MOBILE SOLUTIONS DEVELOPMENT

ASSIGNMENT 6

Computer and Application Security



SUBMITTED BY:

NIXIT AHIR(8748790)

SUBMITTED TO:

Prof.Parampreet Singh,

**Conestoga College Institute of Technology and Advanced Learning**

Contents

[Task 1 3](#_Toc120629288)

[Task 2 4](#_Toc120629289)

[Task 3 6](#_Toc120629290)

[References 7](#_Toc120629291)

# Task 1

Create a company and describe what service or product it provides. You may base this on your own experience, your own company, or create an entirely fictional business. Details to include:

* Company Name:
  + BI-Weekly services.
* What does the company do or provide?
  + Provide secure platform for handling payroll services for different organizations.
* How big is the company?
  + Large-sized business.
* What does your company require to be protected and why?
  + BI-Weekly services works with financial data for payrolls, as this data are sensitive and crucial we have to keep them securely backed up and store.
  + And this data should never be loosed or we cannot afford our service to stop, and that’s the prime reason for us to backing up data, protecting data and also keeping it confidential.

# Task 2

Disaster Recovery Plan:

Describe a backup and recovery plan for your company. Questions to consider and answer:

* What backup and recovery technologies (including hardware and/or software) would you use?
  + For back up and recovery of our data we are using **RAID 6** and **AWS Elastic Disaster Recovery (AWS DRS) [**cloud storage**].**
  + The reason for using RAID 6 is that RAID 6 is capable enough to handle simultaneous frailer of two disks and still be functional.
  + We will also following 3-2-1 rule for back up strategy.
  + The reason for using AWS Elastic Disaster Recovery is that it provides minimum downtime and data loss with fast, reliable recovery cloud storage.
* Is this backup for operational, recovery, archival, or a combination? Why?
  + This back up is combinational backup.
  + For our organization, as I mentioned provide services for payroll, which can be either weekly or bi weekly depending upon the companies policies that uses our services.
  + We are using combination of **incremental** and **differential backup**.
  + Also, our organization keeps data back up at multiple data center, so that frailer to a single data center won’t affect system.
  + And this back up will be **active/active** , not like a active/passive where if one data center goes down, that we transfer traffic to another data center.
  + **Active/active** might has some performance issue during single data center downtime.
* How often does it have to occur? Why?
  + For any organization the payroll can be generated either weekly or Bi weekly.
  + And the payroll generation date can varies organization to organization.
  + So our incremental back-up is going to be 24 hours every single day.
  + And for Full back up which will be done by every week.
  + In time of any disaster situation our system can afford data loss for around 6 hours. RPO = 24 hours.
  + To keep our RTO minimal we have used **active/active** back up strategy, which will help us to recover data in minimal time.
* How long will the backup take? Be sure to put some thought into the numbers when answering this.
  + This depend on many factor such as internet speed, data size and upload speed as well.
  + In ideal condition this back up will take few munities for the **AWS Elastic Disaster Recovery.**
  + For example, at 1gbps would take around 10 min to back up 100 GB of data.
* How resilient is your company to any downtime while the recovery takes place?
  + It depend on the outage time, however in the worst case it would take around 1 day as our incremental back up is around 24 hours.
  + However, **AWS Elastic Disaster Recovery (AWS DRS)** main advantage is thatit offers minimal down time, and It would be really rare that our multi-region active/active data center go down together, so it won’t go down in such situation.
* When does it have to occur? Why?
  + It can occurs in different situation, for example natural disaster at both of our backup data center. As we can not control those situation.
  + Machine failure for both data center.
  + Hacker attack to both data center.

# Task 3

* Advantages to your plan
  + The probability for system to go downtime is nearly 0 percent.
  + The downtime is minimal.
  + Affordable storage with AWS.
  + Offers point in time recovery.
  + Higher data accessibility with RAID 6 technology.
* Dis-advantages to your plan
  + Not cost effective
  + More complex back up structure.
  + Insufficient information management.
  + Not proper guidelines for how often recovery plan’s rehearsal should be performed.
* What, if any, limitations that you must place on your plan because of your company.
  + As our company works with client’s sensitive financial data, there is no comptonization for data recovery, protection to recovery.

# References

### Disaster recovery - AWS Elastic Disaster Recovery - Amazon Web Services

#### Disaster recovery - AWS Elastic Disaster Recovery - Amazon Web Services. (2022). Retrieved 29 November 2022, from https://aws.amazon.com/disaster-recovery/

### Archive vs. backup and why you need to know the differences

#### Archive vs. backup and why you need to know the differences. (2022). Retrieved 29 November 2022, from https://www.techtarget.com/searchdatabackup/tip/What-is-the-difference-between-archives-and-backups

### Foley, T.

#### Foley, T. (2022). Backup and Recovery Methods for Financial Institutions. Retrieved 29 November 2022, from https://www.thinkstack.co/blog/backup-and-recovery-

### Elliott, J.

#### Elliott, J. (2021). What is the 3-2-1 Backup Rule?. Retrieved 29 November 2022, from https://www.uschamber.com/co/run/technology/3-2-1-backup-rule