CONL705: Assignment 2:  
Database Security and Recovery  
Word Count: 1,433

# Introduction

This documented report aims to evaluate potential issues uncovered within the companies centralised Oracle database environment, based on examination by the newly appointed Database Administrator. Firstly, to bring awareness of risks found that could jeopardise the environment, such as security threats, access management and disaster recovery. Secondly, to provide an evaluation of various strategies to alleviate these ailments within the system. Thirdly, to provide recommendations on potential practices to adopt – with justification – ensuring a secure, stable and performant database environment going forward.

# Risks observed

## Inadequate user access management

Unauthorised access describes individuals gaining access to a database systems data without permission [1]. At present, all company employees hold the same level of access, as the Database Administrator, which provides full permissions increasing the risk of data breaches [2], as opposed to only providing access relevant to their role.

One example of this is sensitive data exposure, which is a form of data breach occurring when an organisation inadvertently exposes sensitive data [3]. In this scenario, database users across the company could cause a confidentiality breach, in other words where privileged information disclosing to a third party without consent [4], such as access to other employees’ personal information such as address details, salary, passwords, and bank details.

Furthermore, there is increasing risks for users being able to cause malicious or accidental alteration or removal of data known as availability or integrity breaches [5], where users alter information about an order for personal gain or removing other user’s information on the system due to human error [6].

## No Database Backup or Recovery Strategy

At present, the Database Administrator has seen no evidence of any database backup or recovery strategy in place. Unfortunately, the Oracle database environment currently used is at risk fundamental problems that need addressing, data loss and data corruption. Because of these risks at present, there would be no way to recover or use the data affected by these issues

### Data Loss

Data loss is any process or event that results in data deletion or made unreadable by a user, software, or application [7]. An example of data loss for the database environment could be due to Ransomware attacks, power failure, natural disasters, system failure, as well as user error [8]. The impact of data within the database environment could mean a loss in time, revenue, and reputation of the company [9].

### Data corruption

The database environment is exposed to some elements of [Data](https://www.webopedia.com/definitions/data/) corruption; in other words the process of data becoming unreadable or invalid [10]. One example is update done to a data item by a transaction from one user, vanished as overwritten by the update done by another transaction from another user, also known as a Last Update Problem [11]. Another example of data corruption can include data incorrectly recorded due to a failure within the hardware, input, output, or transmission hosting the database environment [12].

# Evaluation of options explored

The following items below are suggestions from the Database Administrator, as to how risks mentioned above can mitigate through various methods, as well as what benefits or implications could ensure from the potential adoption of said strategy.

## Implement Role-Based Access Control.

The concept of role-based access control (RBAC) restricts the access of a user, based on their role within the organisation, to allow them access to information they need, where necessary [13].

One benefit to this method would ensure that database users access only the information they require to perform their duties [14], restricts access to sensitive information where applicable, as well as allowing the database administrator to have increased visibility of all users and their access privileges in the database environment [15]. An example extract of how the roles could fashion, shown in table 1 below.

However, Harel [16] argues RBAC shows exposure to role explosion which in the longer term could be difficult and expensive to manage [17]. Based on the findings above, RBAC could incorporate, at least in preliminary stages of the Oracle database environment.

|  |  |  |
| --- | --- | --- |
| Role | Role Description | Example psuedocode to implement role |
| helpdesk\_operator | Access to, and can create new records in the call log, as well as read-only access to personnel\_register, equipment\_register, and problem\_regsiter | CREATE ROLE helpdesk\_operator;  GRANT SELECT, UPDATE, INSERT ON call\_log TO helpdesk\_operator;  GRANT SELECT ON equipment\_register TO helpdesk\_operator;  GRANT SELECT ON personnel\_register TO helpdesk\_operator;  GRANT SELECT ON problem\_register TO helpdesk\_operator;  GRANT helpdesk\_operator TO 101; |
| helpdesk\_specialist | Like helpdesk\_operator, but can create and update new records in problem\_register | CREATE ROLE helpdesk\_specialist;  GRANT SELECT, UPDATE, INSERT ON call\_log TO helpdesk\_specialist;  GRANT SELECT ON equipment\_register TO helpdesk\_specialist;  GRANT SELECT ON personnel\_register TO helpdesk\_specialist;  GRANT SELECT ON problem\_register TO helpdesk\_specialist;  GRANT helpdesk\_specialist TO 901; |
| SYSTEM | Assigned to the Database Administer, automatically created when a database is created in Oracle SQL Developer. | Not Applicable |
| manager\_legal | Read-only access to employee records relevant to that managers dept. in this case, the manager would only see legal personnel. | CREATE ROLE manager\_legal;  GRANT SELECT ON personnel\_register TO manager\_legal;  GRANT manager\_legal TO 123; |
| office\_admin | Will be able to search, update and remove employee details. Will also help order equipment used for new starters. | CREATE ROLE office\_admin;  GRANT SELECT, UPDATE, DELETE ON personnel\_register TO office\_admin;  GRANT SELECT, UPDATE, ON equipment\_register TO office\_admin;  GRANT SELECT ON hardware\_register TO office\_admin;  GRANT SELECT ON software\_register TO office\_admin;  GRANT office\_admin TO 123; |
| It\_support | Maintain equipment inventory, | CREATE ROLE it\_support;  GRANT SELECT, ON equipment\_register TO it\_support;  GRANT SELECT, UPDATE, DELETE ON hardware\_register TO it\_support;  GRANT SELECT, UPDATE, DELETE ON software\_register TO it\_support;  GRANT it\_support; TO 123; |
| caller | Read access to any problems they have raised with the helpdesk staff. | CREATE ROLE caller;  GRANT SELECT ON problem\_register TO caller;  GRANT caller TO 123; |

Table 1: Example of Roles that to create using Role-Based Access Control (RBAC), based on previous work in database creation within Oracle SQL Developer.

## Create Views for tables in the database

A view is a virtual table, based on the result of query a database table [18]. Chapple [19] suggests views to use limit the data a user perceives in a table, as well increases the simplicity for the user, in terms of the data in which they need to access. An additional benefit to the use of views within the database environment- as confirmed by Oracle [20], state that a view can provide column-level security, so that a user can only access the columns provided on the output on the result set of the query that creates the view, rather than being exposed to all the columns within the original table itself. An example of how this method could apply, is by a requirement to share details of the employees across the company, but not providing access to certain columns such as home address, or salary for instance; as well as having read only access to the data.

Conversely, a drawback to this method as described by IBM [21] refers to performance degradation, due to the need to execute queries in the backend to show the view data; especially when views used in complex queries with multiple joins. Based on the information provided, whilst creating views may be one method for ensuring security within a database, it should work with other methods for increased security.

## Configure and schedule a database backup process

One strategy to adopted to minimise risk, or at least recover from an unavoidable event is an agreed process to routinely backup all the data held within, allowing for recovery during a data loss event with little effort [22]; say in the event of a power failure. However, there are differing methods and schools of thought on how backups should be conduct, whether to use cold or hot backups for the company’s data.

### Cold Backup vs Hot Backups

Cold backups execute when a system is offline [23]. Conversely, Hot backups refer to a backup executed while the environment is still operational [24]. Hannan [25] suggests a benefit to cold backups being immune to power surges, uninterruptable by viruses or intruders, and prevent accidental overwrites and deletion. The downside of a cold backup as argued by Vitanium [26], that during a backup, no user can access the system during this time. Conversely, Vinchin [27] explains how hot backups are operating by users, with tablespace or database file-level backup, and faster backup speed, but risks include a higher maintenance cost, and increased chance of incorrect read write operations. After examining the comparisons between these methods, in an ideal world, a hybrid approach of both methods would be most optimal, however the cold backup approach to adopt in the first instance; due to the database system not utilised by employees across the company outside of office hours.

# Practices recommended going forward

Based upon the issues examined within the oracle database system, as well as the exploration of options to tackle these risks, the database administrator has decided upon a couple of the suggestions above to implement into the system. In an ideal world, the database administrator would implement all suggestions found, were it possible. However, due to time constraints presented with the immediate need to resolve these issues, the solutions to introduce Role-Based Access Control (RBAC) and Cold database backups will be implemented. The justification for RBAC is due to the dire need of ensuring all company information protected from internal misuse through either malicious intent or negligence, but to prevent the company liable to a great deal of legal and compliance issues with the current data exposure [28].

# Conclusion

In this report, the newly appointed database administrator of the company looks at key areas to be address for the Oracle database environment. The information in this document included risks observed such as sensitive data exposure and no database backup or recovery currently in place, as well as solutions proposed – with evidence- involving the implementation of Role-Based Access Control (RBAC), creation of table views for an extra level of security; in addition to the adopted of performing a schedule of cold backups to recover data in the event of a failure. The database administrator concluded by recommending what practices to adopt immediately. Nevertheless, these recommendations provided are not exhaustive and represent only the beginning of future measures to take. Following the implementation of these actions - with additional scope - the database administrator suggests the company evaluate other options, such as both a hot and cold database backup strategy, the audit of all users in the system and the optimization of transactions in the environment.

# References

[1] Cynet, “Unauthorized Access: 5 Best Practices to Avoid the Next Data Breach,” Cynet, Feb. 10, 2022. https://www.cynet.com/network-attacks/unauthorized-access-5-best-practices-to-avoid-the-next-data-breach/#:~:text=What%20is%20Unauthorized%20Access%3F (accessed Feb. 27, 2022).

[2] Monin, “Why granting the DBA role is a really bad idea!,” Monin, Oct. 27, 2020. https://monin-it.be/2020/10/27/dba-role-bad-idea/ (accessed Feb. 27, 2022).

[3] securiti, “What is Sensitive Data Exposure Vulnerability & How to avoid it?,” Securiti, Jun. 04, 2021. https://securiti.ai/blog/sensitive-data-exposure/#:~:text=Sensitive%20Data%20Exposure%20occurs%20when (accessed Feb. 27, 2022).

[4] Hiscox, “What is a breach of confidentiality? | Hiscox UK,” Hiscox.co.uk, 2019. https://www.hiscox.co.uk/business-insurance/professional-indemnity-insurance/faq/what-is-breach-of-confidentiality (accessed Feb. 27, 2022).

[5] MDU, “Data breaches - The MDU,” www.themdu.com, Nov. 10, 2020. https://www.themdu.com/guidance-and-advice/guides/gdpr-data-breaches#:~:text=integrity%20breach%2C%20where%20there%20is (accessed Feb. 27, 2022).

[6] IBM Cloud Education, “Database Security: An Essential Guide,” www.ibm.com, Aug. 27, 2019. https://www.ibm.com/cloud/learn/database-security (accessed Feb. 27, 2022).

[7] Techopedia, “What is Data Loss? - Definition from Techopedia,” Techopedia.com, 2019. https://www.techopedia.com/definition/29863/data-loss (accessed Feb. 27, 2022).

[8] A. Descalso, “What Are the Risks of Not Backing Up Data?,” www.itsasap.com, Aug. 04, 2021. https://www.itsasap.com/blog/why-backup-your-data (accessed Feb. 27, 2022).

[9] L. Hilinski, “What are the Risks of Not Backing Up Data?,” Record Nations, Sep. 19, 2017. https://www.recordnations.com/2017/09/risks-not-backing-data/ (accessed Feb. 27, 2022).

[10] J. Phillips, “What Is Data Corruption? | Webopedia Definition & Meaning,” Webopedia, Mar. 05, 2021. https://www.webopedia.com/definitions/data-corruption/ (accessed Feb. 27, 2022).

[11] GeeksforGeeks, “Concurrency problems in DBMS Transactions,” GeeksforGeeks, Aug. 23, 2019. https://www.geeksforgeeks.org/concurrency-problems-in-dbms-transactions/#:~:text=Lost%20Update%20Problem%3A (accessed Feb. 27, 2022).

[12] J. Spacey, “What is Data Corruption?,” Simplicable, Dec. 20, 2016. https://simplicable.com/new/data-corruption (accessed Feb. 27, 2022).

[13] E. Zhang, “What is Role-Based Access Control (RBAC)? Examples, Benefits, and More,” Digital Guardian, Dec. 01, 2020. https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more (accessed Feb. 27, 2022).

[14] I. Nikolova, “The Advantages of Role-Based Access Control in Cloud Computing,” www.linkedin.com, Jan. 21, 2021. https://www.linkedin.com/pulse/advantages-role-based-access-control-cloud-computing-nikolova-ph-d-/ (accessed Feb. 27, 2022).

[15] L. Rosencrance, “What is Role-Based Access Control (RBAC)? Definition from SearchSecurity,” SearchSecurity, Sep. 2021. https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC (accessed Feb. 27, 2022).

[16] O. Harel, “The Problem with RBAC,” blog.plainid.com, May 30, 2019. https://blog.plainid.com/problem-with-rbac (accessed Feb. 28, 2022).

[17] O. Harel, “Role Explosion: PBAC to the Rescue,” blog.plainid.com, Apr. 03, 2018. https://blog.plainid.com/role-explosion-policy-based-access-control-rescue (accessed Feb. 28, 2022).

[18]w3schools, “SQL CREATE VIEW, REPLACE VIEW, DROP VIEW Statements,” W3schools.com, 2019. https://www.w3schools.com/SQL/sql\_view.asp (accessed Feb. 27, 2022).

[19] M. Chapple, “How Do You Control Data Access With Views?,” ThoughtCo, Sep. 13, 2020. https://www.thoughtco.com/controlling-data-access-with-views-1019783 (accessed Feb. 27, 2022).

[20] Oracle, “Database Security Guide,” docs.oracle.com, 2022. https://docs.oracle.com/cd/B19306\_01/network.102/b14266/authoriz.htm#i1008214 (accessed Feb. 27, 2022).

[21] IBM, “Advantages and disadvantages of views in Classic federation,” www.ibm.com. https://www.ibm.com/docs/en/idr/11.4.0?topic=views-advantages-disadvantages-in-classic-federation (accessed Feb. 27, 2022).

[22] I. Riki, “Why You Should Always Backup Your Data?,” Stellar Data Recovery Blog, Jun. 25, 2021. https://www.stellarinfo.com/blog/always-backup-data/ (accessed Feb. 27, 2022).

[23] Techopedia, “What is Cold Backup? - Definition from Techopedia,” Techopedia.com, Jun. 27, 2013. https://www.techopedia.com/definition/13589/cold-backup (accessed Feb. 28, 2022).

[24] S. Hilker, “Hot and Cold Backups - Overview,” blog.toadworld.com, Apr. 14, 2013. https://blog.toadworld.com/hot-and-cold-backups-overview (accessed Feb. 28, 2022).

[25] E. Hannan, “What is a Cold Backup (Offline Backup)? Definition from SearchDataBackup,” SearchDataBackup, Sep. 2021. https://www.techtarget.com/searchdatabackup/definition/cold-backup (accessed Feb. 28, 2022).

[26] Vitanium, “Hot backup Vs Cold backup – What is the difference?,” vitanium.com, Aug. 28, 2020. https://vitanium.com/what-is-the-difference-between-hot-backup-and-cold-backup/ (accessed Feb. 28, 2022).

[27] V. machine backup expert, “Blog | Vinchin,” @Vinchin, Aug. 24, 2021. https://www.vinchin.com/en/blog/pros-and-cons-of-cold-backup-and-hot-backup.html (accessed Feb. 28, 2022).

[28] E. Friedman, “Why Role-Based Access Control Is Essential to Database Security,” www.singlestore.com, Aug. 31, 2016. https://www.singlestore.com/blog/why-role-based-access-control-is-essential-to-database-security/ (accessed Feb. 28, 2022).