

Backup strategies

ASSIGNMENT 2 – DBAS3080 – DATABASE BACKUP AND RECOVERY



February 19, 2021

JAMIE LU

W0441213

Table of Contents

[Introduction 2](#_Toc64665448)

[Task One 3](#_Toc64665449)

[Hot Backup Strategy 3](#_Toc64665450)

[Cold Backup Strategy 5](#_Toc64665451)

[Task Two 8](#_Toc64665452)

[United States 8](#_Toc64665453)

[Legislation 8](#_Toc64665454)

[Plan 8](#_Toc64665455)

[Mexico 11](#_Toc64665456)

[Legislation 11](#_Toc64665457)

[Plan 11](#_Toc64665458)

[Brazil 13](#_Toc64665459)

[Legislation 13](#_Toc64665460)

[Plan 13](#_Toc64665461)

[Task Three 15](#_Toc64665462)

[Flow Diagram of the Strategy 15](#_Toc64665463)

[References 16](#_Toc64665464)

# Introduction

This assignment talks all about the different backup methods (hot and cold) and explores each one’s pros and cons through analysis by developing a backup strategy for each one.

This assignment is connected to the previous one, in that it exercises the skill of creating a back up and recovery plan. It goes more in depth as it looks at how legislation of a specific location can affect the plan. The back up plan might follow a certain format and company standards based on the company, but it must be molded to fit the area that it is located in. This is why learning the legislation is important.

This assignment trains us to practice these skills and determine what best practices are there to ensure that there is a solid back up plan in place.

# Task One

## Hot Backup Strategy

A hot backup does not require any downtime as it is constantly running. A script will be created to automate the hot backup to remove the need to have a database operator to down the database service. Saving costs from this will enable me to have a team that will be carefully watching and monitoring the back up process to ensure that the backup has no failures or shortcomings. I will also have the script tested multiple times to ensure it is working well before we use it.

As part of my strategy for the company, I have chosen to use Oracle 12C. As Oracle is one of the principal vendors of the hot backup process[[1]](#footnote-1), the steps below are the steps required when performing a hot backup with Oracle 12C.[[2]](#footnote-2)

First, it must be guaranteed that the database is is in archivelog mode. The command ***archive log list*** can be entered to check this.

Second, the location of which the copied items (or back up location) will be placed in must be determined. There should be enough space, thus checking the space one would need for the backup is essential. To do this, you can run the query:

***select sum(bytes) from dba\_data\_files;***

It is important to remember that the location of the backup must be on a separate set of disks from the live data files.

Third, one must identify which files have to be backed up. Once identified, one has to locate these files which can be done using the statement:

***select name from v$datafile;***

Fourth, it is essential for the maximum sequence number of the online redo logs to be noted. In order to successfully recover the files, all the archive redo logs that were generated when the backup was done is needed. This is why it is crucial to take note of the archivelog sequence prior to beginning the hot backup. This can be done through the statement:

***select thread#, max(sequence#) from v$log group by thread# order by thread#;***

Fifth, the tablespaces have to be altered into back up mode. This can all be done at the same time using the statement:

***alter database begin backup;***

However, if it is an active OLTP database, it is better to do it one at a time as it can degrade the performance if done together. This can be done using the statement:

***alter tablespace <tablespace\_name> begin backup;***

Sixth, the data files have to be copied. This can be done using an OS utility (cp command). For example:

***$ cp /u01/dbfile/O12C/\*.dbf /u01/hbackup/O12C***

Seventh, after all the data files have been copied to the backup location, the tablespaces have to be altered out of the backup mode. This can be done using the statement (if all together):

***alter database end backup;***

and if one at a time,

***alter tablespace <tablespace\_name> end backup;***

It is very important that the tablespaces are taken out of the backup mode as this can seriously worsen the performance and compromise the recovery ability. You can check to make sure this is finished by using the statements:

***alter session set nls\_date\_format = 'DD-MON-RRRR HH24:MI:SS';***

***select \* from v$backup where status='ACTIVE';***

Eighth, the current online redo log must be archived, and the maximum sequence number of the online redo logs must be noted down. The archiving part can be done by using the statement:

***alter system archive log current;***

and the max sequence can be determined using the statement:

***select thread#, max(sequence#) from v$log group by thread# order by thread#;***

Ninth, the control file must be backed up. When using a hot backup, an OS copy command cannot be used in this step. This can be done by using the statement:

***alter database backup controlfile***

Lastly, any archive redo logs generated during the backup must be backed up. This can be done using the OS copy command:

***$ cp <archive redo logs generated during backup> <backup directory>***

This step ensures that one has the logs in the event that a failure occurs soon after the hot backup ends.

## Cold Backup Strategy

A cold backup needs to have their system shut down while doing a back up. This is why I have decided to have the cold backup done at 2am-4am. This will allow those individuals who have work at night to access the services, as well as the individuals who work during the day to access it as well. During the time this is being backed up, I plan to have all the customer services lines open and ready to serve customers using a separate system that can later on be connected to the back up. This is useful for the individuals that need to access the services during the 2am-4am backup time.

I will also have newsletters both emailed and mailed (or depending on the customer’s preference during sign up) that notify the customers of the backup. I will include an apology for the maintenance but will explain the benefit of having this maintenance in place. I will also include that customer service lines are open to serve them during this time. I will have this sent out at least 3-5 days in advance so that they can plan for it.

Since I have established in the previous section that I will be using Oracle 12C. The cold back up procedure below is what I have in place.[[3]](#footnote-3)

First, it must be determined where the backup files will be located and how much space is needed to store them. Like the hot back up strategy, the ideal place to store them would be on separate disks from the live data files. You can get a estimated amount of the space you need for the backup using the following query:

***select sum(sum\_bytes)/1024/1024 m\_bytes***

***from(***

***select sum(bytes) sum\_bytes from v$datafile***

***union***

***select sum(bytes) sum\_bytes from v$tempfile***

***union***

***select (sum(bytes) \* members) sum\_bytes from v$log***

***group by members);***

Next, you have to identify which files you would like to copy. Identify their names and where they are located. You can run the query below to list the file names and their locations which are included in the cold back up:

***select name from v$datafile***

***union***

***select name from v$controlfile***

***union***

***select name from v$tempfile***

***union***

***select member from v$logfile;***

The online redo logs do not have to be backed up but can be backed up if you wish for the restore process to go a bit easier.

Next, the database must be shut down. One can connect as SYS or as a SYSDBA-privileged user then shut it down using either immediate, normal, or transactional. However, immediate is the preferred method as it disconnects the users, rolls back the unfinished transactions, and shuts the database down. For example:

***$ sqlplus / as sysdba***

***SQL> shutdown immediate;***

Next, the backup copies of the files are created. One can use an OS utility to do this. You can also use the Linux/Unix ***cp*** command to copy the database files from the live directory to the back up directory. For example:

***$ cp /u01/dbfile/O12C/\*.\* /u01/cbackup/O12C***

Once all the steps mentioned above are done, the database can now be restarted. To do so, one can run:

***$ sqlplus / as sysdba***

***SQL> startup;***

Another way that we can do a cold backup in Oracle is to use the RMAN or the Recovery Manager. This is a shorter way to do it and the database would not need to be archivelog. This comes in three easy steps:[[4]](#footnote-4)

First, the database must be shut down.

You can use the command:

***SQL> shutdown immediate;***

Next, the database must be started in mount stage.

You can use the command:

***SQL> startup mount;***

Last, the RMAN must be run, and you must connect to the target database, then run RMAN to backup database and connection to the catalog (if one is used).

You can use the commands:

***$ $ORACLE\_HOME/bin/rman target /***

***RMAN> backup database include current controlfile;***

# Task Two

## United States

### Legislation

* The FTC or the Federal Trade Commission has a Health Breach Notification Rule that covers vendors of personal health records (PHR), a PHR-related entity, or third-party service provider for a vendor of PHR or a PHR-related entity. This is only for those not under the HIPAA. (FTC, 2010)

The requirement for notification is triggered when there has been unauthorized acquisition of a PHR. When this happens, each person affected by the breach who is a resident or citizen of the United States, the Federal Trade Commission, and in some instances, the media, must be notified. The affected persons must be notified without unreasonable delay, within 60 calendar days from when the breach occurred. If the breach involves 500 or more people, the FTC must be notified as soon as possible, within 10 business days from the discovery of the breach. If it involves less than 500 people, you can send the breach along with any other breach that occurred that same year, as long as it is within 60 calendar days following the end of the calendar year. When there are at least 500 residents of a particular state, the District of Columbia, or a U.S. Territory are affected by the breach, the media has to be notified without any reasonable delay, within 60 calendar days after the discovery of the breach. (FTC, 2010)

The breach notification must include a summarized description of what had occurred, along with the date of the breach and its discovery (if possible), and the kind of PHR that was compromised. If the breach presents a possible risk or harm for the affected individual/s, the notification must include some suggested methods the individual/s can do to protect themselves. The breach notification must also describe the measures taken by the business to investigate the breach, to secure from future breaches, and to mitigate harm caused by the current breach. (FTC, 2010)

### Plan

* The main HQ (headquarters) for the entire company will be set within the country it will contain the live data. Any data that will be backed up will be stored in a backup facility that is secured and is in a different location that than of the HQ. This will ensure that if any disaster occurs within the area of the HQ, the backup facility will not be affected. This back up facility will only cater to the United States division of the company’s data as well as the company’s own data that does not include the consumer’s personal data.
* 4 Backup Administrators will be designated and will be in charge of all the backup processes. A team will be designated as well, they will assist the backup administrators with these tasks. The team will be split in two, one team will be stationed within the main building of the company, and the other at the backup location. Each team will have a supervisor or lead that will report to the backup administrator. The backup administrator will mainly be at the backup location but will travel between the two from time to time. A weekly meeting will take place within each team to discuss any matter, including how the current system is working out, any issues they have, and any suggestions they would like to add. A monthly meeting between the supervisors and the Backup Administrator will take place as well.
* Multiple back up locations will be placed within each major state that the company’s services are available in. Each of these locations will have their own backup team that reports to the Backup Administrator.
* Everything will be backed up to reduce or mitigate any risk of data loss, this includes but is not limited to files, databases, operating systems, configurations, and applications.
* Due to the advancement of today’s technology, I will consider the BYODs (bring your own device) as part of the important technologies that might contain any critical information regarding the company. This will include but is not limited to any iPads, tablets, cellphones used for company purposes. To ensure transparency, we will ensure that all employees subjected to this will be informed before their data is backed up and cautioned to not use these devices for any use other than company use.
* A mix of hot and cold back up methods will be used. This will create a safeguard that the services mostly used by consumers/customers will continually be available. It will also ensure that the data is secured and backed up. The information that is backed up using hot backup will also be backed up by the cold backup at the end of the day to ensure that there is minimal to no data loss.
* A majority if not all of the employees that are employed within the location of the company (HQ or backup facility) would have to be local as to increase the employment rate within the country. Extensive background checks will be done as well to ensure the security of the company.
* A hybrid of hot and cold back up will be used. This will ensure that the services mostly used by consumers/customers will continually be available. It will also ensure that the data is secured and backed up. The information that is backed up using hot backup will also be backed up by the cold backup at the end of the day to ensure that there is minimal to no data loss.
* A data measurement and monitoring plan will be put in place that will be created by the Backup Administrator and backup team, data security team, heads of the IT department, the legal department, and the CEO. The main goal of the plan will be to ensure that only the required information will be stored and kept within the company’s database and that all the consumers’ information will be secured. This will be marketed as such as well to its’ consumers. Consumers will also be notified as to what data is being collected and when. The goal and vision of the company is to be as transparent as they can to their consumers and to ensure the security of their data.
* In the event of a data breach, the individuals affected by the breach will be notified and a committee will be formed to handle the breach. This committee will determine the magnitude of the breach and once this is determined, the individuals affected, the Federal Trade Commission, and depending on the magnitude, the media will be notified. This will be done within 60 calendar days and without unreasonable delay. This committee will comprise of the individuals included in the making of the data measurement and monitoring plan. An investigation will take place as soon as the report of breach is received, and the company will work and in hand with the law enforcement team to ensure that the culprit is caught. The company will also put plans in place to help those who are affected by the breach. A notification will be sent by mail and include the summarized description of what has happened, the date of the breach and when it was discovered, the kind of data that was compromised, and the suggested methods the individual can do to protect themselves. It will also include the measures taken by the company to investigate the breach and the security measures it has taken to ensure that this does not happen in the future or to mitigate this from happening again. It will also include the measures in place to mitigate harm caused by the breach.

## Mexico

### Legislation

* Mexican law requires data owners to notify the individuals immediately of any collection, storage or use of their data that can in any way affect in a significant matter their patrimonial or moral rights as individuals. (Arceo & Alcocer, 2020)
* Mexican law requires that in the event of a data breach that significantly affects their moral or patrimonial rights, the data owners must notify individuals immediately, with no delay, regarding the breach when the data owner confirms it and when the data owner has taken any actions towards an exhaustive process to determine the magnitude of the breach. (Arceo & Alcocer, 2020)

### Plan

* Although Mexico’s legislation only requires individuals to be notified of any collection, storage, or use of their data if it significantly affects their patrimonial or moral rights, and that it does not specify what would define “significantly affects”, our company will still notify individuals of any or all data that will be collected or stored or used. This will ensure that there is transparency between the company and its consumers.
* A secured HQ (headquarters) will be set within the country that will contain the live data. Any data that will be backed up will be stored in a backup facility that is secured and is in a different location that than of the HQ. This will ensure that if any disaster occurs within the area of the HQ, the backup facility will not be affected.
* I will designate a Backup Administrator that will be in charge of all the backup processes and designate a team that will assist the backup administrator with these tasks. The team will be split in two, one team will be stationed within the main building of the company, and the other at the backup location. Each team will have a supervisor or lead that will report to the backup administrator. The backup administrator will mainly be at the backup location but will travel between the two from time to time. A weekly meeting will take place within each team to discuss any matter, including how the current system is working out, any issues they have, and any suggestions they would like to add. A monthly meeting between the supervisors and the Backup Administrator will take place as well.
* Everything will be backed up to reduce or mitigate any risk of data loss, this includes but is not limited to files, databases, operating systems, configurations, and applications.
* Due to the advancement of today’s technology, I will consider the BYODs (bring your own device) as part of the important technologies that might contain any critical information regarding the company. This will include but is not limited to any iPads, tablets, cellphones used for company purposes. To ensure transparency, we will ensure that all employees subjected to this will be informed before their data is backed up and cautioned to not use these devices for any use other than company use.
* A hybrid of hot and cold back up will be used. This will ensure that the services mostly used by consumers/customers will continually be available. It will also ensure that the data is secured and backed up. The information that is backed up using hot backup will also be backed up by the cold backup at the end of the day to ensure that there is minimal to no data loss.
* A majority if not all of the employees that are employed within the company would have to be local as to increase the employment rate within the country. As an additional measure to the company’s internal safety, an extensive background checks will be done during hiring.
* A hybrid of hot and cold back up will be used. This will ensure that the services mostly used by consumers/customers will continually be available. It will also ensure that the data is secured and backed up. The information that is backed up using hot backup will also be backed up by the cold backup at the end of the day to ensure that there is minimal to no data loss.
* A data measurement and monitoring plan will be put in place that will be created by the Backup Administrator and backup team, data security team, heads of the IT department, the legal department, and the CEO. The main goal of the plan will be to ensure that only the required information will be stored and kept within the company’s database and that all the consumers’ information will be secured. This will be marketed as such as well to its’ consumers. Consumers will also be notified as to what data is being collected and when. The goal and vision of the company is to be as transparent as they can to their consumers and to ensure the security of their data.
* In the event of a data breach, the consumers or not, the consumers shall be notified, and a committee will be formed to handle the breach. This committee will determine the magnitude of the breach and once this is determined, the consumers affected will be notified. This committee will comprise of the individuals included in the making of the data measurement and monitoring plan. An investigation will take place as soon as the report of breach is received, and the company will work and in hand with the law enforcement team to ensure that the culprit is caught. The company will also put plans in place to help those who are affected by the breach. An example would be a notification letter sent by mail regarding the breach and it will contain information on how the consumer can protect themselves from it.

## Brazil

### Legislation

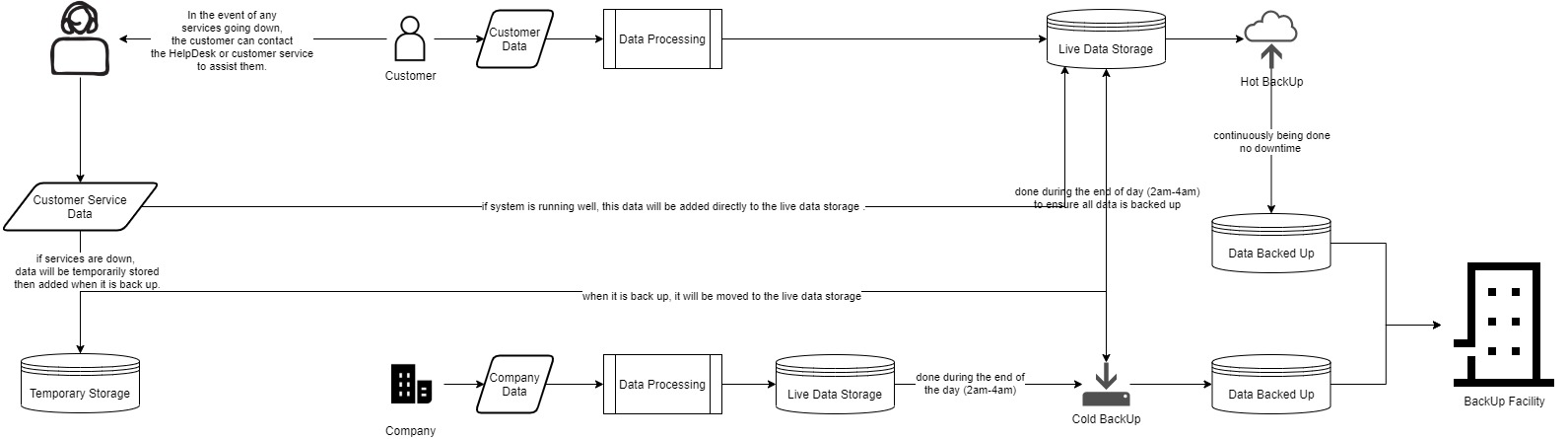
* Global internet companies have to store data on Brazilian users inside the country to shield them from spying. (Boadle, 2014)
* Brazil’s “internet constitution” has set limits to the amount of their internet users’ metadata that is gathered and used. (Boadle, 2014)

### Plan

* Due to Brazil’s legislation on how they would like Brazilians have their data stored, I will ensure that not only will the live data be stored within the country but also the back up. Due to best practice however, they will not be stored within the same area.
* I will designate a Backup Administrator that will be in charge of all the backup processes and designate a team that will assist the backup administrator with these tasks. The team will be split in two, one team will be stationed within the main building of the company, and the other at the backup location. Each team will have a supervisor or lead that will report to the backup administrator. The backup administrator will mainly be at the backup location but will travel between the two from time to time. A weekly meeting will take place within each team to discuss any matter, including how the current system is working out, any issues they have, and any suggestions they would like to add. A monthly meeting between the supervisors and the Backup Administrator will take place as well.
* Everything will be backed up to reduce or mitigate any risk of data loss, this includes but is not limited to files, databases, operating systems, configurations, and applications.
* Due to the advancement of today’s technology, I will consider the BYODs (bring your own device) as part of the important technologies that might contain any critical information regarding the company. This will include but is not limited to any iPads, tablets, cellphones used for company purposes. To ensure transparency, we will ensure that all employees subjected to this will be informed before their data is backed up and cautioned to not use these devices for any use other than company use.
* A majority if not all of the employees that are employed within the company would have to be local as to increase the employment rate within the country. Extensive background checks will also be done to each new employee to ensure the company’s security.
* Both hot and cold back up will be used. This will ensure that the services mostly used by consumers/customers will continually be available. It will also ensure that the data is secured and backed up. The information that is backed up using hot backup will also be backed up by the cold backup at the end of the day to ensure that there is minimal to no data loss.
* A data measurement and monitoring plan will be put in place that will be created by the Backup Administrator and backup team, data security team, heads of the IT department, the legal department, and the CEO. The main goal of the plan will be to ensure that only the required information will be stored and kept within the company’s database and that all the consumers’ information will be secured. This will be marketed as such as well to its’ consumers. Consumers will also be notified as to what data is being collected and when. The goal and vision of the company is to be as transparent as they can to their consumers and to ensure the security of their data.
* In the event of a data breach, the consumers shall be notified as soon as possible, and a committee will be formed to handle the breach. This committee will comprise of the individuals included in the making of the data measurement and monitoring plan. An investigation will take place as soon as the report of breach is received, and the company will work and in hand with the law enforcement team to ensure that the culprit is caught. The company will also put plans in place to help those who are affected by the breach. An example would be a notification letter sent by mail regarding the breach and it will contain information on how the consumer can protect themselves from it.

# Task Three

## Flow Diagram of the Strategy



A clearer photo has been uploaded along with the document for clarity.

# References

Acronis. (n.d.). *Data Backup – What is it?* Retrieved February 19, 2021, from Acronis: https://www.acronis.com/en-us/articles/data-backup/

Arceo, A. D., & Alcocer, G. A. (2020, June 07). *https://iclg.com/practice-areas/data-protection-laws-and-regulations/mexico.* Retrieved February 19, 2021, from ICLG: https://iclg.com/practice-areas/data-protection-laws-and-regulations/mexico

Boadle, A. (2014, March 18). *Brazil to drop local data storage rule in Internet bill.* Retrieved from Reuters: https://www.reuters.com/article/us-brazil-internet/brazil-to-drop-local-data-storage-rule-in-internet-bill-idUKBREA2I03O20140319

*Brazil Removes Local Data Storage Requirement from Internet Bill.* (2014, March 19). Retrieved February 19, 2021, from Hunton Privacy Blog: https://www.huntonprivacyblog.com/2014/03/19/brazil-removes-local-data-storage-requirement-internet-bill/

*Cold-Backup Strategy for a Noarchivelog Mode Oracle Database 12C.* (2020, January 02). Retrieved February 18, 2021, from Oracle Patches: https://oracle-patches.com/en/databases/oracle/4083-cold-backup-strategy-for-a-noarchivelog-mode-oracle-database-12c

FTC. (2010, April). *Complying with the FTC's health breach notification rule*. Retrieved November 13, 2020, from FTC: https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

Glickhouse, R. (2014, March 27). *Explainer: What Is Brazil's Internet Constitution?* Retrieved February 19, 2021, from AS/COA: https://www.as-coa.org/articles/explainer-what-brazils-internet-constitution

*Implementing a Hot Backup Strategy for Oracle Database 12C.* (2020, January 03). Retrieved February 18, 2021, from Oracle Patches: https://oracle-patches.com/en/databases/oracle/4085-implementing-a-hot-backup-strategy-for-oracle-database-12c

Lima, A. (2010, April 22). *How to create cold backup using RMAN?* Retrieved February 18, 2021, from An Oracle Spin: https://oraclespin.com/2010/04/22/how-to-create-cold-backup-using-rman/

Mari, A. (2013, November 01). *All you need to know about Brazil's "Internet Constitution".* Retrieved February 19, 2021, from ZDNet: https://www.zdnet.com/article/all-you-need-to-know-about-brazils-internet-constitution/

Street, E. (n.d.). *Hot and Cold Backups.* Retrieved February 18, 2021, from Brightspace: https://nscconline.desire2learn.com/d2l/le/content/185497/viewContent/2385631/View

1. Referenced from (Street) [↑](#footnote-ref-1)
2. Referenced from (Implementing a Hot Backup Strategy for Oracle Database 12C, 2020) [↑](#footnote-ref-2)
3. Referenced from: (Cold-Backup Strategy for a Noarchivelog Mode Oracle Database 12C, 2020) [↑](#footnote-ref-3)
4. Referenced from: (Lima, 2010) [↑](#footnote-ref-4)