterprise Data Masking [3]）和开源的 Percona 数据脱敏插件（Percona Data Masking Plugin [84]），用于更高级地屏蔽敏感列数据。例如，可以使用 GRANT SELECT (product_name, description) ON products TO PublicRole 来允许公众访问产品信息，同时限制对成本和利润等敏感信息的访问。对于非生产环境，可以使用 MySQL Enterprise Data Masking 将实际的客户电子邮件地址替换为匿名值。要在 MySQL 中授予特定列的权限，可以使用 GRANT 语句 [75]。例如，要授予用户 john 对表 employees 中 salary 列的 SELECT 权限，可以使用命令 GRANT SELECT (salary) ON employees TO 'john'@'localhost'; [75]。可以使用 REVOKE 语句撤销权限 [75]。

6. 非生产环境的数据脱敏技术

数据脱敏是一种通过替换敏感信息来创建数据的非生产副本来保护敏感信息的技术。脱敏后的数据对于测试、开发和分析等非生产用途仍然有用，但不再包含真实的敏感信息。

- **Oracle** 数据脱敏：Oracle 数据脱敏提供了一套全面的工具，用于在非生产环境中匿名化敏感数据 [89]。它提供了各种脱敏格式，包括混淆、替换、加密和随机数据生成 [89]。实施步骤通常包括识别敏感数据、定义脱敏格式、创建脱敏定义、生成和应用脚本 [89]。在实施过程中需要考虑性能、引用完整性和数据可用性 [89]。例如，为了创建一个测试环境，可以克隆生产数据库，然后使用 Oracle 数据脱敏将所有实际客户姓名替换为随机生成的姓名，同时确保客户及其订单之间的关系保持不变。
- **MySQL** 数据脱敏：MySQL 提供了静态和动态数据脱敏方法 [3]。可以使用原生 MySQL 函数（例如 CONCAT、SUBSTRING）进行基本脱敏 [3]。MySQL 企业版数据脱敏提供了内置函数，用于选择性脱敏、随机替换和字典替换 [82]。Percona 数据脱敏插件是一个开源替代方案，提供通用和专用脱敏函数 [84]。DataSunrise 等工具也提供了简化的动态数据

脱敏功能 [3]。例如，为了进行测试，可以使用 MySQL 企业版数据脱敏来屏蔽克隆数据库中的信用卡号，将除最后四位数字外的所有数字替换为“X”。

- **SQL Server** 数据脱敏：SQL Server 提供了静态数据脱敏功能，用于创建清理过的数据库副本 [67]，以及动态数据脱敏 (DDM)，用于实时屏蔽查询结果 [64]。DDM 提供了多种屏蔽函数，包括默认、电子邮件、随机、部分和日期时间屏蔽 [66]。静态脱敏适用于创建永久匿名副本以供非生产使用，而动态脱敏则允许实时混淆查询结果中的敏感数据，从而在安全性和数据可用性之间取得平衡 [66]。例如，可以使用 SQL Server 动态数据脱敏来屏蔽报告数据库中客户的电子邮件地址，仅显示第一个字母和域名，而实际数据在底层表中保持不变。

7. 高级数据保护策略：加密和数据库活动监控

除了访问控制技术外，加密和数据库活动监控 (DAM) 也是保护数据库中数据可见性的重要策略。

- 加密：加密是一种通过将数据转换为只有拥有密钥的人才能读取的代码来保护数据的基本方法 [1]。这包括加密存储中的数据（静态数据）和传输中的数据（动态数据）[1]。Oracle、SQL Server 和 PostgreSQL 都支持透明数据加密 (TDE)，用于在磁盘上加密整个数据库 [63]。此外，还提供了列级加密选项，例如 SQL Server 中的 Always Encrypted [61] 和 PostgreSQL 中的 pgcrypto [50]，允许加密特定的敏感字段 [50]。有效的密钥管理对于确保加密数据的安全至关重要 [2]。
- 数据库活动监控 **(DAM)**：数据库活动监控 (DAM) 涉及监控和审计数据库的访问和活动 [1]。这包括跟踪用户执行的操作 [117]，识别潜在的漏洞并确保访问权限适当 [4]，以及检测可疑行为并响应安全事件 [1]。通过持续监控数据库活动，组织可以及时发现并应对未经授权的访问尝试或可疑活动 [1]。DAM 还能够提供对数据库使用情况的可见性，帮助组织遵守审计要求并改进其安全态势 [4]。

8. 比较分析：不同技术的性能、安全性与可管理性

下表对不同数据库系统中用于控制数据可见性的各种技术进行了比较分析：

技术	数据库系统	性能影响	安全级别	可管理性	用例	主要特点
行级安全性 **(RLS)**	Oracle (VPD, OLS)	中到高	高	中到高	需要基于用户上下文限制数据行访问的场景，如多租户应用、按部门或区域划分的数	动态查询修改（VPD），基于标签的访问控制（OLS），细粒度策略定义。

					据访问。	
	PostgreSQL	中	高	中	同 Oracle RLS。	使用 CREATE POLICY 定义灵活的访问规则，支持允许性和限制性策略。
	SQL Server	中	高	中	同 Oracle RLS。	使用安全谓词（表值函数）和安全策略，支持筛选和阻止谓词。
	MySQL	低到中	中	低到中	同 Oracle RLS，通常通过视图和函数实现。	基于 CURRENT_USER() 的视图过滤，使用函数返回筛选条件。
列级权限	PostgreSQL	低	中	低	需要限制用户对表中特定列的查看或修改权限的场景，如隐藏敏感信息（如薪资）。	使用 GRANT 和 REVOKE 控制列级 SELECT、INSERT、UPDATE、REFERENCES 权限，使用视图限制列可见性。
	SQL Server	低到高	中到高	中	同 PostgreSQL 列级权限，以及需要列级加密	使用 GRANT 和 DENY 控制列权限，Always

					或动态屏蔽的场景。	Encrypted 提供列级加密，动态数据脱敏实时屏蔽列数据。
	MySQL	低	中	低	同 PostgreSQL 列级权限，以及需要数据脱敏的场景。	使用 GRANT 和 REVOKE 控制列权限，使用视图限制列可见性，MySQL 企业版提供数据脱敏功能。
数据脱敏	Oracle	中到高	高	中	需要在非生产环境中创建匿名化数据的场景，如测试、开发和分析。	提供广泛的脱敏格式，支持静态和动态脱敏，可维护引用完整性。
	PostgreSQL	中	中到高	低到中	同 Oracle 数据脱敏，通常通过脚本或内置函数实现。	批量数据脱敏技术，可使用函数和触发器，但原生功能有限。
	SQL Server	中	中到高	中	同 Oracle 数据脱敏，支持静态和动态脱敏。	提供多种动态数据脱敏函数，静态脱敏用于创建永久匿名副本。
	MySQL	低到中	中	低到中	同 Oracle 数据脱敏，支持静态	原生函数提供基本脱敏，企业版和

					和动态脱敏。	Percona 插件提供更高级功能。

9. 实施数据库数据可见性控制的最佳实践

实施有效的数据可见性控制需要采用多方面的方法，结合多种技术并遵守安全最佳实践：

- 采纳最小权限原则：仅授予用户执行其工作职责所需的最低限度的访问权限 [4]。
- 实施强大的身份验证机制：使用强密码策略和多因素身份验证等方法来验证用户身份 [1]。
- 利用 **RBAC** 简化用户权限管理：通过将权限分配给角色而不是直接分配给用户来简化管理 [9]。
- 采用 **RLS** 对数据行访问进行细粒度控制：使用 VPD、OLS、安全策略或视图和函数等技术来限制用户可以查看或修改的数据行 [14]。
- 使用列级权限限制对敏感属性的访问：使用 GRANT 和 REVOKE 语句来控制用户对表中特定列的权限 [46]。
- 为非生产环境实施数据脱敏以保护敏感信息：使用静态或动态数据脱敏技术来替换测试和开发环境中的敏感数据 [3]。
- 将访问控制技术与加密相结合以实现纵深防御：使用 TDE 和列级加密来保护静态数据和传输中的数据 [9]。
- 定期审计和监控数据库活动：跟踪用户操作和访问模式以检测可疑行为和潜在的安全漏洞 [1]。
- 保持访问控制策略更新以反映组织变化：随着人员和职责的变化，定期审查和更新权限和策略 [1]。
- 对所有数据利益干系人进行数据安全最佳实践培训：提高员工对数据安全重要性和常见威胁的认识 [5]。
- 彻底测试和验证访问控制实施：在生产环境中部署之前，确保所有访问控制机制按预期工作 [99]。
- 考虑使用身份和访问管理 **(IAM)** 解决方案进行集中控制：利用 IAM 工具来集中管理用户身份、访问权限和身份验证机制 [1]。
- 将数据库服务器与 **Web** 服务器分离以最小化攻击面：通过隔离数据库服务器来减少潜在的攻击入口 [7]。
- 通过加强密码保护和访问控制来加固数据库：实施强密码策略并限制不必要的访问权限 [7]。

实施有效的数据可见性控制需要一个多层次的安全策略，该策略结合了各种技术并遵循了安全最佳实践 [1]。仅仅实施 RLS 可能是不够的，组织还应确保强大的身份验证、应用最小权限原则，并考虑对非生产系统进行数据脱敏，以构建强大的安全态势。

10. 结论：为您的特定需求选择最佳方法

控制数据可见性的技术多种多样，组织应根据其特定需求和环境选择最合适的方法。在选择技术时，需要考虑的关键因素包括数据的敏感性、适用的法规要求、对数据库性能的潜在影响、管理复杂性以及所使用的特定数据库系统。通常，结合使用不同的技术可以提供最全面的解决方案。例如，组织可能选择使用 RBAC 来管理广泛的角色级权限，使用 RLS 来实现对特定数据行的细粒度控制，并对非生产环境中的敏感数据应用数据脱敏技术。

持续监控和调整安全策略对于维护安全且合规的数据库环境至关重要。随着组织的发展和安全威胁的演变，需要定期审查和更新数据可见性控制措施，以确保其持续有效。最终，实施细粒度的数据可见性控制对于维护安全且合规的数据库环境起着至关重要的作用。没有一种通用的解决方案，最佳方法取决于对组织特定需求、数据库系统功能以及安全性、性能和可管理性之间权衡的仔细评估 [18]。例如，一家小型初创公司最初可能会发现 RBAC 和基本的 RLS 就足够了，而一家处理高度敏感数据的大型金融机构则可能需要实施 RBAC、RLS、列级加密和数据脱敏的组合，并进行强大的监控和审计。

Works cited

1. Database Access Control: Strategies for Protecting Sensitive Information - Identity Fusion, accessed April 25, 2025, https://www.identityfusion.com/blog/database-access-control-strategies-for-protecting-sensitive-information
2. Effective Database Security Solutions - Oracle, accessed April 25, 2025, https://www.oracle.com/security/database-security/
3. Data Masking in MySQL: Enhanced Security & Best Practices - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/knowledge-center/data-masking-in-mysql/
4. What is Access Control in Database Security? Learn more - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/professional-info/what-is-access-control/
5. What Is Data Access Control? A Quick Guide | Fortra's Digital Guardian, accessed April 25, 2025, https://www.digitalguardian.com/blog/what-data-access-control-quick-guide
6. Access Control 101: A Comprehensive Guide to Database Access Control - Satori, accessed April 25, 2025, https://satoricyber.com/access-control/access-control-101-a-comprehensive-guide-to-database-access-control/
7. 7 Database Security Best Practices: Database Security Guide - eSecurity Planet, accessed April 25, 2025, https://www.esecurityplanet.com/networks/database-security-best-practices/
8. Best Practices for Securing Your PostgreSQL Database - Percona, accessed April 25, 2025, https://www.percona.com/blog/postgresql-database-security-what-you-need-to

-know/
9. Introduction to Access Control Techniques - Forest Admin, accessed April 25, 2025, https://www.forestadmin.com/blog/access-control-techniques/
10. Access Control Models and Methods | Types of Access Control - Delinea, accessed April 25, 2025, https://delinea.com/blog/access-control-models-methods
11. PostgreSQL Row Level Security (RLS): Basics and Examples - Satori Cyber, accessed April 25, 2025, https://satoricyber.com/postgres-security/postgres-row-level-security/
12. Practical Guide to Oracle Access Control for Secure Data Management - Surety Systems, accessed April 25, 2025, https://www.suretysystems.com/insights/practical-guide-to-oracle-access-control-for-secure-data-management/
13. Fine-grained Access Control (FGAC) vs. Row Level Security (R... - Ask TOM, accessed April 25, 2025, https://asktom.oracle.com/ords/f?p=100:11:0::::P11_QUESTION_ID:9532605800346121507
14. Introduction to Row Level Security. Examining access rights differentiation systems implemented in Oracle и PostgreSQL - HackMag, accessed April 25, 2025, https://hackmag.com/security/row-level-security/
15. Oracle row level security by column value, not by user id - Stack Overflow, accessed April 25, 2025, https://stackoverflow.com/questions/66403953/oracle-row-level-security-by-column-value-not-by-user-id
16. Oracle row level security setup? - Database Administrators Stack Exchange, accessed April 25, 2025, https://dba.stackexchange.com/questions/78357/oracle-row-level-security-setup
17. Oracle data masking: hide information from users with an easy-to-use VPD - Pretius, accessed April 25, 2025, https://pretius.com/blog/oracle-data-masking/
18. Best Practices For Implementing Row-Level Security In Oracle Analytics, accessed April 25, 2025, https://blogs.oracle.com/analytics/post/best-practices-for-implementing-rowlevel-security-in-oracle-analytics-1
19. Row level security(RLS) performance is significantly slower in postgres. - Stack Overflow, accessed April 25, 2025, https://stackoverflow.com/questions/41186880/row-level-securityrls-performance-is-significantly-slower-in-postgres
20. Work With Row-Level Security - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/en/middleware/bi/analytics-server/datamodel-oas/work-row-level-security.html
21. Enforcing Row-Level Security with Oracle Label Security, accessed April 25, 2025, https://docs.oracle.com/en/database/oracle/oracle-database/12.2/tdpsg/enforcing-row-level-security-with-oracle-label-security.html
22. Documentation: 17: 5.9. Row Security Policies - PostgreSQL, accessed April 25, 2025, https://www.postgresql.org/docs/current/ddl-rowsecurity.html

23. PostgreSQL Row-Level Security - Neon, accessed April 25, 2025, https://neon.tech/postgresql/postgresql-administration/postgresql-row-level-security
24. Hands-on with PostgreSQL Authorization - Part 2 - Row-Level Security - Tangram Vision, accessed April 25, 2025, https://www.tangramvision.com/blog/hands-on-with-postgresql-authorization-part-2-row-level-security
25. An introduction to Postgres Row Level Security (RLS) - DEV Community, accessed April 25, 2025, https://dev.to/brianmmdev/an-introduction-to-postgres-row-level-security-rls-306k
26. A Friendly Introduction to RLS Policies in Postgres - Cord, accessed April 25, 2025, https://cord.com/techhub/architecture/articles/a-friendly-introduction-to-rls-policies-in-postgre
27. Documentation: 17: CREATE POLICY - PostgreSQL, accessed April 25, 2025, https://www.postgresql.org/docs/current/sql-createpolicy.html
28. Row Level Security | Tutorials | Crunchy Data, accessed April 25, 2025, https://www.crunchydata.com/developers/playground/row-level-security
29. Row-level security - SQL Server | Microsoft Learn, accessed April 25, 2025, https://learn.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16
30. Introduction to Row-Level Security in SQL Server - SQLShack, accessed April 25, 2025, https://www.sqlshack.com/introduction-to-row-level-security-in-sql-server/
31. SQL Server Row Level Security Deep Dive. Part 1 - Introduction and Use Cases, accessed April 25, 2025, https://www.red-gate.com/simple-talk/blogs/sql-server-row-level-security-introduction/
32. Implementing Row Level Security on SQL Server - YouTube, accessed April 25, 2025, https://www.youtube.com/watch?v=q0e_0Iw23F0
33. Row-level security in SQL server - Microsoft Q&A, accessed April 25, 2025, https://learn.microsoft.com/en-us/answers/questions/1659829/row-level-security-in-sql-server
34. Am I abusing Row Level Security? (RLS) - DBA Stack Exchange, accessed April 25, 2025, https://dba.stackexchange.com/questions/329320/am-i-abusing-row-level-security-rls
35. Row-Level Security and Dynamic Data Masking - Skillzcafe, accessed April 25, 2025, https://skillzcafe.com/blog/microsoft/sql-server/row-level-security-and-dynamic-data-masking
36. Limiting access to data using Row-Level Security - Microsoft SQL Server Blog, accessed April 25, 2025, https://www.microsoft.com/en-us/sql-server/blog/2016/01/21/limiting-access-to-data-using-row-level-security/

37. What are the Pros and cons of row-level security Microsoft SQL Server - JanBask Training, accessed April 25, 2025, https://www.janbasktraining.com/community/sql-server/what-are-the-pros-and-cons-of-row-level-security-microsoft-sql-server1
38. What are the performance impact will happen when we implement RLS for azure sql database - Learn Microsoft, accessed April 25, 2025, https://learn.microsoft.com/en-us/answers/questions/1078822/what-are-the-performance-impact-will-happen-when-w
39. Row-level security based on IS_MEMBER function - Stack Overflow, accessed April 25, 2025, https://stackoverflow.com/questions/60748489/row-level-security-based-on-is-member-function
40. SQL Server Row Level Security Deep Dive. Part 3 – Performance and Troubleshooting, accessed April 25, 2025, https://www.red-gate.com/simple-talk/blogs/sql-server-rls-performance-and-troubleshooting/
41. Should I use Row Level Security : r/SQLServer - Reddit, accessed April 25, 2025, https://www.reddit.com/r/SQLServer/comments/hzuqvl/should_i_use_row_level_security/
42. MySQL Row Level Security: Controlling Access to Sensitive Data - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/knowledge-center/mysql-row-level-security/
43. MySQL Row-Level Security - Satori, accessed April 25, 2025, https://satoricyber.com/mysql-security/mysql-row-level-security/
44. Implementing row level security in MySQL - SQL Maestro Group, accessed April 25, 2025, https://www.sqlmaestro.com/resources/all/row_level_security_mysql/
45. Webapp: Mysql: Row level security. Pro/cons? A better way to do this? - Stack Overflow, accessed April 25, 2025, https://stackoverflow.com/questions/8296821/webapp-mysql-row-level-security-pro-cons-a-better-way-to-do-this
46. Documentation: 17: 5.8. Privileges - PostgreSQL, accessed April 25, 2025, https://www.postgresql.org/docs/current/ddl-priv.html
47. Column Level Security | Supabase Docs, accessed April 25, 2025, https://supabase.com/docs/guides/database/postgres/column-level-security
48. Column and row level security in the Arenadata Postgres cluster ..., accessed April 25, 2025, https://docs.arenadata.io/en/ADPG/current/how-to/security/column-security.html
49. Documentation: 9.1: GRANT - PostgreSQL, accessed April 25, 2025, https://www.postgresql.org/docs/9.1/sql-grant.html
50. How to implement Column and Row level security in PostgreSQL - EDB, accessed April 25, 2025, https://www.enterprisedb.com/postgres-tutorials/how-implement-column-and-row-level-security-postgresql
51. How to set column level permissions for specific users on a Postgres Database already in production without using views? - Stack Overflow, accessed April 25,

2025, https://stackoverflow.com/questions/77357420/how-to-set-column-level-permissions-for-specific-users-on-a-postgres-database-al
52. Postgres Column Level Security - DBA Stack Exchange, accessed April 25, 2025, https://dba.stackexchange.com/questions/239577/postgres-column-level-security
53. Learn how to manage security in PostgreSQL [Tutorial] - Packt, accessed April 25, 2025, https://www.packtpub.com/en-us/learning/how-to-tutorials/learn-how-to-manage-security-in-postgresql-tutorial
54. Explicitly granting permissions to update the sequence for a serial column necessary?, accessed April 25, 2025, https://dba.stackexchange.com/questions/71528/explicitly-granting-permissions-to-update-the-sequence-for-a-serial-column-neces
55. [Postgres][Question] Grant column level permissions : r/PostgreSQL - Reddit, accessed April 25, 2025, https://www.reddit.com/r/PostgreSQL/comments/bbxnj2/postgresquestion_grant_column_level_permissions/
56. Flexible column-level security : r/PostgreSQL - Reddit, accessed April 25, 2025, https://www.reddit.com/r/PostgreSQL/comments/w925kj/flexible_columnlevel_security/
57. Column Level Security in SQL Server: Implementation Guide - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/knowledge-center/column-level-security-in-sql-server/
58. SQL Server Column Level Permissions - A Learning HUB for Database Administration, accessed April 25, 2025, https://www.sqldbahub.com/p/sql-server-column-level-permissions.html
59. How to Implement Row and Column Level Security in SQL Server - Netwrix Blog, accessed April 25, 2025, https://blog.netwrix.com/2019/06/27/how-to-implement-row-and-column-level-security-in-sql-server/
60. sql server - Request granted select permissions on column level for MSSQL - Stack Overflow, accessed April 25, 2025, https://stackoverflow.com/questions/75950041/request-granted-select-permissions-on-column-level-for-mssql
61. Always Encrypted - SQL Server | Microsoft Learn, accessed April 25, 2025, https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver16
62. SQL server Column level security - Microsoft Q&A, accessed April 25, 2025, https://learn.microsoft.com/en-us/answers/questions/279369/sql-server-column-level-security
63. 6 Practical Data Protection Features in SQL Server (Pros & Cons) - Core BTS, accessed April 25, 2025, https://corebts.com/blog/6-practical-sql-server-data-features/

64. SQL Server security best practices - Learn Microsoft, accessed April 25, 2025, https://learn.microsoft.com/en-us/sql/relational-databases/security/sql-server-security-best-practices?view=sql-server-ver16
65. Column-Level Encryption: Implementation & Benefits - Piiano, accessed April 25, 2025, https://www.piiano.com/blog/column-level-encryption
66. Dynamic data masking - SQL Server | Microsoft Learn, accessed April 25, 2025, https://learn.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver16
67. SQL Server Data Masking: Static vs Dynamic - Satori, accessed April 25, 2025, https://satoricyber.com/sql-server-security/sql-server-data-masking/
68. Ultimate Guide to Data Masking in SQL Server | Blog | Tonic.ai, accessed April 25, 2025, https://www.tonic.ai/blog/the-ultimate-guide-to-data-masking-in-sql-server
69. Data Masking in SQL Server - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/knowledge-center/data-masking-in-sql-server/
70. Ways of Dynamic Data Masking SQL Server Fields - GeoPITS, accessed April 25, 2025, https://www.geopits.com/blog/dynamic-data-masking.html
71. Understanding SQL Server Dynamic Data Masking - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/knowledge-center/sql-server-dynamic-data-masking/
72. Data Masking: Static vs Dynamic - DZone, accessed April 25, 2025, https://dzone.com/articles/data-masking-static-vs-dynamic
73. Dynamic Data Masking performance overhead - DBA Stack Exchange, accessed April 25, 2025, https://dba.stackexchange.com/questions/182870/dynamic-data-masking-performance-overhead
74. SQL Server Column Level Security: 3 Ways to Protect Columns - Satori Cyber, accessed April 25, 2025, https://satoricyber.com/sql-server-security/sql-server-column-level-security/
75. MySQL 8.4 Reference Manual :: 8.2.3 Grant Tables - MySQL, accessed April 25, 2025, https://dev.mysql.com/doc/refman/8.0/en/grant-tables.html
76. Granting MySQL Permissions: Table and Column Levels - Atlassian, accessed April 25, 2025, https://www.atlassian.com/data/admin/grant-permissions-for-mysql
77. Tag Archives: How To Grant User Privileges at the Column Level? on MySQL - Bright DBA, accessed April 25, 2025, https://www.br8dba.com/tag/how-to-grant-user-privileges-at-the-column-level-on-mysql/
78. How to provide Column Level Permission to user on a table in MySQL Server - YouTube, accessed April 25, 2025, https://www.youtube.com/watch?v=lcMKx-IEVks
79. MySQL Grant and Revoke Privileges: A Comprehensive Guide with Examples - Devart, accessed April 25, 2025, https://www.devart.com/dbforge/mysql/studio/mysql-grant-revoke-privileges.html

80. 4.3 Grant Tables - Security in MySQL, accessed April 25, 2025, https://dev.mysql.com/doc/mysql-security-excerpt/8.0/en/grant-tables.html
81. Mastering MySQL Views: A Comprehensive Guide - RisingWave, accessed April 25, 2025, https://risingwave.com/blog/mastering-mysql-views-a-comprehensive-guide/
82. MySQL 5.7 Reference Manual :: 6.5.3 Using MySQL ... - MySQL, accessed April 25, 2025, https://dev.mysql.com/doc/refman/5.7/en/data-masking-usage.html
83. MySQL Enterprise Masking and De-identification - MySQL, accessed April 25, 2025, https://www.mysql.com/products/enterprise/masking.html
84. Data Masking for MySQL Databases - Bytebase, accessed April 25, 2025, https://www.bytebase.com/blog/mysql-data-masking/
85. 8.5 MySQL Enterprise Data Masking and De-Identification, accessed April 25, 2025, https://dev.mysql.com/doc/refman/8.4/en/data-masking.html
86. Data Masking in MySQL, accessed April 25, 2025, https://dev.mysql.com/blog-archive/data-masking-in-mysql/
87. Protecting Sensitive Data with Dynamic Data Masking in MySQL - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/knowledge-center/dynamic-data-masking-in-mysql/
88. Data masking plugin functions - Percona Server for MySQL, accessed April 25, 2025, https://docs.percona.com/percona-server/8.0/data-masking-plugin-functions.html
89. Data Masking - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/en/database/oracle/oracle-database/19/dmksb/data_masking.html
90. Managing Oracle Data Masking Policies - Commvault Documentation, accessed April 25, 2025, https://documentation.commvault.com/11.20/managing_oracle_data_masking_policies.html
91. Data Masking - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/en-us/iaas/Content/fusion-applications/manage-security-data-masking.htm
92. Data Masking - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/iaas/Content/applications-manager/manage-apps-security-data-masking.htm
93. Data Masking Overview - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/en/cloud/paas/data-safe/udscs/data-masking-overview.html
94. Data Masking in Oracle - DataSunrise, accessed April 25, 2025, https://www.datasunrise.com/knowledge-center/data-masking-in-oracle/
95. mask-data — OCI CLI Command Reference 3.54.0 documentation, accessed April 25, 2025, https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/tools/oci-cli/3.49.2/oci_cli_docs/cmdref/data-safe/masking-policy/mask-data.html

96. 1 Introduction to Oracle Data Masking and Subsetting, accessed April 25, 2025, https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dmksb/intro.html
97. Oracle Data Masking and Subsetting, accessed April 25, 2025, https://www.oracle.com/security/database-security/data-masking/
98. Data Masking and Subsetting Guide - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dmksb/oracle-data-masking-and-subsetting-users-guide.pdf
99. Oracle Data Masking: A Basic Tutorial - Tricentis, accessed April 25, 2025, https://www.tricentis.com/learn/oracle-data-masking-a-basic-tutorial
100. Data Masking and Subsetting Guide - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/en/database/oracle/oracle-database/23/dmksb/introduction.html
101. Securing non-production databases with data masking and subsetting - YouTube, accessed April 25, 2025, https://www.youtube.com/watch?v=nH19PdNe8iE
102. Replacing Sensitive Data By Using the Data Masking Pack - Oracle, accessed April 25, 2025, https://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/366947.htm
103. Creating realistic masked data with Oracle Data Masking & Subsetting - YouTube, accessed April 25, 2025, https://www.youtube.com/watch?v=5jG74fYHypk
104. Data masking in Oracle - DATPROF, accessed April 25, 2025, https://www.datprof.com/solutions/data-masking-in-oracle/
105. Oracle Data Masking: Benefits, Barriers, and Beyond - K2view, accessed April 25, 2025, https://www.k2view.com/blog/oracle-data-masking/
106. Oracle Data Masking | Oracle Enterprise Manager vs. ADM - Accutive Security, accessed April 25, 2025, https://accutivesecurity.com/oracle-data-masking-oracle-enterprise-vs-alternatives/
107. Oracle Advanced Security vs Oracle Data Masking and Subsetting comparison - PeerSpot, accessed April 25, 2025, https://www.peerspot.com/products/comparisons/oracle-advanced-security_vs_oracle-data-masking-and-subsetting
108. Oracle Data Masking and Subsetting Reviews & Ratings 2025 - TrustRadius, accessed April 25, 2025, https://www.trustradius.com/products/oracle-data-masking-and-subsetting/reviews
109. Data Masking Tools for SQL Server: What, Why, and How? - K2view, accessed April 25, 2025, https://www.k2view.com/blog/data-masking-tools-for-sql-server/
110. SQL Server Data Masking - Commvault Documentation, accessed April 25, 2025, https://documentation.commvault.com/11.20/sql_server_data_masking.html

111. 3 Best Practices for SQL Data Masking at Scale - Perforce, accessed April 25, 2025, https://www.perforce.com/blog/pdx/sql-data-masking
112. What Is Database Security? - Palo Alto Networks, accessed April 25, 2025, https://www.paloaltonetworks.com/cyberpedia/database-security
113. 2 Options and Packs - Oracle Help Center, accessed April 25, 2025, https://docs.oracle.com/cd/E55822_01/DBLIC/options.htm
114. What is Data Masking? | Tonic.ai, accessed April 25, 2025, https://www.tonic.ai/guides/what-is-data-masking
115. MySQL vs MSSQL - Which is Better? | UltaHost Blog, accessed April 25, 2025, https://ultahost.com/blog/mysql-vs-mssql/
116. PostgreSQL vs. MySQL - LogicMonitor, accessed April 25, 2025, https://www.logicmonitor.com/blog/postgresql-vs-mysql
117. Control methods of Database Security | GeeksforGeeks, accessed April 25, 2025, https://www.geeksforgeeks.org/control-methods-of-database-security/
118. Best Practices for User Access Control in Access Databases - Emmanuel Katto Uganda, accessed April 25, 2025, https://www.access-programmers.co.uk/forums/threads/best-practices-for-user-access-control-in-access-databases-emmanuel-katto-uganda.332247/
119. Pros and cons of row level security Microsoft SQL Server - DBA Stack Exchange, accessed April 25, 2025, https://dba.stackexchange.com/questions/211838/pros-and-cons-of-row-level-security-microsoft-sql-server