nscc

Assignment 1

Risk Analysis & DR Plan

DBAS 3080 Database Backup & Recovery

Jeong Eun Jang (W0451032)

Paul Street

January 23, 2022

TABLE OF CONTENTS

INTRODUCTION

Risk assessment is an essential and useful decision-making tool and Safety and security of a company. Risk can be hard to notice, but it can be managed and prepared for by well-planned risk analysis and business disaster plan. It will also help to secure the critical data and business continuity.

Through this assignment, I will be implementing risk analysis and creating disaster recovery plan for Womble Carlyle Company. It will identify and analyze the current IT issues and it would be a great resource to reduce the risks and help improving the decision-making efficiently.

TASK 1. Risk Assessment

1. Existing System

Womble Carlyle is one of the largest law firms in the mid-Atlantic and the Southeast. There are approximately 450 lawyers and hundreds of laptop-toting attorneys traveling across the globe. The company expects to get the same level of reliability as the desktop systems and fast IT restoration process system.

2. Identification of the current system

2.1. Advantages of the current system

- Has a technologically advanced system
- Has well-trained IT department and staffs
- Use of the laptops
- Able to communicate with each other globally

2.2. Disadvantages of the current system

- Use of old communication methods such as phones
- Non-efficient restoration process by sending a CD or a new hard drive
- Time consuming restoration process
- Result in the productivity loss of lawyers

2.3. Risk Analysis Tool: SWOT

STRENGTH	WEAKNESS
❖ Large organization size ❖ Well-equipped technology system ❖ having a professional IT department	❖ Slow and non-efficient technology service ❖ Old communication process ❖ Lack of backup and recovery plan
OPPORTUNITY	**THREAT**
❖ Technical support following global time ❖ Build up data backup and recovery plan ❖ Enhancing data security ❖ Keeping up to date with technology ❖ Increasing the productivity for lawyers	❖ Reducing productivity of lawyers ❖ Insecure data management ❖ Incurring expenses for building a new restoration system ❖ Requiring technical training for staffs

3. Recommended Solutions

3.1. Remote Technical Service

: I would recommend building a remote technical service for Womble Carlyle. A remote technical team can communicate with lawyers about technical problems using a live chat and resolve computer problems without issues of location and business hours. The remote technical teams can provide high-quality technical support as follows:

- Hardware and software troubleshooting

- Data restoration and backup
- Remote training
- Issues with network, wi-fi and firewalls

This may also reduce the cost of sending equipment for repair and replacement and save time. Moreover, it will help lawyers working in different time zones by flexible 24/7 tech support (Shield Geo, n.d.).

3.2. Hybrid Backup

: I would recommend using a hybrid backup for secure data backup. Hybrid backup can be the best practice for implementing 3-2-1 compliant strategy. The 3-2-1 backup is an effective solution for reliable backup and disaster recovery. For 3-2-1 backup, the company should have 3 copies: the original copy and 2 backup copies in different places, on-premises backup, and off-premises cloud backup (Vanover, 2021). The hybrid backup also provides real-time file access to lawyers if they work globally.

3.3. Data Recovery Plan

I would recommend that the company establish a data recovery plan for business continuity. Technology recovery strategies are essential for restoring hardware, application, and data. I also recommend making data documentation to use, retrieve and manage data easier (Street, 2022). We could use this document to describe the level of data security and privileges and apply these levels to users.

TASK 2. Disaster Recovery Plan

1. The Importance of a Disaster Recovery Plan

This disaster recovery plan (DRP) contains important strategies and instructions on minimizing the effects of unplanned incidents, such as natural disasters and environmental interruptions. The DRP should include compiling an inventory of hardware, software and application and data. It also should include a strategy to back up all critical information. Lastly, the plan also should be tested periodically to make sure it works. The well-prepared data backup and recovery plan would be an important key for securing the company's business continuity.

2. A Simple Disaster Recovery Plan

Policy

This plan has been created as per the requirements of the following administrative regulations:

- Creation, use and maintenance of district information
- Operation of a company in emergency circumstances

Objectives

The major goals of this disaster recovery plan are as follows:

- To minimize interruptions to the critical operations
- To minimize the economic damage of the disruption
- To train employees with emergency procedures

- To provide efficient and fast restoration of service

Responsibility

- Jeong Eun Jang, IT Manager, Communications
- Backup: Jim Dave

Recovery Strategy and Location

- List all the applications
    - The critical level of assets
- Computer room environment
- Hardware
    - The manufacturer, model, serial number, cost, being owned or leased
- Connectivity to a service provider
- Data and restoration
    - Documentation, off site copy, multiple backups, management log

Assumptions

- What equipment/facilities have been destroyed?
    - The main facility of the organization
    - Off-site storage facilities and materials
    - Available staffs for performing the disaster recovery plan
- What records, files and materials were protected from destruction?
- What resources are available after the disaster?
    - People, equipment, communication methods, transportation
    - Hot site and alternate site

Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

Service Tier	IT Service or Application Name	Recovery Time Objective	Recovery Point Objective
0	Data Centre Facility	4	24
0	Core Routing	12	24
0	Storage Services	12	24
0	Server Services	12	24
0	WAN Connectivity	12	24
0	Firewall Services	12	24
0	Active Directory	12	24
1	Payroll	24	24
1	Email	24	24

Recovery Procedure

- Emergency response procedures: The procedures demonstrate proper emergency actions to a natural disaster, a building fire, or any other interruptions to protect employees and reduce damage.
- Backup operations procedures: The procedures contain essential data processing operational tasks that should be conducted after a disaster.
- Recovery actions procedures: The procedures facilitate the rapid restoration of a data processing system after the disruption.

Test Procedure

- Testing and evaluating the plan regularly is important for successful contingency planning. Due to the volatile nature of data, this test should be reflected and updated according to the result.
- We can use checklists as follows:
    - Clarification of each department responsibility and command
    - Management to recover and process in case of key people's absence

- Recovery of individual's application systems
- Determination of priority for each system
- Rapid communication system with key designated people
- Evaluation of the test results and recommendations for changes

Resume Procedure

- Contact the designated company to arrange technical support.
- Contact technicians to be on-site and transfer the configuration and user data from the recovery system.
- Contact Bell to switch the main line back to the phone system.

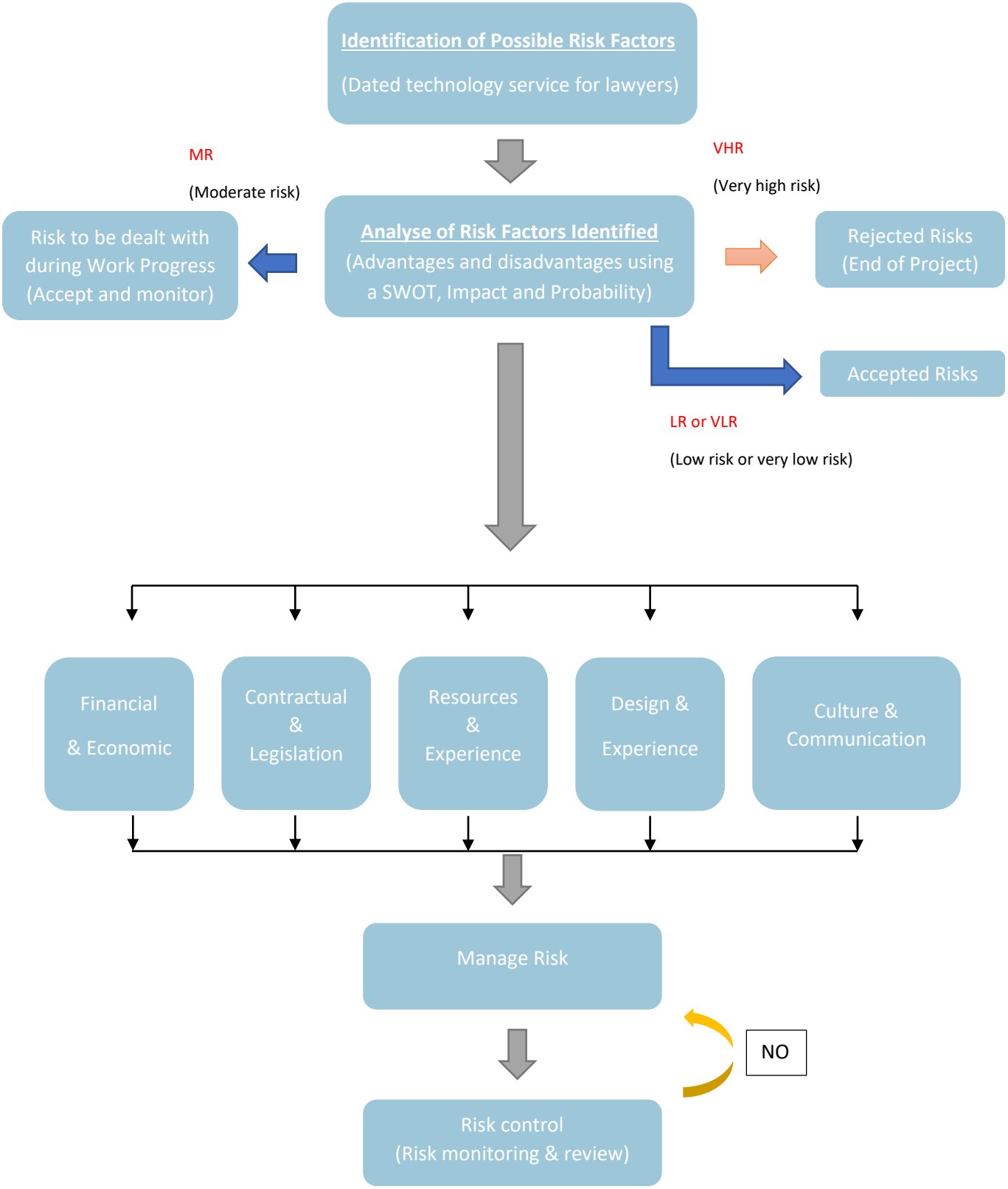
TASK 3. Risk Analysis Model

1. Risk Analysis Model

This risk analysis will help Womble Carlyle to identify potential dangers affecting business in a negative way. It will lead to make a right decision by looking at what negative impact is. There are two important steps for conducting risk analysis. The first step is identifying threats. We can consider potential threats as follows (WTO, n.d.):

- Project: budgets, key tasks, service, or product quality
- Technical: technical advances and technical failures
- Financial: an impact on company finances
- Operations: potential operation disruptions, a loss of assets

The second step is estimating risk. Once a company complete a list of potential threats, they should estimate the chances of the threats occurring and the description of potential impact.


Identification of Possible Risk Factors
(Dated technology service for lawyers)
MR
(Moderate risk)
VHR
(Very high risk)
Risk to be dealt with during Work Progress (Accept and monitor)
Analyse of Risk Factors Identified
(Advantages and disadvantages using a SWOT, Impact and Probability)
Rejected Risks (End of Project)
Accepted Risks
LR or VLR
(Low risk or very low risk)
Financial & Economic
Contractual & Legislation
Resources & Experience
Design & Experience
Culture & Communication
Manage Risk
NO
Risk control
(Risk monitoring & review)

2. Advantages and Disadvantage of Risk Analysis Model

This risk analysis model could give dynamic views and options to dealing with potential risks. I assigned risk assumptions to each different perspective, such as financial, legislation, communication, etc. It will provide more various approaches to expected risks and help to build more detailed risk actions. Moreover, the plan should be tested regularly. If the test failed, the company should consider going back to the previous steps and make sure to modify issues.

The disadvantage of this model is that it should be more detailed about numerical values, for example, the comparison of current risk score and last risk score. The numeric value is more efficient in determining the risks and will help to predict the consequences. We can also consider adding more detailed response activities and timeline.

CONCLUSION

This is my first attempt to build a risk assessment and a disaster recovery plan, so it could have many flaws. However, I have learned the importance of risk management and what kind of actions and preparations should be ahead to ensure business continuity, as DBA. It also provided a great experience for integrating and applying my knowledge of business analysis and data security. I will keep developing my insight with this lesson.

REFERENCES

IBM. (n.d.). *Example: Disaster Recovery Plan*. https://www.ibm.com/docs/en/i/7.1?topic=system-example-disaster-recovery-plan

Shield Geo. (n.d.). *Establishing and Managing a Remote Technical Team*. https://shieldgeo.com/establishing-and-managing-a-remote-technical-team/

Street, P. (January 17, 2022). *Business Continuity*. [Power Point]. Nova Scotia Community College. https://nscconline.desire2learn.com/d2l/le/content/227202/viewContent/3061166/View

TCii Strategic and Management Consultants. (January 31, 2012). *Writing A Disaster Recovery Plan.* https://www.mondaq.com/uk/operational-performance-management/162946/writing-a-disaster-recovery-plan

Vanover, R. (October 21, 2021). *What is the 3-2-1 backup rule?* https://www.veeam.com/blog/321-backup-rule.html

WTO. (n.d.). *Risk Analysis Guide and Tips.* https://www.wordtemplatesonline.net/risk-analysis-template/#google_vignette