**Assignment**

**Brief**

Migration to cloud is not a trivial work. It involves detailed analysis in migrating large set of data, complex softwares, and sophisticated IT processes from one place to another. In this assignment, learners will be group in 3 to research on the given challenges and provide the best solutions they could garner.

Note: At this time, learners are led to become exposed to more cloud infrastructure related topics at a high level. The depth of learning will come in later part of the lessons.

**Challenge 1 - Compatibility Issue**

Scenario: Your superior wants to leverage on serverless technology as it eliminates operational overheads but the software is not serverless ready.

**Challenge 2: Vendor Lock-in**

Scenario: You have picked Cloud X as the destination of your migration only to find out that you'll better with Cloud Y as your technology scale.

**Challenge 3: Processes & Policies**

Scenario: Locally (in data center) configured security policies is not identical to the policies architecture in the Cloud. The deployment process of the current IT Operations Team may not fit well with the Cloud's.

|  |  |  |
| --- | --- | --- |
| **Challenge #** | **Describe the challenge with assumptions** | **Proposed Solution(s)** |
| 1 | Assuming that the businesses in question are in highly regulated sector, as such, the company is unable to make the leap into cloud for a certain part of business, the decision may already be made as to whether to house the software and related sensitive services applications on premise to do business. In addition, other considerations include: on-premise applications are reliable and allows enterprises to maintain a level of control that cloud often cannot. | Not every aspect of the company needs to move into the public cloud. A hybrid cloud solution can be offered as a solution, which enables enterprise to deploy their sensitive applications in a private cloud (constructed either on premises or through a hosted private cloud provider) to make greater data protection and move other lesser sensitive services along with its infrastructure into public models to make a huge savings by eliminating operational overheads. This hybrid model allows enterprise to combine deployment models to fit their business needs e.g. compliance and control for data privacy. The downside to adopt multiple cloud systems is that it increases the complexity of managing their services and the hybrid company will pay for both private and public cloud usage. |
| 2 | This challenge involves moving our workloads from one cloud to another cloud, which is known as vendor lock-in. As such we assume that the business has taken steps to avoid cloud vendor lock-in before they first make move into the cloud. Typical best practices are as below: identify complex dependencies; understand the commonalities; consider upgrading before migrating; make apps aligned with open standards; ensure portability once migrated; adopt modern SDLC methodologies; develop a multi-cloud strategy and where possible establish a clear exit strategy. Most of the steps mentioned above are designed to be technology-independent of cloud service management and operations. | Multicloud solution can be considered as there are certain reasons why we choose one provider over another as a certain provider specialize in providing a certain type of service e.g. here Cloud Y is specialized in technology scale whereas Cloud X can reduce latency for serving users from data centres, which are closest to them. The downside of using multicloud is the complexity of dealing with many different services and multiple platforms, which involves training teams to use multiple cloud systems. |
| 3 | Assuming that the enterprise in question operates under some form of regulatory control and possesses extra sensitive information , as such, it is imperative that the enterprise remains compliant in the sense that the data must be protected at all times. The enterprise must have a certain level of security and privacy that an on-premises environment provides. Should enterprise choose cloud computing model, the management must do their due diligence and ensure that the cloud provider is up to code and compliant with all regulatory mandates within the industry. | Security and Compliance is a shared responsibility between AWS and Customer. This differentiation of responsibility is commonly referred to as Security of Cloud for AWS versus Security in the Cloud for Customer. As such, customer responsibility will be determined by the AWS Cloud Services which a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. This means that as a customer for the cloud, the enterprise still retains control of the security it chooses to implement to protect its content, platform, applications, system, and networks no differently than the enterprise would in an on-site data centre. |