**Risk Assessment Report for Ozmart Retail Group Cloud Migration**

**Overview**

It is a Risk Assessment Report that is centred on the technology risks that surround the process of implementing Ozmart Retail Group’s IT framework in cloud with AWS services. Thorough documentation of the methodology, major technical threats put to consideration, assumptions made in the process and most importantly, measures that were taken to address these threats, is provided in the report. The is to achieve a smooth migration with minimal impact to the systems, yet at the same time keep all relevant systems safe and operational.

**1. Risk Assessment Process**

The risk assessment for the cloud migration project involved the following technical steps:

1. **Technical Risk Identification**: As for the second characteristic, it should be mentioned that the project team provided extensive covering of all the technical aspects of the cloud migration. These included what was currently in the network, the workings of the applications, how data is transferred and how cloud services are set up. Challenges were evaluated with regards to risks that might be arising from possible weaknesses, system conflicts, and performance lag that might be realized during the migration process or afterwards.
2. **Technical Risk Evaluation:** The risks identified had to be put under scrutiny depending on the effects that they could impose on the system in the aspects of performance, security, and data accuracy. An evaluation of the probability of each risk arising was made from historical precedent, technical difficulty, and the status of IT systems. A risk matrix was developed for these risks with regard to those that would be most damaging to business operations or data.
3. **Technical Risk Mitigation Planning:** Risk treatments are technical and in the case of every high-risk factor, a technical risk management plan was prepared. This encompassed choosing the right cloud services, deploying necessary security measures, choosing the right tools for monitoring and alerting as well as thinking of disaster recovery mechanisms.
4. **Continuous Technical Monitoring and Review:** It was built a model and installing AWS System Cloud watch and other monitoring tools to tracks risk 24/7 to identify the anomalous events or any codes that are trying to completely compromise the system. Technical reviews were planned at periodic intervals to evaluate the outcomes of the envisaged control measures and make further refinements, if necessary.

**2. Technical Assumptions**

During the risk assessment, several technical assumptions were made:

* **Cloud Service Performance:** For this work, it was assumed that AWS services like EC2, S3 and RDS would act as advertised as well as their stated throughput and performance under different loads and time.
* **Data Transfer Reliability:** It was believed that transferring data on the AWS from the on-premises systems would be safe and efficient through using AWS Direct connect and Virtual private connections for this purpose.
* **Security Configurations:** AWS security tools like VPC, Security Groups, IAM roles, and encryption would be implemented appropriately in order prevent illicit access as well as data loss.

**3. Key Technical Risks and Mitigation Strategies**

1. **Data Loss During Migration:** Some of the risks include data corruption when in the process of transferring it to AWS S3 or RDS.
   * **Mitigation:** Store your data using AWS Data Sync to perform secure transfers, implement multi-region backups, and verify data checksums or by using AWS Glue.
2. **Network Configuration Errors:** This is because misconfiguration of VPC or subnets or security groups may result to network failures or insecurity.
   * **Mitigation:** It recommended to use CloudFormation templates for creating VPCs to ensure that they are created and set up correctly, to regularly perform compliance checks utilising AWS Config and to review rules established for security groups.
3. **Application Compatibility Issues**: There might be issues of compatibility of the legacy applications with the AWS environment hence the applications may slow down.
   * **Mitigation:** For compatibility testing, carry out a test in an AWS sandbox, utilize AWS Application Discovery Service to discover the dependencies of applications and adjust the applications if they are not compatible with the cloud platform.
4. **Insufficient Security Measures**: Lack of proper security measures would result in vulnerability to break-ins and consequent boasts to sensitive data.
   * **Mitigation**: Implement IAM security by following AWS Identity and Access Management Best Practices, deploy AWS Shield to help protect against DDoS attacks, mandate MFA and employ AWS Key Management Service (KMS) when it comes to encryption.

**4. Conclusion**

A recent technical risk evaluation of Ozmart Retail Group cloud migration project I defined the following critical risks. These risks can be minimized by the appropriate provision of oriented technical controls and the constant scanning of AWS environment; thereby making Ozmart’s transition to cloud environment secure and frictionless. Some of the changes that it will be crucial to conduct periodically may include the following; The risk- mitigation instruments need to be updated from time to time given that the nature of threats change over time, to ensure that the integrity and performance of cloud systems are preserved.