

Evaluating resources

ASSIGNMENT 1 – DBAS3080 – DATABASE BACKUP AND RECOVERY



January 30, 2021

JAMIE LU

W0441213

Table of Contents

[Introduction 2](#_Toc62941306)

[Task One 3](#_Toc62941307)

[Advantages of current state 3](#_Toc62941308)

[Disadvantages of current state 3](#_Toc62941309)

[SWOT Analysis 3](#_Toc62941310)

[Solutions 4](#_Toc62941311)

[Task Two 5](#_Toc62941312)

[DR Plan 5](#_Toc62941313)

[1. Recovery Time Objective and Recovery Point Objective 5](#_Toc62941314)

[2. Creating a Risk Analysis Model 5](#_Toc62941315)

[3. Recovery goals 5](#_Toc62941316)

[4. What to do 5](#_Toc62941317)

[Task Three 7](#_Toc62941318)

[Risk Analysis Model 7](#_Toc62941319)

[References 9](#_Toc62941320)

# Introduction

This assignment talks all about risks and helps us realize the importance of Database Back up and Recovery. A risk is both the likelihood of something going wrong and the bad consequences that happening. The consequences of risks are quite costly especially when you have not planned for it accordingly. That is why having a risk analysis model as well as a data recovery plan or any sort of back up plan is essential to any business or organization.

This assignment trains us to practice doing risk analysis and creating back up plans. It tasks us with analyzing the company given, which is the law firm Womble Carlyle, determining the possible risks they face, and coming up with solutions to deter the determined risks.

# Task One

The first step for improvement is always to look at the current state of things. This is what task one is all about. Through analysis, both the advantages and disadvantages of the company will be identified. I have also included a SWOT Analysis to have a better view of their current state. Possible solutions for the issues and challenges will also be identified.

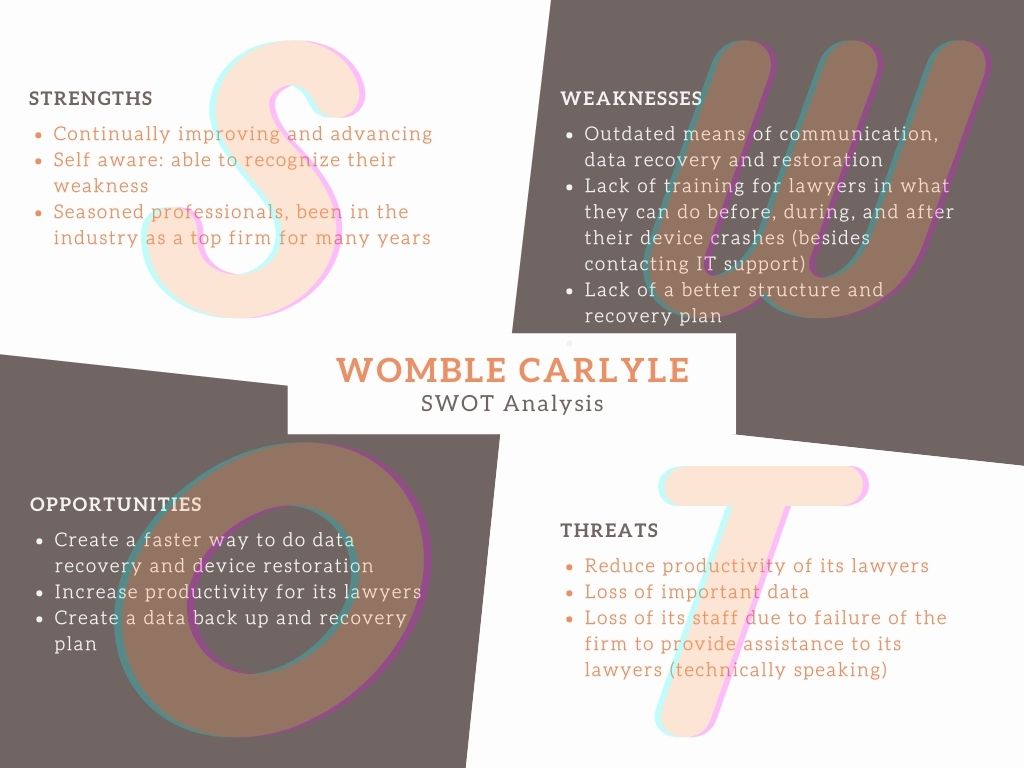
## Advantages of current state

* Technologically advanced
* Enables their lawyers access to their company’s information even while travelling
* Has existing back up plan
* Has an IT department with IT support that can walk through restoration process
* Able to restore laptop
* Able to send a CD or hard drive worldwide

## Disadvantages of current state

* Restoration process takes a long time
* Communication method is dated
* Method of restoration process is dated

### SWOT Analysis

Below is a SWOT analysis on Womble Carlyle's current state:

## Solutions

* I would suggest for the company to embrace new methods of communication such as a video conference or call, or live chat, other than just a regular phone call. This might prove to save costs as well because a video conference or call can be done through the internet which saves more money than doing long distance calls (in the instance of lawyers and other employees working overseas).
* I would suggest that the current restoration process be revisited, analyzed, and updated to more advanced methods. Sending a CD or hard drive, for example, is very outdated. Many companies, such as Best Buy Geek Squad, are able to do repairs through the internet. I think they should be able to do restorations through a cloud-based service or something related to the internet, that way they can do the fix as soon as possible, instead of having the lawyer wait 24hrs for a CD or hard drive.
* I would also suggest having a Data Recovery Plan that is more updated and is frequently revisited in order to stay up to date on the latest technology. It is also important that in this plan, they will include training not only to IT staff but to all their staff on the importance of backing their information and data and always having a spare laptop or hard drive in case of failure or crashes. Knowledge is power.

# Task Two

## DR Plan

It is important that we make the DR plan as detailed as possible as well as tailored to the company.

### Recovery Time Objective and Recovery Point Objective[[1]](#footnote-1)

The first step in my suggested Data Recovery Plan, is to identify a recovery time objective. This is basically the maximum length of time that the company, application, or even laptop is down or offline. This is more implemented to large scale disasters but can be used as a guideline for smaller disasters.

Large scale disasters would constitute at least 40% of the company’s total productivity, whereas medium scale disasters would constitute at least 10% of the company’s total productivity, smaller scale disasters constitute productivity loss of less than 10% and can include individual productivity loss (such as the one given in the scenario, a lawyer’s laptop crashes).

It is also important to determine a Recovery Point Objective, which is basically the maximum amount of time wherein data might be lost due to the incident.

The smaller the recovery time objective and recovery point objective values are, the more it will cost for an application or company to run.

### Creating a Risk Analysis Model

This step is concerned with looking at the current state of the system in place. We explore the strengths and weaknesses and the possible areas of failure. Different methods such as a SWOT Analysis, and Fishbone diagram (to name a few) have to be used to have a better look at the positives and negatives and where we can improve on.

This step is very important as the entirety of the Data Recovery plan will be based on this as all the weaknesses and areas of improvement are determined. Analysis of the current state and what the company’s goals are will shape the DR plan.

### Recovery goals

When we create our DR plan, it is important to set the recovery goals. We have to determine which areas we would prioritize to be fixed first, ideally the areas we need to have the company or application running again.

### What to do[[2]](#footnote-2)

To determine what needs to be done, this has to be according to what our recovery goals are and how they are related to the Recovery Time and Point objectives. Some key things that must be done are:

1. End-to-end Recovery

* This ensures that the plan not only includes the back up and archiving of the data, but also covers the entire recovery process. This means it covers backing up and restoring to clean up.

1. On site back up

* This means that the backup storage should be located within the workplace. This is so that the back up data is easily accessed and available. This also allows for part A (end-to-end recovery, full back up) to be possible and done faster.

1. Regular Back ups

* This means that a full backup will be done daily, as well as hourly. This ensures that should data be lost, we can easily recover from the last back up.

1. Cloud Back ups

* This means that a users’ personal work PC, notebook or laptop would be backed up to a cloud regularly (hourly basis: part C) to ensure that if they are overseas or far from the work site, the data can still be accessed.

1. Security

* It is very important to have a security system in place in the event of a disaster. Safeguards will take place where if the company does go down and lose productivity, the company’s data, even on the cloud, can only be accessed by the right individuals (IT Support).

1. Training

* As mentioned before, knowledge is power. Training will be provided not only to IT Staff but to all staff that will need access to the company’s system and application to do work. They will be trained on the DR plan, what to do, how to handle situations, etc. This will ensure that no one will be like a deer in the headlights or lost especially when they are overseas.

1. Scheduled Meeting

* The current DR plan will regularly be revisited and updated if necessary. A meeting will take place, and if there are changes made, training will be conducted to inform the employees.

# Task Three

## Risk Analysis Model

This model is advantageous for Womble Carlyle as it uses the most important part of handling a risk, which is analyzing the current state. This means that the shortcomings of the current state would be addressed and that it would be tailored specifically for the company. It also goes through determining the possible risks and dissecting these risks and classifying them into different categories which would determine how to handle these risks and how much they will affect the company (risk threshold). It also has a predictive aspect as we would need to predict the possible consequences of the risk, this part is advantageous because we would be thinking of different scenarios and be ready for them, should they come. This model also includes testing which means that once a risk management method is determined, testing will be done to ensure that this does in fact work and that it fixes the issues.

However, this model still has its issues and flaws. It needs to be more specific to be more tailored to the company. It also fails to specifically classify the categories and if these categories made are enough for all possible risks, as it is not guaranteed that the company can be prepared for everything. In addition to this, prediction of the consequences could also be inaccurate as like determining the risks, we cannot account for everything.

With this, I do suggest that besides having the risk management model and the data recovery plan, meetings have to be conducted to be able to determine the priorities of the company and determine what the company can specifically face as the people of the company are the most aware of what is going on and what can happen. I also would suggest using risk analysis software such as nTask, Resolver, TimeCamp, CURA, etc. [[3]](#footnote-3)

# References

admin, CloudSecureTech. (2016, December 23). *5 Step Action Plan for Data Recovery for Businesses*. Retrieved from Cloud Secure Tech: https://www.cloudsecuretech.com/5-step-action-plan-for-data-recovery-for-businesses/

Brush, K., & Crocetti, P. (n.d.). *disaster recovery plan (DRP)*. Retrieved January 29, 2021, from SearchDisasterRecovery: https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20plan%20(DRP)%20is%20a%20documented%2C%20structured,on%20a%20functioning%20IT%20infrastructure.

Chong, J. (2015, April 07). *The 5 criteria for a workable Disaster Recovery and Business Continuity - Data Protection*. Retrieved January 29, 2021, from LinkedIn: https://www.linkedin.com/pulse/5-criteria-workable-disaster-recovery-business-continuity-jin-chong/

*Corps Risk Management Model*. (n.d.). Retrieved January 30, 2021, from US Army Corps of Engineers, Institute for Water Resources Website: https://www.iwr.usace.army.mil/Missions/Risk-Analysis-Gateway/Risk-Management/Corps-Risk-Management-Model/

GE. (n.d.). *Risk Assessment Data Model*. Retrieved January 30, 2021, from GE: https://www.ge.com/digital/documentation/meridium/Help/V43020/Default/Subsystems/Operations/Content/RiskAssessmentDataModel.htm

Google Cloud. (n.d.). *Disaster recovery planning guide*. Retrieved January 29, 2021, from Google Cloud: https://cloud.google.com/solutions/dr-scenarios-planning-guide

IBM. (n.d.). *What is a disaster recovery (DR) plan?* Retrieved January 29, 2021, from IBM: https://www.ibm.com/services/business-continuity/disaster-recovery-plan

MindTools Content Team. (n.d.). *SWOT Analysis: How to Develop a Strategy For Success*. Retrieved January 29, 2021, from MindTools: https://www.mindtools.com/pages/article/newTMC\_05.htm

Street, E. (n.d.). *Risk Analysis*. Retrieved January 30, 2021, from https://nscconline.desire2learn.com/d2l/le/content/185497/viewContent/2291292/View

1. Referenced from (Google Cloud, n.d.) and (Chong, 2015) [↑](#footnote-ref-1)
2. Referenced from (Google Cloud, n.d.) and (Chong, 2015) [↑](#footnote-ref-2)
3. Referenced from: (Street, n.d.) [↑](#footnote-ref-3)