**University of Toronto  
School of Continuing Studies  
Foundations of Enterprise Architecture**

Individual Assignment 2

## You have been hired as an Enterprise Architect of a medium enterprise for over six months now (you can use your own enterprise for this assignment). Your organization has approached you to develop a plan to create a Cloud-based Disaster Recovery (DR) option. Your manager made the argument that we should have an on-premise solution as oppose to a cloud-based solution. Your director seems to be more progressive and wants you to make a case for a cloud solution.

1. **Describe in detail what a cloud-based disaster recovery entails.**

Cloud based *Disaster Recovery* is non-productive environment, it is commonly a secondary environment that is maintained for use in certain disaster scenarios that is something that can occur anywhere. From natural disaster to location disaster, power outages, physical or cyber-attack as well as human disaster, which is the most prolific disaster. Thanks to Cloud Computing elasticity nature, the *DR* cost went down significantly allowing you to pay for what you use. Moreover, gain the ability to test *DR* procedures more frequently.

1. **What will be your strategy to come up with an on-premise solution to a cloud-based solution?**

When enterprises move their workloads and data to the cloud, their on-premises datacenters still keep playing an important role. The term *hybrid* *cloud* consists in a combination between *public cloud* and *on-premises data centers* (local), in order to create an integrated IT environment that includes both. Some companies utilize *hybrid cloud* as a strategy to migrate their whole datacenter to the cloud in long term. Other organizations use cloud services to extend their existing on-premises infrastructure.

1. **Propose a set of objective arguments for and against cloud-based DR solution**.

Having cloud-based *DR* reduces the necessity for data center space, IT infrastructure as well as IT resources, which leads to significant cost reductions, enabling smaller companies to deploy disaster recovery options that were previously only found in larger enterprises. Reduce on premises infrastructure allowing you to remove aging technologies that sometimes is not reliable. To offer the right level of DR services to meet the needs of the user in their organization.

But disaster recovery in the cloud is not a perfect solution, and its challenges need to be clearly understood before a firm venture into it. It is not all-or-nothing thing. It is necessary to do an assessment to determine is crucial and what is tolerable *BIA*, it means, define priorities. It is important to define properly RTO and RPO suitable for each company to encompass their regulations, policies in case of a disaster.

1. **Use APSA for your analyses.**

A Business impact analysis *BIA* differentiates critical and non-critical organization activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected mainly by the cost of recovery solutions. A function may also be considered critical if dictated by polices regulations or law. For each critical function, two values are assigned

* **Recovery Point Objective** *RPO* – Tolerable latency of data that will not be recovered.
* **Recovery Time Objective** *RTO* – Tolerable amount of time to restore the function.

The recovery point objective must ensure that the maximum acceptable data loss for each activity is not exceeded. The recovery time objective must ensure that the *Maximum Tolerable Period of Disruption* (*MTPoD*) for each activity is not exceeded. Moreover, the impact analysis results in the recovery requirements for each critical function.

Recovery requirements consist of the following information:

* The business requirements for recovery of the critical function
* The technical requirements for recovery of the critical function

When designing your disaster recovery plan, choose targeted strategies that address companies’ specific use cases. For example, in the case of historical compliance-oriented data, you probably don't need speedy access to the data; however, in the event that your service experiences an interruption, you'll most likely want to be able to recover both the data and the application as quickly as possible. It isn't enough to simply have a plan for backing up or archiving your data. Make sure your disaster recovery plan addresses the full recovery process, from backups to restores to cleanup.

1. **Develop a list of key criteria and considerations to help you evaluate both options.**

The analysis phase begins with the business impact analysis, during which the following activities take place: critical business processes, systems, personnel, records, and data are identified, any contractual commitments made for business continuity are collected, recovery priorities are set, internal and external dependencies are documented, financial impacts for outages are quantified.

This process may be iterative, requiring one or two passes by key business users and senior management. It also involves providing training to such individuals who may not be familiar with business continuity planning or the meaning of RPO and RTO.

It is expected that some users to define very stringent *RPO* and *RTO* numbers when the business need is not entirely clear; accept that these figures could be reconsidered once the cost of the resultant recovery solutions becomes clear to them during the design stage.

It is also necessary to understand the detail behind the RTO. For example, if an RTO is set at 3 days, does this business process need to be restored completely? Or could it be recovered in stages?

*RTO* is not always a single number for an organization. There may be different *RTOs* by business, department, function, geography, application system, or system platform (mainframe, web, server, etc.).

*RPO* and *RTO* numbers have been generated by the *BIA* process and by business users, and have been signed off by management.

**RPO:** *Recovery Point Objective*

**RTO:** *Recovery Time Objective*

**BIA:** *Business impact analysis*

**MTPoD:** *Maximum Tolerable Period of Disruption*

**APSA:** *Architecture, Privacy, Security and Accessibility*

**DR:** *Disaster Recovery*

***Reference:***

***Wikbon*** *:*

[*http://wikibon.org/wiki/v/Recovery\_point\_objective\_-\_recovery\_time\_objective\_strategy*](http://wikibon.org/wiki/v/Recovery_point_objective_-_recovery_time_objective_strategy)

**TechTarget***:*

<https://searchdisasterrecovery.techtarget.com/definition/cloud-disaster-recovery-cloud-DR>

**Wikipedia:**

<https://en.wikipedia.org/wiki/Business_continuity_planning>

**Cloud Google***:*

[*https://cloud.google.com/solutions/designing-a-disaster-recovery-plan*](https://cloud.google.com/solutions/designing-a-disaster-recovery-plan)

**YouTube Journey Through the Cloud - Disaster Recovery:**

<https://www.youtube.com/watch?v=YFuOTcOI8Bw>