

data governance

ASSIGNMENT 3 – DBAS3080 – DATABASE BACKUP AND RECOVERY



March 12, 2021

JAMIE LU

W0441213

Table of Contents

[Introduction 2](#_Toc66475778)

[Task One 3](#_Toc66475779)

[Business Case 3](#_Toc66475780)

[Strategic Context 3](#_Toc66475781)

[Benefits 3](#_Toc66475782)

[Financial Case 3](#_Toc66475783)

[Task Two 4](#_Toc66475784)

[Solutions 4](#_Toc66475785)

[Task Three 5](#_Toc66475786)

[Case studies 5](#_Toc66475787)

[Bonus Question 6](#_Toc66475788)

[Unit of Inquiry 6](#_Toc66475789)

[References 7](#_Toc66475790)

# Introduction

This assignment exercises our analytical abilities by looking at a given scenario and analyzing what the context is and what needs to be done. The answer is given through a business case and proposed solutions. It also enables us to analyze the solutions and compare this with the solutions used by the different companies in the industry.

This assignment shows the importance of research as it explores the different solutions created by other individuals. It also shows the importance of back up, recovery, and creating a plan.

# Task One

## Business Case

### Strategic Context

#### Problems

The back up site and the main production site are in close proximity from one another. There is only a 10-mile distance from the back up site to the main production site. There were several disasters the company faced, and it is uncertain that the company will not face any more. More disasters might come, some even of greater magnitude. It seems like the company either has a poor disaster recovery plan, or none at all.

#### Risks

The problems stated in the previous section poses a lot of threats or risks to the security and overall health of the company. It is unwise to have the main and back up production site so close together because if there is a disaster in one site, the same disaster could affect the other. They have already seen the affects of this when the company lost several hard drives and the information that was stored on them. Based on the previous disasters, it seems like the disaster recovery plan of the company was either insufficient or even non-existent. This is something that has to be dealt with as well as it could disallow the company to be prepared for future disasters and threats.

### Benefits

Data is proving to be very valuable nowadays, even more expensive than oil or gold. It is important to recognize that the company’s data is everything. It is important to ensure that the company’s data is secured, backed up, and managed, especially since it is a bank. The problems faced by the First Community Bank and Trust will affect the company’s data significantly. Dealing with the problems at hand now could help the company avoid any more loses. This is a time sensitive change and should be done as soon as possible as we do not know when another disaster will strike. This will not only save the company a lot of money, but also save its reputation or even improve it, as investors and stakeholders will become more secure in the company.

### Financial Case

#### Cost

The cost of the project to fix the issues presented in the previous sections might seem a lot, but this outweighs the costs the company will incur when another disaster strikes. The amount of money they will have to pay from recovering from a disaster they were not prepared for, will be more than the cost of the project. They will also need to recover from PR issues if they are not properly and sufficiently prepared the next time around.

#### Timeline

This project is time sensitive. It is important to act now as we do not know when the next disaster will strike. The goal is to have everything in place and ready within 18-24 months.[[1]](#footnote-1) The sooner it starts, the sooner the project will finish.

# Task Two

## Solutions

* The back up facility has to be moved to a different location that is further from the main facility. It is important to have the backup facility away from the main facility as it not only follows the 3 2 1 rule (3 copies of the data, 2 back ups, and one back up copy offsite) but also ensures that if any disasters come in the main facility, the back up facility would be further away thus a very much reduced chance of having the back up facility affected.
* If the company wishes to keep the back up facility and the main facility, I suggest creating a second back up facility to ensure that if both the main and back up facilities experience disaster, the third one would still be up.
* Revise (or create) a disaster recovery plan. This is essential as it is important to have a contingency plan for when a disaster will strike. You can never tell when and what it could be thus it is important to ensure you are ready for anything.
* Revise (or create) a back up recovery plan. This is as essential as the disaster recovery plan. This ensures that the data is properly backed up because there is a guide or standard in place.
* A committee should be created to oversee the back up and disaster recovery and back up recovery plans and maintain that there is proper compliance of the guidelines set.
* I would also recommend checking the local legislation and seeing to it that the disaster recovery plans adhere to the local legislation.
* The 3, 2, 1 rule should be followed, and once the data is backed up, it should be determined if storage of this data is for long term storage or not. This ensures that the data collected and stored is meaningful.
* It is best to store data in the bank’s data centers and not in the cloud. This is due to the sensitivity of the information that banks store. It can also prove to cost a lot to move the data to the cloud. It can be time consuming and might require some skills and tools that are not available to the bank at the present time. There are also regulatory issues that the bank could face if they move to the cloud as most financial institutions are not permitted to move to the cloud if there is a danger of not meeting the requirements set by the regulators.[[2]](#footnote-2)
* I would also recommend a hybrid of a cold and hot back up strategy as it ensures that the data would be backed up without a risk of data loss but also ensures that there is minimal downtime. I would also recommend that there be a full backup performed every 24 hours and incremental backups every 3-4 hours and transaction logs every half hour.[[3]](#footnote-3)

# Task Three

## Case studies

I could not find any case studies from other companies in the industry, but I have found some articles that talk about the common practices, standards, and strategies that some companies use.

One practice I have found with banks is that they have their own data centers and create back ups of the back ups.[[4]](#footnote-4) This is similar to the solutions I have presented in the previous section, about creating a new back up center further away from the main and back up facility (the first one that is 10 miles away). This is also similar, in that, the data centers are owned by the bank.

Another resource I found states the importance of data and a disaster recovery plan. Something that I have highlighted a few times in the previous sections. They did, however, include a disaster recovery database system. Something I did not specify in my solutions. I think that this is a great idea, and I would like to know more about it in the future as the literature I found did not have the complete details. The resource I have found also talks about the role the regulators or local legislation has in disaster recovery plans. This is something that I have considered in the previous section. It is important for the bank to consider the local legislation of the location of the data center, and it is equally important for the legislators to enact laws that would enforce banks to create disaster recovery plans and secure the data of their clients.[[5]](#footnote-5)

Another resource that I found also mentions the importance of a Disaster Recovery Plan. It also talks about the details of the plan, including analyzing any possible threats, increasing cybersecurity, running tests, maintaining proper compliance, and storing securely in multiple locations. A few of these I have included in the solutions I have recommended but there are a few I have missed as well. Through the creation of the committee that I have mentioned in the previous section and having them create or revise a disaster recovery plan and back up recovery plan, an analysis would be done for any possible threats. I have also included in my suggested solutions for maintenance of the plan and ensuring that there is proper compliance of the guidelines. I have also mentioned storing in multiple separate locations (which was the main issue presented). I have, however, missed increasing cybersecurity, which is a great idea as you can never be too secure especially with such important data. Another I have missed is running tests regularly, this is something important as well as it shows the current system and what areas it can be vulnerable in. It checks if the proper procedures are followed and ensure that these procedures are effective. This resource also included the importance of knowing the downtime, which I covered a bit in my solution. It is important that should a disaster strike, downtime is kept to a minimum as downtime could mean loss of profit.[[6]](#footnote-6)

# Bonus Question

## Unit of Inquiry

A unit of inquiry is an exploration of a given concept. This usually takes about 6-8 weeks. For example, a main idea or concept will be given by the teacher as the guidelines of what a student needs to research or learn more about. There are several parts of a unit of inquiry, this includes, the central idea, the summative assessment, lines of inquiry, teacher questions, provocations, formative assessments, learning experiences, resources, student inquiries, and reflections. (What is a Unit of Inquiry?, n.d.)

This is a very important aid in learning as it enables students to go further than what is presented in a classroom. It shows the value of research and open mindedness as part of learning. It also practices research skills and locating information and evaluating its relevance and legitimacy. It promotes higher order thinking and helps in getting students more involved and engaged in real-world problems. It promotes social responsibility.[[7]](#footnote-7)

# References

2020 Project Management. (n.d.). *The business case.* Retrieved March 11, 2021, from 2020 Project Management: https://2020projectmanagement.com/resources/project-documentation/the-business-case

*About database Cold backup vs. Hot backup.* (2015, September 02). Retrieved March 12, 2021, from Alibaba Cloud: https://topic.alibabacloud.com/a/about-database-cold-backup-vs-hot-backup\_8\_8\_30083280.html

Association for Project Management. (n.d.). *What is a business case?* Retrieved March 11, 2021, from APM: https://www.apm.org.uk/resources/what-is-project-management/what-is-a-business-case/

Cragg, J. (2020, July 08). *What's stopping financial institutions from using the Cloud?* Retrieved March 12, 2021, from Finextra: https://www.finextra.com/blogposting/18982/whats-stopping-financial-institutions-from-using-the-cloud

*Data Backup and Disaster Recovery for Banks*. (2020, January 30). Retrieved March 12, 2021, from Net2Vault: https://www.net2vault.com/industry-insights/data-backup-disaster-recovery.asp

*How do banks backup their data?* (2004, December 05). Retrieved March 12, 2021, from Hetzner: https://www.webhostingtalk.com/showthread.php?t=350268#:~:text=Most%20banks%20have%20there%20own,make%20backups%20of%20the%20backups.&text=I%20can't%20say%20I,balances%20for%20the%20accounts%20involved.

Huisache, S. (2019, September 26). *How Often Should You Back Up Your Data?* Retrieved March 12, 2021, from TrustRadius: https://www.trustradius.com/buyer-blog/how-often-should-you-backup-your-data#:~:text=If%20you%20want%20to%20take,at%20least%20every%20half%2Dhour.

Krutikov, M. (2013, May 09). *Don’t Break the Bank: Back up Your Files.* Retrieved March 12, 2021, from Bank Systems and Technology: https://www.banktech.com/donand-8217t-break-the-bank-back-up-your-files/a/d-id/1296349d41d.html?

Mayer, A. (2017, November 13). *The 3-2-1 Backup Rule – An Efficient Data Protection Strategy.* Retrieved March 11, 2021, from Nakivo: https://www.nakivo.com/blog/3-2-1-backup-rule-efficient-data-protection-strategy/

*Unit Of Inquiry*. (n.d.). Retrieved March 12, 2021, from Burwood Heights Primary School and Kindergarten: https://www.burwoodhps.vic.edu.au/page/243/Unit-of-Inquiry#:~:text=Develops%20students'%20higher%20order%20thinking,navigate%2C%20evaluate%20and%20use%20information.

US Chamber of Commerce Technology Engagement Center. (n.d.). *Data Centers.* Retrieved March 11, 2021, from US Chamber of Commerce: https://www.uschamber.com/sites/default/files/ctec\_datacenterrpt\_lowres.pdf

Wey, L. A. (2019). *Database Backup System for Banks*. Retrieved March 12, 2021, from Grin: https://www.grin.com/document/512588

*What is a Unit of Inquiry?* (n.d.). Retrieved March 12, 2021, from Hilton IB PYP: https://sites.google.com/a/ga.hiltoncsd.net/hilton-ib-pyp/what-is-a-unit-of-inquiry

1. Time estimation from (US Chamber of Commerce Technology Engagement Center) [↑](#footnote-ref-1)
2. Referenced from (Cragg, 2020) [↑](#footnote-ref-2)
3. Referenced from (Huisache, 2019) [↑](#footnote-ref-3)
4. Referenced from (How do banks backup their data?, 2004) [↑](#footnote-ref-4)
5. Referenced from (Wey, 2019) [↑](#footnote-ref-5)
6. Referenced from (Data Backup and Disaster Recovery for Banks, 2020) [↑](#footnote-ref-6)
7. Referenced from (Unit Of Inquiry, n.d.) [↑](#footnote-ref-7)