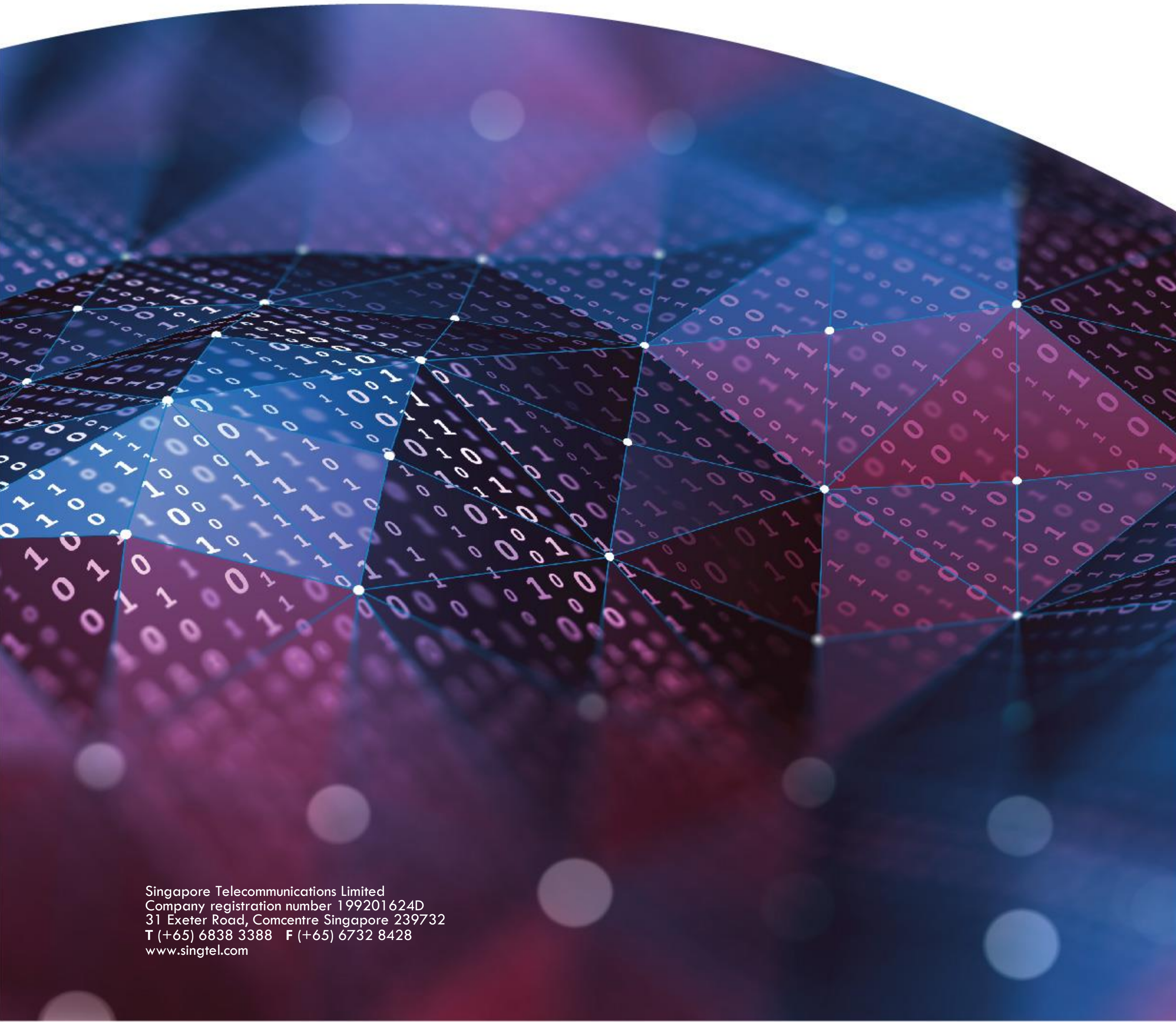
Singtel Group Enterprise

Public Cloud Services Partner Panel RFP

v3.7



Singapore Telecommunications Limited
Company registration number 199201624D
31 Exeter Road, Comcentre Singapore 239732
T (+65) 6838 3388 **F** (+65) 6732 8428
www.singtel.com

Request for Proposal

RFP No. ________________________

INVITATION: Proposals, subject to the attached conditions, shall be received on or before **5th July 2021 @ 12:00 PM, local time** for a Cloud Day 1 Professional Services Panel described below.

The Vendor must submit collaboration proposals addressed to:

The Evaluation Committee
Cloud Day 1 Professional Services Panel
Singtel Telecommunications Ltd

This document contains proprietary and confidential information of or relating to the Singtel Group of companies, which is provided for the sole purpose of permitting the recipient to respond to the Request for Proposal (RFP) submitted herewith. In consideration of receipt of this RFP, the recipient agrees to maintain such information in confidence and not to use, reproduce or otherwise disclose this information for any other purpose or to any person outside the group directly responsible for responding to its contents.

There is no obligation to maintain the confidentiality of any information that was known to the recipient prior to receipt of such information from the Singtel, or becomes publicly known through no fault of the recipient, or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to Singtel. No warranty is made as to the accuracy, completeness or adequacy of the information set out in the RFP and the recipient shall rely solely on its own independent judgment and analysis in evaluating the requirements, adequacy and suitability of any submission in response to the RFP or otherwise.

Contents

1. Background

Asia's leading communications technology group

Singtel is Asia's leading communications technology group, operating in one of the world's fastest growing and most dynamic regions. Besides core telecom services, we provide an extensive range of digital solutions. This includes cloud, cyber security and digital advertising to enterprises as well as entertainment and mobile financial services to millions of consumers. We are dedicated to continuous innovation, harnessing next-generation technologies to create new and exciting customer experiences as we shape a more sustainable, digital future.

1.1 Overview of the RFP

Singtel is looking to appoint Cloud Professional Services delivery vendors to completement Singtel's existing Hybrid Cloud Professional Services capabilities and help our Enterprise Customers accelerate their respective Cloud Transformation projects in Singapore and overseas. Potential Cloud Services providers will be selectively invited to participate in this RFP.

1.2 In-scope Entities

The scope of the RFP includes Singapore Telecommunications Ltd ("Singtel") and its Global Offices for support of its customer projects. Other Singtel entities may be included over the contract term at the sole discretion of Singtel.

1.3 Key RFP outcomes and Term

This RFP is aimed at selecting one or more Cloud Professional Services Delivery Vendors to work with Singtel on customer projects over a 1 year term with an option to extend for another 1 year.

1.4 Timelines

The following table lists the activities relevant to the RFC process. The Singtel Group reserves the right to change these activities and/or timelines and will notify the vendor in such cases.

No.	Milestone	Date
2	Release of RFP Document	21st June 2021
3	Vendors to submit RFP	5th July 2021

1.5 How to read this RFP

It is mandatory to fully address all aspects of Sections 2 to 8 when responding to this RFP.

- To prevent any confusion about identifying requirements in this RFC, the following definition is offered: The word "shall" be used to designate a mandatory requirement.
- The vendor shall respond to the requirements in this RFP by indicating items of non-Compliance "NC" as appropriate and furnish details and propose alternative clauses for each clause marked for non-Compliance "NC" to facilitate Singtel's assessment and evaluation of the responses and overall collaboration proposition.
- Compliance Tables are to be strictly followed and vendors are advised not to remove or add columns, otherwise section would be classified as non-Compliance "NC".

1.6 Pre-Requisites

By participating in the RFP, the vendor accepts Singtel's Procurement Policies as stated in https://www.singtel.com/about-us/tenders, in particular the :

Singtel's Whistle-blower Policy as outlined in :
https://www.singtel.com/about-us/company/corporate-governance/whistleblower-policy

Singtel Group Supplier Code of Conduct as outlined in :
https://www.singtel.com/content/dam/singtel/about-us-singtel/tender/singtel-group-supplier-code-of-conduct.pdf

Singtel Standard Terms and Conditions as outlined in :
https://www.singtel.com/content/dam/singtel/about-us-singtel/tender/singtel-standard-terms-and-conditions.pdf

The RFP shall also be administered on the Ariba Network. Please refer to the guide for supplier registration and bid submission process in Ariba Network :
https://www.singtel.com/content/dam/singtel/about-us-singtel/tender/ARIBA-Singtel-Supplier-Training-(Sourcing).pdf

Upon Award of the RFP, the successful Tenderer will be required to execute the Singtel Group Master Supply Agreement (GMSA), Services Module, and an SOW associated with the RFP.

All pricing to be quoted in Singapore dollars. Proposals shall remain valid 6 months from the submission of the RFP.

2. About the RFP

2.1 Overview of the RFP

The RFP will have 2 areas of Focus:

1. Public Cloud (AWS, Azure, GCP) – Base SOW
2. Public Cloud (AWS, Azure, GCP) - Resource Rates (Man-days for certified personnel)

2.2 Singtel Professional Services for Hybrid Cloud environments

Singtel is passionate about creating technologies and services that help Enterprises and Public Sector organizations succeed. Our Professional Services team delivers transformation services to help enterprise customers as they shift to a cloud-based operating model and incorporate Cloud services into their overall architecture, whether on Public, Private or Hybrid Cloud environments.

Our Professional Services teams work together with customer teams and our Public or Private Cloud partners to provide deep expertise in the architecture, design, development, and implementation of cloud computing initiatives that result in real business outcomes.

In addition to delivering standardized services, the Professional Services team builds customized solutions that accelerate Hybrid adoption and provide meaningful customer insights that help address immediate challenges and form roadmaps for continued development. The variety of customers, partners, and technology challenges Singtel Professional Services consultants encounter gives them unprecedented exposure and experience to address even the most complex of customer challenges.

2.3 Public Cloud (AWS, Azure, GCP) – Standard SOW

Businesses are embracing the cloud to gain scalability, agility and cost efficiencies and as a result, looking to migrate existing applications and data to new cloud environments. Moving enterprise applications and data outside the data center to the cloud is no easy task. Expertise, tools and planning help ensure all bases are covered including costs, security, governance and staff training.

Singtel has developed Standard SOWs to help Customers with their different Cloud transformation projects. The vendor is to perform the base SOWs listed in Appendix A to J.

These are:

Public Cloud (AWS, Azure, GCP)

- Landing Zone Design

- Migrations – Windows Server
- Migrations – Microsoft SQL
- VMware on AWS

The vendor shall propose additional enhancements to the standard SOWs. Such enhancements may be included in the standard SOW during the BAFO stage of the RFP at the sole discretion of Singtel whether it was proposed by the vendor or other vendors.

The vendor shall propose the pricing to deliver the standard SOWs in Appendix A to J.

2.4 Public Cloud (AWS, Azure, GCP) Resource Rates (Man-days for certified personnel)

Cloud transformation projects vary on scale, duration, cost and complexity. Where the customer's requirements extend beyond the base-SOW, Singtel will work with the selected vendors to provide the necessary level of expertise for customer projects. The vendor will work with Singtel on the SOW for specific customer projects and provide the right level of expertise as requested by Singtel.

The vendor is to propose (i) on-site and (ii) offshore man-day rates for certified personnel. This shall include but not be limited to :

Public Cloud (Associate, Professional or Specializations levels)

- AWS certified personnel
- Azure certified personnel
- GCP certified personnel

The vendor is to propose the respective man-day rates for the specific requirements for Cloud certified personnel within the template provided in Appendix O.

3. Manpower Services

As the trusted Cloud Service Provider to our Customers, Singtel has to ensure that all Customer Projects are delivered to a high standard and on-time. The vendor is to outline your Cloud Professional Services Capabilities, including the Certifications and Competencies in Public, Private and Hybrid Clouds, including number of delivery personnel in Singapore and overseas, as well as frameworks and methodologies. Please complete the attached table in Appendix J.

4. Customer References

Many customers—including the fastest-growing start-ups, largest enterprises, and leading government agencies—are using Cloud to lower costs, become more agile, and innovate faster. Customer references are consistently recognized by successful Cloud Organizations as one of the top reasons they are selected by net-new customers.

Customer references give you the opportunity to highlight previous successes and demonstrate how your organization can solve current business challenges for Singtel's customers. The vendor is to outline a list of Customer Projects in Singapore and overseas, and highlight the Customer's challenge, objectives, complexities of the project, why you were selected, and how did you differentiate your company from the competition.

Please submit your Customer References in the table attached in Appendix K.

5. Key differentiators

Please highlight your key differentiators and the unique value proposition which your company can brings to Singtel and its customers. Please highlight your key differentiators in Appendix L.

6. Contract Terms and Conditions

Upon successful award of the RFP, the selected vendor (s) is / are required to execute :

1. The Singtel Group Mater Supply Agreement (GMSA)
2. Services Module
3. Statement of Works

By participating in the RFP, the vendor accepts all terms in the GMSA and Services Module as shown in Appendix M, and will in good faith work with Singtel to finalise the Statement of works within 2 weeks from the award of the RFP.

7. Governance

The Vendors shall propose a Collaboration Governance structure to function as a decision-making body within the collaboration framework, that consists of top managers and decision makers who provide, review and monitor strategic direction and policy guidance to the collaboration working teams and other stakeholders.

The Collaboration Governance model shall include regular deal cadences, project reviews, escalation and support paths to ensure Customer Projects are delivered successfully.

Please submit a governance structure in Appendix N.

8. General Information for Partners

8.1 Single Point of Contact

The Vendor shall appoint a Single Point of Contact (SPoC) for this RFC. The SPoC will serve as the primary contact for all communications related to this RFC.

8.2 Certification of Non-Collusion

The Vendor shall certify that the collaboration proposal is submitted without collusion, fraud or misrepresentation as to other proposing Vendor, so that all proposals for the collaboration will result in free, open and competitive submissions.

8.3 Right of Modification (Addendum)

The Singtel Group reserves the right to add, modify or alter the requirements in the RFP document. The Singtel Group may advise Vendors of any altered, additional or modified requirements by email or such other means as may be deemed suitable at the sole and absolute discretion of Singtel in the form of an Addendum. An e-mail from Vendors acknowledging receipt of the addendum will be requested. The failure of the Vendors to provide the said acknowledgement shall not be evidence that they have not received the notification of any addendum and it shall be the responsibility of the Vendors to ensure that it receives any addendum that has been released by the Singtel Group, and the Singtel Group shall bear no responsibility whatsoever due to the failure of any Partner from receiving the award due to the failure of the Vendors to receive any addendums for any reason whatsoever.

8.4 Right to the Use of Information

The Singtel Group may use and make copies of any Response or offer from the Vendors for the purpose of evaluation, clarification and finalizing any definitive agreements. Singtel will retain all Responses or offers. The Vendor represents to Singtel that it owns all intellectual property contained in the Response or offer and the Vendors shall indemnify the Singtel Group against any Third-Party or any other claims that may arise out of or in connection with any use by The Singtel Group of the information supplied in a Response or offer.

8.5 Oral Communication not binding

The Singtel Group shall not be bound by any oral advice given or oral information furnished by any Singtel Group officer, employee or agent of the Singtel Group in respect of the RFP. No negotiations, decisions, or actions shall be executed by any Partner as a result of any discussions with any Singtel Group employee, officer or agent prior to the execution of the Collaboration Framework Contract with the Vendor.

8.6 The Singtel Group Discretion

The Singtel Group may in its sole and absolute discretion:

- Reject any response where the Singtel Group is of the view that the response does not comply with the RFP documents in any respect.

- Reject any response with caveat imposed on the pricing or discount validity or otherwise e.g. time bounded discount.
- Decline to consider any and/or all response(s) (confirming or otherwise) regardless of its financial or technical merit.
- Contact the Vendor in writing for further details with respect to their response.
- Interpret and apply any provision of the RFP in such manner as it deems fit, such interpretation and application shall be conclusive and binding on the Vendor.
- Decide to award or decline to award the Contract to any Partner without assigning any reason therefor.

8.7 RFP Terms Incorporated as part of Contract

The Singtel Group reserves the right to award or not to award the RFP (whether in whole or in part) at its sole discretion. The Vendor awarded the RFP or any part or module or component of the RFP agrees that the terms and conditions of this RFP shall be deemed incorporated, along with all other submissions and written correspondence concerning this RFP which are expressly accepted or provided by the Vendor, into the contract(s) for the RFP or such part or module or component of the RFP.

8.8 RFP and response as property of the Singtel Group

The Singtel Group owns all intellectual property rights in the RFP. Nothing in the RFP shall be construed as an agreement to assign any intellectual property in this RFP to any Partner. All written Response submission material shall become the property of the Singtel Group, and the Singtel Group shall be entitled to retain the same.

8.9 Right of additional information without liability

The Singtel Group shall not be liable in any circumstances for any costs or expenses incurred including, without limitation, the costs of submitting additional information, preparation for an attendance at meetings by the Partner in compiling its Response or participating in this RFP regardless of, without limitation, the conduct or outcome of the Response evaluation and selection process.

8.10 Right of Termination or Modification without Liability

The Singtel Group may terminate the process set out in this RFP at any time or alter the process, from time to time, in its absolute discretion. Without limitation, the Singtel Group shall not at any time be liable for any cost, loss, damage, charge, expenses or payment which a Vendor suffers, incurs or is liable for in respect of the termination or alteration of the process.

8.11 Non-Solicitation of Supplier

During the contractual period of this SOW and 2 years after, the Supplier shall not, without the prior written consent of Singtel, persuade or encourage any business partners or business affiliates or End Customers to cease doing business with Singtel and/or any of its Affiliates or End Customer. The Supplier should also provide Singtel the first right of refusal to jointly participate in any new business opportunities arising from this RFP

Appendix A -Landing Zone Design – AWS

1. Overview

The Vendor is to set up a landing zone on AWS cloud. A foundational setup, when implemented, will provide, the end-customer with an AWS environment upon which either new applications can be implemented, or existing applications can be migrated. This shall be achieved with the help of AWS Landing Zone that takes into consideration the Well Architected Principles of AWS. The key ingredients of a Landing Zone are given below:

- Multi account strategy
- Account Security: Ensuring account access is not compromised
- Compliance: Ensuring correct processes are actualized
- Logging: Secured audit trail, logs for all AWS Cloud activity
- Networking: Shared Services with connectivity to physical Data center, internet

The Success criteria of the engagement will be defined as follows:

- Centralization of billing and identity management
- Attribution of costs to various departments
- Centralized Governance of Cloud infrastructure
- Approved custom Landing Zone design
- Implementation of fully automated custom Landing Zone
- Establishment of Security best practices with no red flags at the end of the implementation against CIS benchmarking on Landing Zone accounts
- Centralised user access management

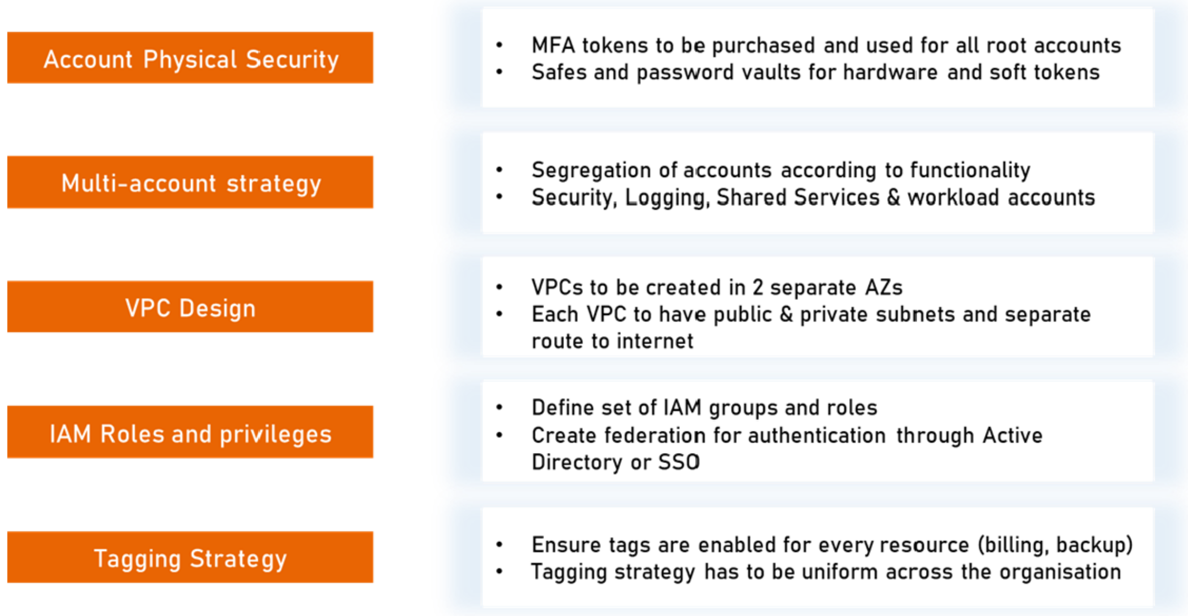
2. AWS Landing Zone Solution Overview

2.1. Goal

- To provide a strategy and set of high-level recommendations to be used by an Account Bootstrapping Pipeline to apply standard configuration to all AWS accounts, which will bring them to a secure and compliant baseline
- To ensure that all actions taken within an account are logged and stored in a secure location in a dedicated AWS account
- To ensure that point-in-time configurations of all resources in an AWS account are taken and stored in a secure location
- To ensure that the master account has full visibility into the sub accounts in terms of billing as well as the services being used
- To ensure that the master account has the capability to create service control policies to govern and manage the AWS accounts being used by different entities in the company and as per regulatory law

- To ensure that the servers currently running in the AWS environment are migrated to the new landing zone.
- To ensure application is hosted in secure AWS region within prod and non-prod environments

2.2. Key Areas for Designing an AWS Custom Landing Zone



Account Physical Security

- MFA tokens to be purchased and used for all root accounts
- Safes and password vaults for hardware and soft tokens

Multi-account strategy

- Segregation of accounts according to functionality
- Security, Logging, Shared Services & workload accounts

VPC Design

- VPCs to be created in 2 separate AZs
- Each VPC to have public & private subnets and separate route to internet

IAM Roles and privileges

- Define set of IAM groups and roles
- Create federation for authentication through Active Directory or SSO

Tagging Strategy

- Ensure tags are enabled for every resource (billing, backup)
- Tagging strategy has to be uniform across the organisation

2.2.1. Account Physical Security

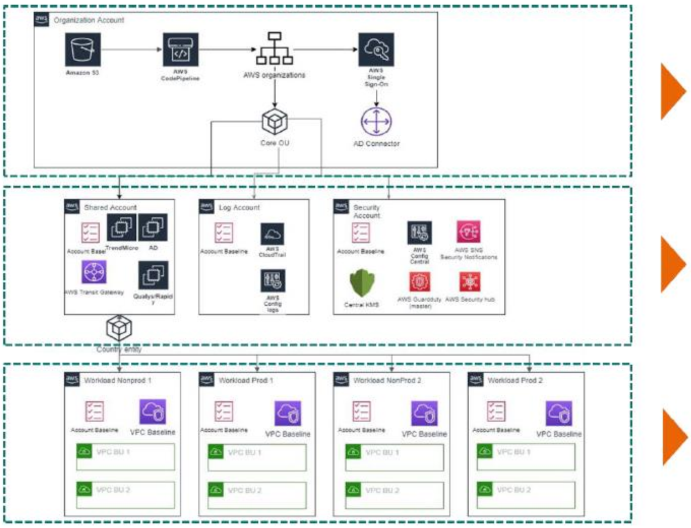
MFA tokens shall purchased by the end-customer for the initial set of AWS Accounts. To ensure compliance of the Root credentials, end customer shall also provide a lockbox or safe is required to store MFA tokens. It is highly recommended that the lockbox be dual key, and a dual stakeholder model is implemented to gain access to said credentials. Root Password should be stored in a reputable Password Manager such as KeePass 2(with associated replication), 1Password 3(with associated teams accounts) or CyberArk4

2.2.2. AWS Organization (Master) Account

This AWS account will also act as a master or root account to which Vendor will integrate all other end-customer AWS accounts. The AWS Organizations account will provide an ability to manage the accounts in terms of security as well provide the group an overview of the billing being incurred by the managed member accounts. The Master account will be used for-

- A single consolidated billing dashboard will be setup for a single payment method for all AWS accounts used in this solution, also an a read only role would be provided to the users in the organizations account so as to have a holistic view of the billing being incurred by individual accounts.

- This Organization account will host minimal services as this account will be used only for management purpose, such as Service Control Policies (SCPs), AWS Single Sign- On (SSO), and customer Azure AD authentication configuration
- For centralized management for group companywide a user with the role to access the billing dashboard and SCP would be created.
- The Organization account will also be the the master account that will link to all other accounts as shown in the figure below:



- The Organisation account for AWS SSO, creating organisation, AD connectivity
- AWS SSO also needs to be configured here

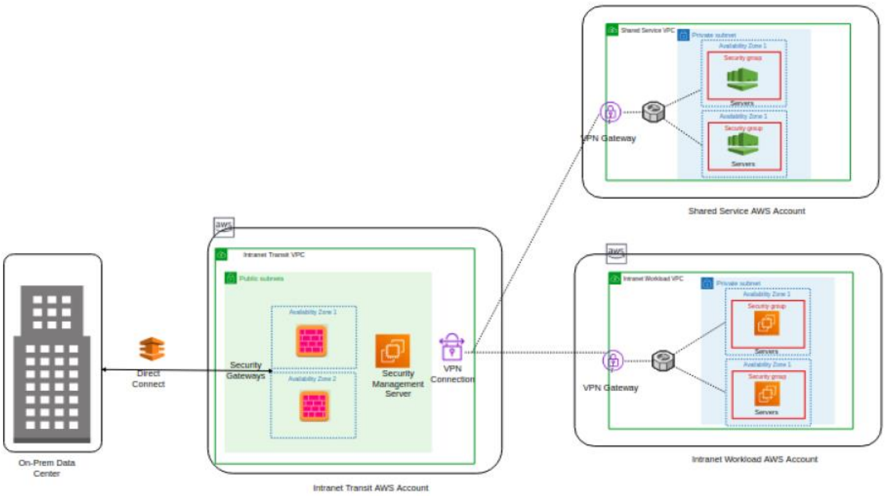
- Shared Services & Security/Logging accounts
- All Security tools, logs and patch services to be present in these accounts

- Workload accounts for production and non-production environments
- All applications (public and internal) to be hosted here

2.2.3. Shared Services Account

The Shared Services account is a reference for creating infrastructure shared services such as directory services. By default, this account hosts AWS Managed Active Directory for AWS SSO integration in a shared Amazon Virtual Private Cloud (Amazon VPC) that can be automatically peered with new AWS accounts created with the Account Vending Machine (AVM).

- Vendor will provision this AWS account to host a set of shared services which are common across all other accounts such as-
- Bastion Hosts
- Active Directory Service
- Centrally Managed Shared Golden AMIs
- EBS and other Centralized backups
- Centralized DNS
- DevOps Toolchain
- Next generation third-party firewalls (if required)



The Shared Services account will host the Bastion hosts which will be used by OS administrators to logon to the instances of production and non-production workloads as OS level. The Shared Services account design will take the maximum amount of time and will be an integral part of the network design. The following components need to be decided while designing the Shared Services Account:

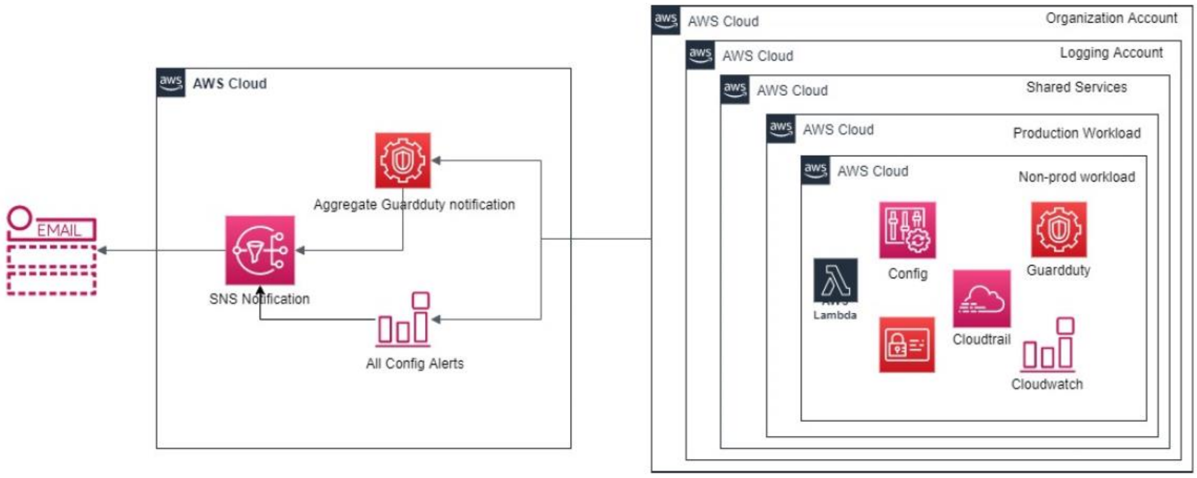
- Communication with other accounts
- Communication with on-premise or other clouds
- Transit gateway design and set-up
- Communication between VPCs

2.2.4. Security Account

Vendor will configure the Security Account aggregate the security and config events from all other AWS accounts using one or more of the following services:

- AWS Config
- AWS CloudTrail
- CloudWatch Alarms
- AWS GuardDuty

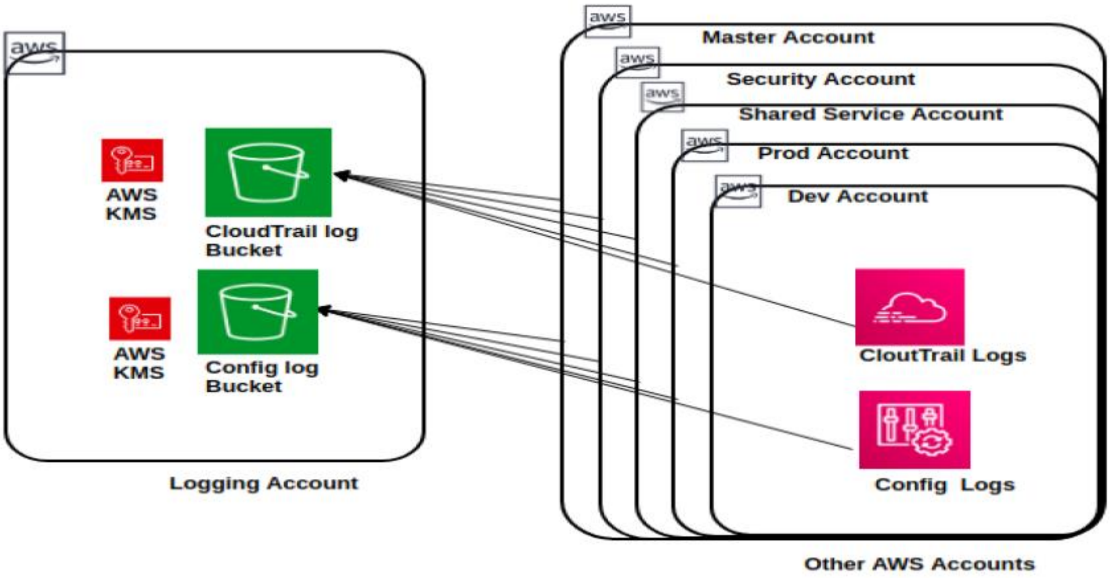
Thereafter, these alerts and notification will be forwarded to appropriate SNS topics subscribed for security and AWS config notification.



2.2.5. Log Archive Account

Vendor will configure the logging account to centrally store CloudTrail and Config logs from all other accounts.

- This account will be completely isolated from all other AWS accounts.
- It will not host any service other than S3 buckets to store CloudTrail and Config logs sent from the other accounts.
- All the logs in the logging account will be encrypted using AWS KMS service.



2.2.6. Workload Accounts

Vendor shall configure the workload accounts to host the applications. Typically, the number of workload accounts have to be determined based on the objectives. The factors that influence the total number of workload accounts as well as the design of each account are as follows:

- Segregation with respect to environments, namely separate accounts for non-production and production workloads
- Segregation based on business units using the applications hosted in a workload account
- Segregation based on the type of applications hosted, such as internet and intranet workloads
- Segregation based on the country using the workload account

2.2.7. Network Design

Vendor is to ensure the Network design is based on the multi-account strategy described above. The design will be enhanced, and granular level of details will be implemented after discussions with the customer architects. One important consideration for the network design will be to allow or disallow internet connectivity to the different AWS accounts. As a rule of thumb, only the Shared Services account will have internet gateway attached to it whereas the workload accounts will by default not have any internet access although provisions will be kept enabling that if required. Based on the internet availability of the accounts the workload accounts will be classified as follows:

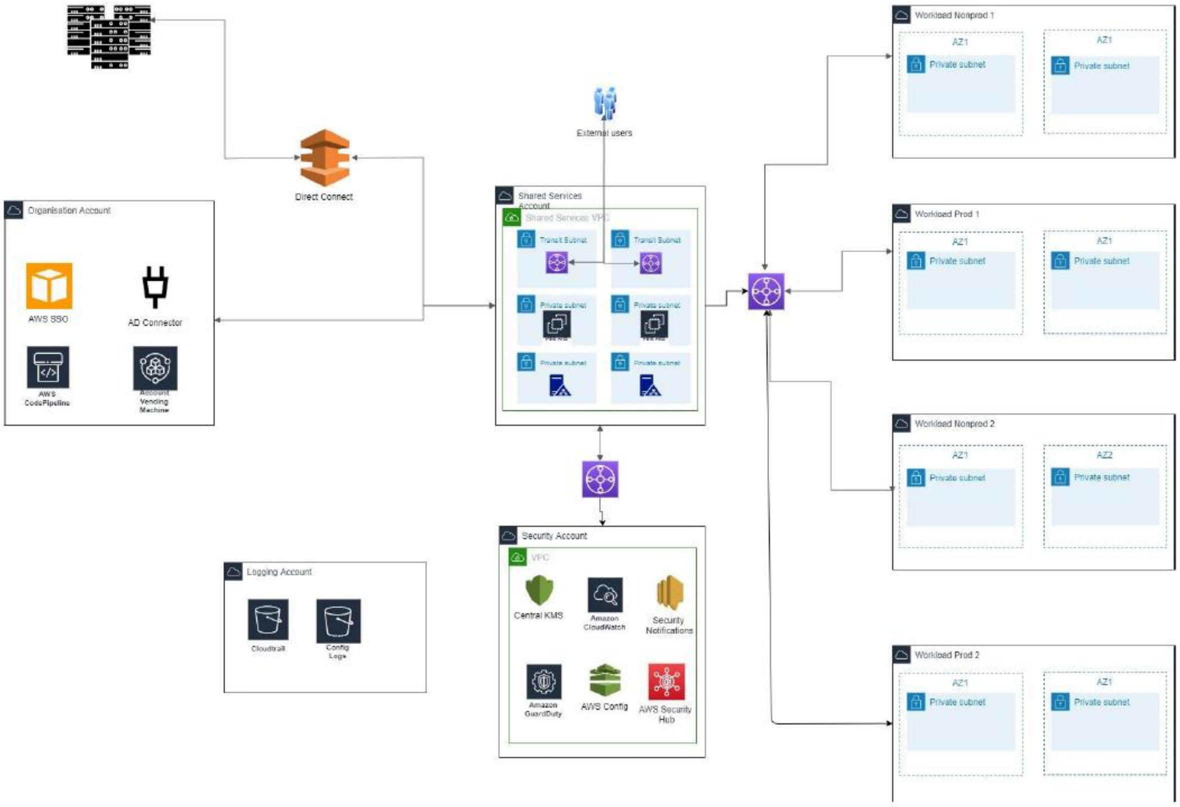
Intranet Transit AWS Account
This account connects to on-premise using Direct Connect. In order to filter incoming traffic from on-prem a NGFW will be used in HA. This account will direct traffic coming from on-premise users request to either Intranet Workload AWS Account or DMZ Workload AWS account.

Internet Transit AWS Account
The internet transit account is designed to host internet facing VPC with a set of security controls such as DDOS and NGFW to protect application hosted in the DMZ workload AWS account.

Intranet Workload AWS Account
The Intranet Workload AWS Account will host internal applications. A direct connect connection from Intranet Transit VPC Account will be established to this account to enable internal users to have access to intranet applications.

DMZ Workload AWS Account
All external facing applications interacting with the internet users are part of this account. This account will use transit routes. One connection to connect it from Intranet Transit AWS account to route intranet users to DMZ workload and other connection to connect internet users request coming from Internet Transit AWS account to backend servers. A Web Application Firewall will filter all incoming requests to backend servers to protect against web based attacks.

- Direct Connect – In order to connect on premise office to AWS resources securely to AWS direct connectivity will be established between corporate office and AWS account using direct connect.
- Intranet Transit VPC - This VPC will connect to on-premise network using direct connect. In order to filter incoming traffic from on-premise a NGFW will be used in HA in this VPC. This VPC will direct incoming on-premise users request to either Intranet Workload AWS Account or DMZ Workload AWS account.
- Internet Transit VPC- All the traffic coming from the internet will be filtered and analyzed in this VPC using network and application security controls before it is forwarded to the applications hosted in the DMZ Workload AWS Account.
- Transit gateway: For all VPC's to have a single zone internet or intranet traffic route, TGW would be used.



2.2.8. VPC Design

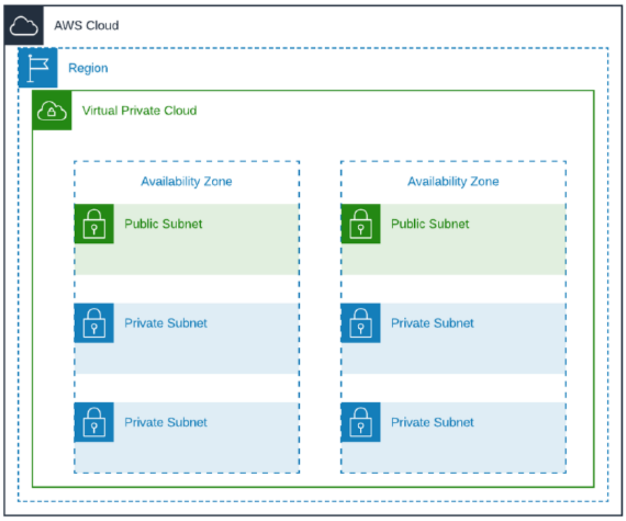
- Vendor shall create a virtual network infrastructure just like a traditional data center. The resources will be deployed within this virtual network infrastructure and be able to connect to the Internet.
- DirectX Connection /VPN: For integration with on premise resources VPN can be used to extend network of cloud to on premise.
- No bigger than /21: To avoid unused IP space and reaching some of the limits of the VPC service, every Virtual Network should not be bigger than /21 IP block size (a larger /20 can be considered depending on the demand).

- Multiple availability Zones: All virtual Networks should be spanned with multi availability zones, deploying the same subnet groups in each availability zone. Non-Prod should follow the same design to accommodate testing factors like Production environments.
- 3 Types of subnets per VPC
  - Public - Internet accessible resources, such as Bastion host, Nat, Load balancer.
  - Private - App layer, for hosting compute resources
  - Data - Database layer, such as RDS, DynamoDB, etc...

- VPC Design High Availability requirements: Every service that requires HA is mandatory to be deployed in a group of 2 or more resources per stack. These 2 resources should be allocated to different Availability Zones.

The VPC contains three tiers:

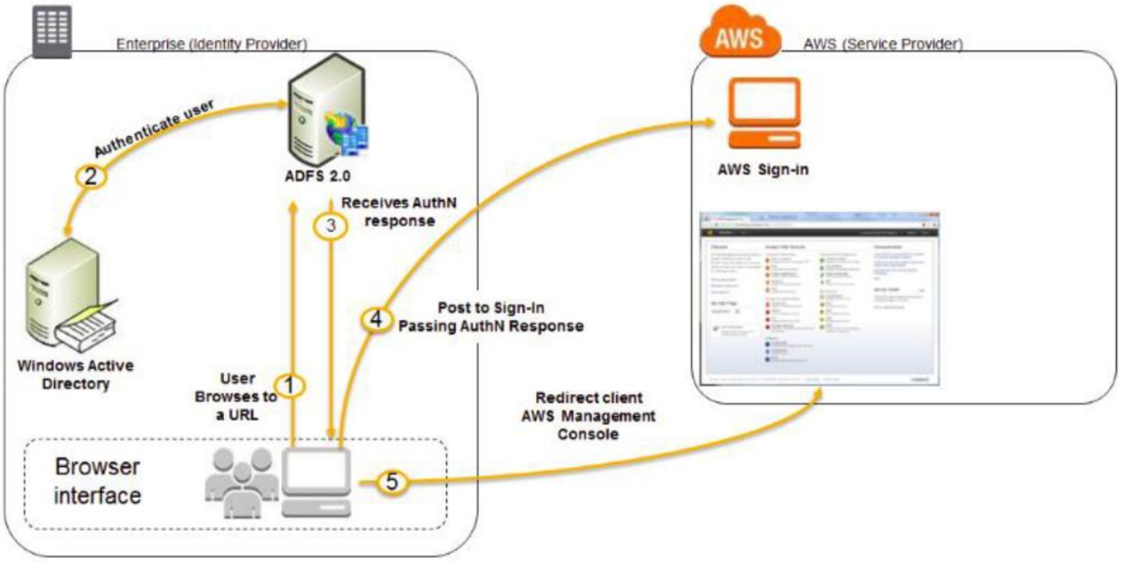
- The Public subnets, which exclusively host AWS load balancers (ELB/NLB/ALB)
- Private subnets which hosts all compute services such as middleware servers, app servers, AWS Lambdas, HPC servers and internally facing load balancers



- VPC Design Contains 3 layers spread across 2 separate AZs
- Public Subnets to be used exclusively for hosting external Load Balancers (ALB/ELB/NLB)
- Private Subnets that will host app servers, web servers, Lambdas, HPC servers and internal load balancers
- Private Data Subnets for hosting RDS, database servers, Elasticache

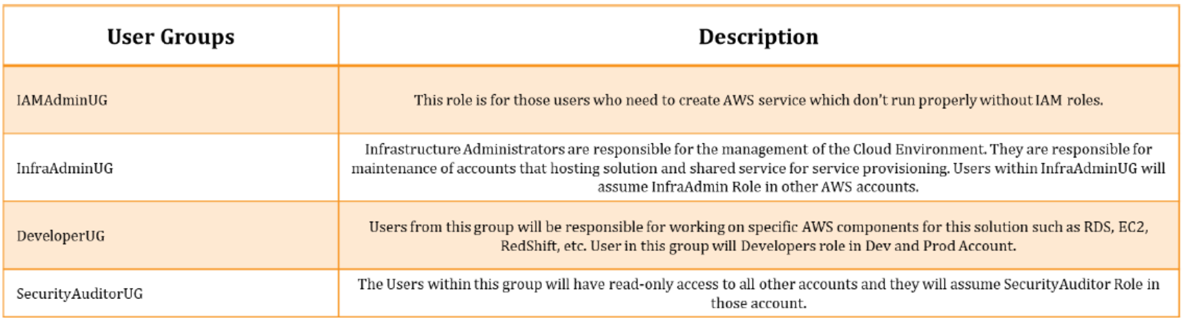
2.2.9. IAM Roles and Privileges

Vendor shall ensure User access management can be handled in AWS IAM and integrate IAM with the organization’s Active Directory. This will help the organization to centrally manage users’ authentication and authorizations. Alternatively, federation services such as ADFS can control user authentication from a centralized user management system. The decision on the option for centralizing user authentication needs to be discussed and finalized in the Design phase. The diagram below depicts the mechanism followed for user authentication via ADFS.

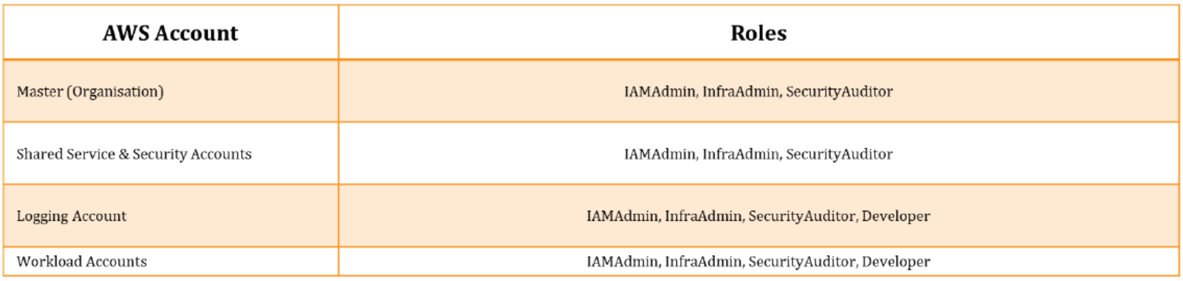


User Groups and Roles

The standard user roles and groups to be created are provided below. This may need addition of further roles and groups depending upon the country and number of roles to be created.



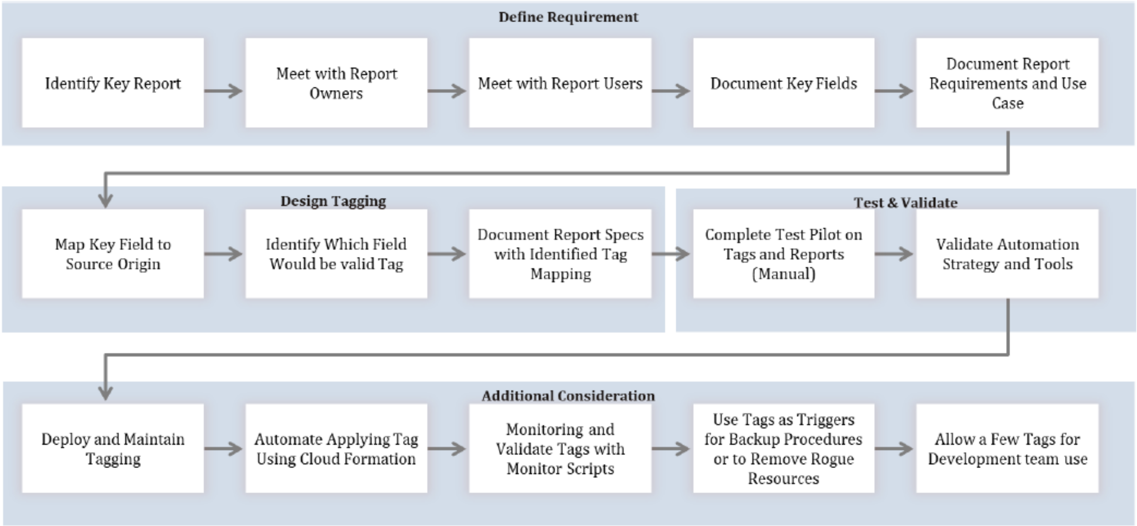
User Groups	Description
IAMAdminUG	This role is for those users who need to create AWS service which don't run properly without IAM roles.
InfraAdminUG	Infrastructure Administrators are responsible for the management of the Cloud Environment. They are responsible for maintenance of accounts that hosting solution and shared service for service provisioning. Users within InfraAdminUG will assume InfraAdmin Role in other AWS accounts.
DeveloperUG	Users from this group will be responsible for working on specific AWS components for this solution such as RDS, EC2, RedShift, etc. User in this group will Developers role in Dev and Prod Account.
SecurityAuditorUG	The Users within this group will have read-only access to all other accounts and they will assume SecurityAuditor Role in those account.



AWS Account	Roles
Master (Organisation)	IAMAdmin, InfraAdmin, SecurityAuditor
Shared Service & Security Accounts	IAMAdmin, InfraAdmin, SecurityAuditor
Logging Account	IAMAdmin, InfraAdmin, SecurityAuditor, Developer
Workload Accounts	IAMAdmin, InfraAdmin, SecurityAuditor, Developer

2.2.10. Tagging Strategy

A tag is a label that is assigned to an AWS resource. Each tag consists of a key and an optional value. Tags allow the categorization of AWS resources in different ways, such as, by purpose, owner, or environment. This is useful especially when there are multiple resources of the same type. Tags if assigned properly will help in quick identification of the resource. The strategy for tagging must be uniform across the organization. The following diagram depicts a standard tagging strategy.


Define Requirement
Identify Key Report
Meet with Report Owners
Meet with Report Users
Document Key Fields
Document Report Requirements and Use Case
Design Tagging
Map Key Field to Source Origin
Identify Which Field Would be valid Tag
Document Report Specs with Identified Tag Mapping
Test & Validate
Complete Test Pilot on Tags and Reports (Manual)
Validate Automation Strategy and Tools
Additional Consideration
Deploy and Maintain Tagging
Automate Applying Tag Using Cloud Formation
Monitoring and Validate Tags with Monitor Scripts
Use Tags as Triggers for Backup Procedures or to Remove Rogue Resources
Allow a Few Tags for Development team use

3. Solution Approach

Vendor shall take a 3 phased approach will be adopted for setting up an AWS Landing Zone. At a high level the phases will be as follows:

3.1. Assessment Phase

The assessment phase includes the understanding of the IT strategy and the application landscape of the organization. These details are used to define the following:

- Number of accounts for production and non-production workloads
- Security design
- Logging strategy
- Billing strategy
- Network design
- Generic services e.g. Patch management, end point security, jump server
- User authorization and administration
- Administrator login
- Define strategy of realigning the current account with new landing zone.
- Planning would be done in such a way there is minimum impact to the business
- Application understanding for future deployment in AWS cloud perspective
- Any third-party involvement understanding
- Surrounding system impacts understanding, if any

3.2. Design Phase

In the design phase, the requirements gathered in the assessment phase are utilized to design the following:

- AWS Account design
- Security
- Network
- Logging

- VPC
- Shared Services
- Prod and non-prod environment design
- AWS components design

3.3. Implementation Phase

The implementation phase includes the setting up of the different accounts and services as per the Landing Zone design. This will be an iterative phase where the changes to security and network design may have to be done based on multiple reviews. Every change will need a relook and modification of the design. In the implementation phase all the accounts including the VPCs are set-up.

4. AWS Landing Zone Setup - Scope of Work

Phases	Activities	Deliverables
Phase 1 – Project Set up	Project Kick off • Stakeholder Identification • Detailed planning of activities • Finalization of project deliverables	• Project deliverables sign off • Stakeholders List with roles • Project Plan
Phase 2 - Assessment	• Understand the security guidelines and • organization structure • Understand regulatory requirements • Understand cloud migration strategy • Understand current data governance policy • Gather information on IT strategy and • billing strategy • Define user access requirements via AD • federation or AD connector • Number of departments and the accounts • required	• Security and network requirements • Accounts and user authorization and authentication
Phase 3 - Design	• Design the different workload accounts and • shared accounts namely Security, Logging, • Shared Services • Network Design (including Transit • Gateway)	• Landing Zone design • User roles, policies and groups • 3rd party tools for security and logging • Tools and Services for security and logging

	• Select tools/services for firewall, WAF, • DDOS, end point security, log monitoring • VPC Design • VPC communication and flow design • User authentication via Active Directory • • Design Sign off from customer	
Phase 4 – Implement	• Implement all the required accounts • Create deployment pipeline for hardened • AMI baking • User authentication via ADFS Networking • AWS Gateway configurations from end-customer on-premises to AWS Cloud via • VPN (Provided Direct Connect lines are established between partner and end-customer) • Creation of VPCs ○ Primary VPC (Production) Subnets (DMZ, Private) ○ Standard VPC (Non-Production) Subnets (DMZ, Private) • VPC Peering Connection ○ Production VPCs ○ Regional Domain Services VPC (if exists in India region) • Implementation of the VPC design and configuration of the IP address blocks into the AWS Accounts that were setup • Provide internet gateway and public subnet (DMZ zone) • One-time Class-less Inter Domain Routing (CIDR) setup based on IP addresses allocated by customer	Custom Landing Zone ready for use • Pipeline for AMI creation • Centralized logging • Centralized identity Management

	Security Baseline • Implement best practices for Identity and Access Management including Two Factor Authentication (2FA) and password ageing • Use AWS best practices to design and implement coarse-grained control using Network Access Control Lists (NACLs) for the foundation layer. • Provide end-customer with NACL templates that can be used as additional applications are implemented on AWS • Understand end-customer's requirements for key management and create an initial key management design including decision points on: o Using Fully Managed or Centralized Key management o Rotation frequency (Monthly or Quarterly) Integration of encryption into applications using AWS provided SDKs • Configure CloudTrail to gain visibility into privileged user activity • Integrate on-premises Active Directory with authentication on AWS using Active Directory Federation Services. The role mapping between on-premises Active Directory and Roles on AWS will be completed by end-Customer • Create CloudWatch alarms to monitor and alert on account activity e.g. root login, changes in networking,	

	• CloudTrail configuration for logging all API logs Logging • Identify, architect and implement a log collection mechanism for infrastructure logs from CloudWatch, VPC Flow Logs, S3 Access Logs, and OS Syslog. Guide end-customer on how these logs can be sent from AWS to the customer instances • Configure AWS Simple Notification Services (SNS) for critical alerts for the foundation phase, excluding application alerts • Setup all logs into Logging Account CloudTrail logs will be switched ON for all accounts Operations & Management • Design and configuration of a Shared Services VPC • Implementation of a Bastion Host in this VPC • Implementation of a Remote Management hosts in this VPC Disaster Recovery and Functional Testing • Guiding end-customer to implement scalable and resilient applications using AWS services, e.g. Auto Scaling Groups and using AWS provided managed services, e.g. Amazon RDS • Guiding end-Customer through methods to test infrastructure component failover. This will focus on AWS component failure, e.g. EC2 shutdown	

	Billing & Tagging • AWS resource and cost tracking using tags for custom AWS billing strategies • Tagging all resources as per Singtel Naming convention Setup Identity and Access Management • Setup and define access control for users • Define roles and policies for the Users	
Phase 4 – Governance Model	Understand the infrastructure provisioning and user creation and approval processes • Security audit requirement analysis and set up automated audit possibility • Create target operating model along with roles and responsibilities on AWS • Regular audits against compliance guidelines (eg. PCI DSS, ISO 27001, CIS etc.)	Infrastructure provisioning guide • Centralized identity Management • Back-up and Restore guide • Security Audit Template
Phase 5 – Sign off and Transition/handover to customer	Handover Landing Zone to customer • Provide training and supporting documentation to customer team • Project Sign Off	Handover to customer team • Sign Off

5. Out of Scope

a) Application Deployment and migration will be customer’s responsibility and will be out of scope for the Vendor
b) Implementation and configuration of any third-party firewalls and network devices
c) Setup of Antivirus will be out of scope for this engagement
d) VAPT scans will be out of scope for this engagement
e) Any data migration to AWS
f) Any changes required for the on-premise components will not be performed
g) Data Loss prevention (DLP) is out of scope
h) Any activity on application will be out of scope
i) Creation of Operational guidelines for infrastructure management
j) Integration of any third-party tools will be out of scope
k) Operating System hardening

l) Setting up of Direct Connect between AWS and on-premise
m) Any Set-up of a separate Active Directory on AWS
n) Managed services support for the newly hosted AWS environment
o) Implementation of DevOps pipelines for deployment
p) Project management will be out of scope

6. Project Timeline

The vendor shall outline the Project Timeline to complete the scope in this Appendix.

7. Pricing

The vendor shall provide the pricing for this SOW (Landing Zone Design – AWS) in Appendix O.

Appendix B - Landing Zone Design - Azure

1. Overview

The Landing Zone Design – Azure should meet the following requirements:

- Security and compliance - Meet the organization's security and auditing requirements
- Scalability and resilience - Ready to support highly available and scalable workloads
- Adaptability and flexibility - Configurable to support evolving business requirements

The Vendor is to propose an Azure Cloud Landing Zone solution to smoothen the workloads onboarding on Azure cloud, with following key attributes:

- Azure Account Structure
  - Management Groups
  - Subscriptions

- Network Architecture
  - Site to Cloud Connectivity

- Security Risk and Governance
  - Identity and Access management
  - Logging and Monitoring
  - Security

- Cost & Billing Management
  - Cost Analysis
  - Budgets
  - Naming & Tagging
  - Azure Enterprise Reports

2. Scope of Work

The Vendor is to perform the following phased approach for setting up of a Landing Zone on Azure Cloud :

Phases	Activities	Deliverables / Outcomes
Project Set up	• Kick-off with stakeholders • Stakeholder identification • Detailed planning of activities • Finalization of project deliverables	• Stakeholder List with roles
Assessment and Requirement Gathering	• Understand the security guidelines and organization structure. • Understand account structure requirement • Understand regulatory requirements.	• Overall understanding of the landing zone requirement

	• Understand target state strategy for cloud adoption • Gather information on IT strategy and billing strategy. • Define user access requirements via AD federation or AD connector. • Number of business units and the accounts required. • Decision on Terraform scripts for implementation	
Design	• Design the different workload accounts, Identity subscription account, Connectivity subscription account, Management subscription account and Sandbox subscription account. • Network Architecture Design • Security design • Design Identity & Directory Architecture • Design DNS Architecture • Define Logging and monitoring policy • Define Cost & Billing Management • Design Sign off from customer • Design Terraform script for automating resource provisioning	• Custom Landing Zone design • User roles, policies and groups
Implementation	• Implement all the required accounts. • Implement Network components as per agreed design. • Setup security resources and guidelines as per customer requirements • Setup identity and directory architecture • Implement DNS as per agreed design • Setup logging and monitoring policy as per organization standard • Setup cost & billing management for defined accounts	• Custom Landing Zone ready for use • Centralized logging • Centralized identity management
Transition/Handover	• Handover Azure Landing Zone to customer for resource deployment • Provide training and supporting documentation to customer team • Project Sign Off	• Landing Zone Design document • Landing Zone architecture • Sign off report

2.1 Out of Scope

- Network connectivity setup from on-premises to Azure cloud using Azure Express Route.
- Any Integration of Singtel on-premises services & tools, not limited to below on-premises tools only.
  - PCloud
  - HPSA
  - Infoblox DNS

    - TrendMicro
    - Monitoring tools

- Any workload implementation & configuration for Singtel on-premises is out of scope.
- Vendor & contract management for Singtel on-premises workloads is out of scope.
- New Active Directory Forest and ADFS setup and configuration for on-premise is out of scope.
- Any on-premise migration of application and data to Azure cloud
- Setup of Antivirus will be out of scope for this engagement
- VAPT scans will be out of scope for this engagement
- Integration of existing accounts to the new Landing Zone if any
- Creation of Operational guidelines for infrastructure management
- Operating System hardening

3. Solution Approach

The Vendor shall provide a High level overview of the Design Architecture. The final verified high-level design will be made available after the end-customer workshop for requirement gathering and assessment is carried out.

3.1. AZURE Cloud Discovery & Assessment

The Vendor team shall organise workshops with Singtel and the end-Customer team as well as any relevant parties in the Cloud Azure Landing Zone Scope program to understand and freeze on the requirements.

Workshop for Azure Landing Zone

The Vendor in collaboration with Singtel and the end-customer will organise a set of workshops in order to review and finalize the Singtel current point in time status of the Azure cloud roadmap.

- Stakeholder identification from Singtel Cloud Team, Blazeclan and relevant third-party vendors
- Review and assess the Azure Account structure requirement
- Review and assess the Azure Network Architecture requirement
- Review and assess the Azure Security Architecture requirement
- Review and assess the Azure Identity & Directory Architecture requirement
- Review and assess the Azure DNS Architecture requirement
- Review and assess the Azure Logging & Monitoring Architecture requirement
- Review and assess the Azure Cost & Billing management requirement

Finalize Solution Design for Azure Landing Zone

The outcomes from the workshop is an Azure cloud design that will scope a number of design areas and the outcome is a high-level design as well as a detailed design document.

High level design document will be shared with Singtel and the end-customer, post completion of Design phase.

3.2. AZURE ACCOUNT STRUCTURE DESIGN

The Vendor shall ensure the Azure Account structure will be based on Department, Azure Account, management groups and subscriptions.

The Azure Portal will be used to manage the Azure subscription and Azure resources. The following functions can be performed:

- Define roles for subscription Owner, Contributor etc.
- Manage Azure RBAC, resources & services
- Tasks:
    - Manage RBAC using Azure & Azure AD Roles
    - Manage Resources

3.3. PROPOSED AZURE LANDING ZONE ARCHITECTURE DESIGN

Azure landing zones are the output of a multi subscription Azure environment that accounts for scale, security, governance, networking, and identity. The vendor's design of Azure landing zone is to consider all platform resources that are required to support Singtel's end-customer's application portfolio and doesn't differentiate between infrastructure as a service or platform as a service.

This enterprise-scale landing zone architecture is defined by a set of design considerations and recommendations across multiple critical design areas

Critical Design Areas

- Enterprise Agreement (EA) enrolment (if applicable) and Azure Active Directory tenants **:** An EA enrolment represents the commercial relationship between Microsoft and how Singtel uses Azure as well as Singtel's organization hierarchy. An Azure AD tenant provides identity and access management, which is an important part of security posture. An Azure AD tenant ensures that authenticated and authorized users have access to only the resources for which they have access permissions. Azure AD provides these services to applications and services deployed in Azure and to services and applications deployed outside of Azure (such as on-premises or third-party cloud providers).
- **Identity and access management** Identity provides the basis of a large percentage of security assurance. It enables access based on identity authentication and authorization controls in cloud services to protect data and resources and to decide which requests should be permitted. Enterprise organizations typically follow a least-privileged approach to operational access. This model should be expanded to consider Azure through Azure Active Directory (Azure AD), Azure role-based access control (Azure RBAC), and custom role definitions. Configure DNS and name resolution for on-premises and Azure resources.

- **Management group and subscription organization:** Management group structures within an Azure Active Directory (Azure AD) tenant support organizational mapping. Subscriptions are a unit of management, billing, and scale within Azure.
- Network topology and connectivity
    - Plan for IP addressing
    - Define an Azure network topology
    - Connectivity to Azure
    - Plan for landing zone network segmentation
    - Define network encryption requirements
    - Plan for traffic inspection
- **Management and monitoring**: Plan platform management and monitoring. Operationally maintain an Azure enterprise estate with centralized management and monitoring at a platform level.
    - Use an Azure Monitor Log Analytics workspace as an administrative boundary
    - Application-centric platform monitoring, encompassing both hot and cold telemetry paths for metrics and logs(Optional, to be discussed in detail, if required, efforts are not captured for this configuration)
    - Security audit logging and achieving a horizontal security lens across your organization's entire Azure estate
    - Azure data retention thresholds and archiving requirements

Plan for application management and monitoring (Optional). Ensure that application teams can operationally maintain workloads.

- Application monitoring can use dedicated Log Analytics workspaces.
- For applications that are deployed to virtual machines, logs should be stored centrally to the dedicated Log Analytics workspace from a platform perspective. Application teams can access the logs subject to the Azure RBAC they have on their applications or virtual machines.
- Application performance and health monitoring for both infrastructure as a service (IaaS) and platform as a service (PaaS) resources.
- Data aggregation across all application components.
- Health modelling and operationalization

- **Enterprise-scale business continuity and disaster recovery**: Design suitable, platform-level capabilities that application workloads can consume to meet their specific requirements. Specifically, these application workloads have requirements pertaining to recover time objective (RTO) and recovery point objective (RPO). Capture disaster recovery (DR) requirements in order to design capabilities appropriately for these workloads.

- **Enterprise-scale security, governance and compliance** : Define encryption and key management, plan for governance, define security monitoring and an audit policy, and plan for platform security.

3.4. PROPOSED AZURE NETWORK ARCHITECTURE

Singtel end-customer’s Network Requirement

- Singtel’s end customer needs private connectivity to Azure and an IPSec VPN encryption over Azure ExpressRoute.
- MTU Size of 1500+
- Dedicated private connectivity from Singtel on-premises to Azure Prod and Non-Prod Singtel workloads.
- Singtel don’t expose on-premises internal networks on Singtel Transport Cloud routers.
- IPSec VPN encryption should be establish between Singtel Palo Alto Firewall (P1, P2, P3) to Azure ExpressRoute gateway.
- Solution should support sustainability of multiple components failure scenarios.
- Solution should have dedicated tunnels for each environment (Ex: IPSec1 dedicated for Prod, IPSec2 dedicated for UAT).
- Solution should avoid asymmetric routing scenarios.
- Singtel network will only be advertised on IPSec layer VPN tunnels.
- Singtel networks will not advertise on underlay transport network routers.
- Singtel Palo Alto firewall initiating IPSec VPN tunnels from Singtel will only have private IP address.

Proposed network architecture components :

- Azure Express Route + Azure Virtual WAN + ExpressRoute Gateway + Cisco CSR NVA
- Azure Express Route provides dedicated private connectivity from on-premise DC to Azure Cloud
- Azure Express Route Private connectivity with 300 Mbps bandwidth
- Cisco CSR NVA to be hosted in Azure Virtual WAN Hub to provide encrypted IPSEC VPN connectivity and support higher jumbo rates
- Cisco CSR NVA has in-built support for Azure Virtual WAN HUB
- Azure Virtual WAN HUB to provide VNET Peering attachment to Prod & Non-Prod platform, LOB & Sandbox subscription

3.5. PROPOSED AZURE IDENTITY AND DIRECTORY SERVICES SOLUTION

Singtel's Requirement

- User Access & Server/Workload Access standards are clearly defined—user Access governed as per MAS 655 guidelines to secure access to Azure Console with 2FA.
- Server/Workload Access standards are clearly defined to authentication/authorization of workloads hosted on Azure & On- Premise secure and seamless.

Proposed Identity and Directory Services Solution

Singtel security allows on-premises root domain to be exposed in the cloud.

- A new single resource forest, single domain to be created for Azure workloads resources to authenticate.
- On-premise new resource forest and domain to be extended to Azure cloud under identity subscription.
- Two separate forests proposed, one for Production and the other for the SIT environment.
- One-way forest trust to be established between on-premises Singtel forest and newly created cloud resource forest

Azure Identity Governance

Azure Active Directory (Azure AD) Identity Governance allows Singtel to balance the need for security and employee productivity with the right processes and visibility. It provides the capabilities to ensure that the right people have the right access to the right resources.
Identity Governance gives the ability to do the following tasks across employees, business partners and vendors, and across services and applications both on-premises and in clouds:

- Govern the identity lifecycle
- Govern access lifecycle
- Secure privileged access for administration

Identity Lifecycle

Identity Governance helps organizations achieve a balance between productivity and security. Identity lifecycle management is the foundation for Identity Governance, and effective governance at scale requires modernizing the identity lifecycle management infrastructure for applications

The following tools are used to help manage identify lifecycle:

- Azure AD Entitlement Management
- Microsoft Identity Manager
- Azure AD reports

Access Lifecycle
Singtel needs a process to manage access beyond what was initially provisioned for a user when that user's identity was created. Furthermore, Singtel needs to be able to scale efficiently to be able to develop and enforce access policy and controls on an ongoing basis.

The following tools are used to help manage access lifecycle:

- Azure AD Entitlement Management
- Azure AD Access Reviews
- Conditional Access
-

Privileged Access Lifecycle

- Governing privileged access is a key part of Identity Governance given the potential for misuse associated with those administrator rights can cause. The employees, vendors, and contractors that take on administrative rights need to be governed.

The following tools are used to help manage access lifecycle:

- Azure AD Privileged Identity Management (PIM)
- PIM Alerts

Azure AD Privileged Identity Management (PIM) provides additional controls tailored to securing access rights for resources, across Azure AD, Azure, and other Microsoft Online Services. The just-in-time access, and role change alerting capabilities provided by Azure AD PIM, in addition to multi-factor authentication and Conditional Access, provide a comprehensive set of governance controls to help secure Singtel's resources. Singtel can use access reviews to configure recurring access recertification for all users in administrator roles.

Azure Identity Compliance
Identity compliance can be achieved using the following:

Azure Policy
Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per -resource, per-policy granularity. It also helps to bring resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.
It evaluates resources in Azure by comparing the properties of those resources to business rules. These business rules, described in JSON format, are known as policy definitions. To simplify management, several business rules can be grouped together to form a policy initiative (sometimes called a policySet). Once business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources. The assignment applies to all resources within the Resource Manager scope of that assignment.
The journey of creating and implementing a policy in Azure Policy begins with creating a policy definition. A collection of policy definitions that are tailored towards achieving a singular

overarching goal is called initiative definition. Initiative definitions simplify managing and assigning policy definitions. They simplify by grouping a set of policies as one single item.
An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource.

Azure RBAC
Azure role-based access control (Azure RBAC) helps to manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. Designating groups or individual roles responsible for specific functions in Azure helps avoid confusion that can lead to human and automation errors that create security risks. Restricting access based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access.RBAC would include Security principal, role definition, role assignment and scope.

3.6. PROPOSED AZURE DNS ARCHITECTURE

Singtel Azure Landing Zone needs to have a DNS solution to provide the name resolution for cloud-based workloads.

Proposed Azure DNS Solution

- Virtual network connected to on-premises via ExpressRoute private connectivity
- Peered virtual network to other Azure subscriptions virtual network
- DNS forwarder deployed in Azure identity subscription which forward DNS queries to Azure and on-premise DNS zone
- Private DNS zones which contains type A record will be hosted in Azure cloud
- Private endpoint information (FQDN record name and private IP address)

3.7. AZURE LOGGING AND MONITORING ARCHITECTURE

The Vendor shall propose a centralized logging and monitoring solution for its on-premises and multi cloud workloads.

Proposed Logging and Monitoring Solution

Logging and Monitoring requirements will be achieved using the following:

- Azure Monitor
- Azure Log Analytics Workspace
- Platform Logs
- Resource Logs
- Activity Logs
- Azure AD Logs

- Azure logging and monitoring solution can be extended to public cloud as well as on-premises workloads.

3.8 PROPOSED AZURE SECURITY ARCHITECTURE SOLUTION

Security & Audit Surface	Platform	Solution
Antivirus Solution	On-Premises TrendMicro Solution to be extended to Azure	TrendMicro Satellite Servers to be hosted on Azure VM's
Patching Solution	On-Premises HPSA Solution to be extended to Azure	HPSA Satellite Servers to be hosted on Azure VM's
Directory Service	A separate resource forest to be hosted in On-premise Singtel DC's and extended to Azure Cloud	Read / Write DC of resource forest domain to be hosted in Azure Cloud Identity subscription
Identity Service	Leaked Cred protection Behaviour Analytics	Azure AD Identity Protection
Access Management	On-Premises Active Directory, ADFS and Azure IAM	Active directory federation service to federate access management.
DLP	On-Premises DLP Solution or Azure Information Protection	Azure Information Protection (AIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content. AIP can be extended to on-premise or customer in-house DLP will be used for on-premise and all cloud workloads.
Threat Protection	Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.	Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP)
Audit & Compliance	Azure cloud-native audit system and policy definition & assignment	Azure Monitor & Azure Policy
Network	Network security group (NSG) flow logs and allow or block network traffic	Azure Network Watcher (Traffic Analytics), Azure Firewall and Application & network security groups
Security Dashboard	Azure cloud-native dashboard	Azure Security Centre
Logging and Monitoring	On-Premises Logging solution or Azure Hybrid logging & monitoring	Azure Monitor & Azure Log Analytics
Monitoring	On-Premises or Azure Monitor	Azure Monitor can monitor cloud native + On-premise workloads
SIEM	On-premise or Azure Sentinel	
Encryption	Disk & Storage encryption	Azure Key Vault
Computing	Protect data while processing	Azure Confidential Computing

3.9. PROPOSED AZURE COST AND BILLING ARCHITECTURE

The Vendor needs to propose a centralized billing and cost management on Azure Cloud.

The Vendor shall propose the use of the following for cost and billing management:

- Azure Cost management + Billing
- Cost Analysis
- Budgets
- Enterprise Agreement Bill
- Review Invoice Charges
- Review Service Overage Charges
- Review Marketplace invoice
- Azure Enterprise Report
- Usage summary and graphs
- Service usage report
- Balance and charge report
- Usage detail report
- Azure Marketplace charges report
- Price sheet
- Advanced report download
- CSV report formatting
- Power BI Reporting
- Naming & Tagging
- Define naming strategy
- Define tagging strategy

3.10. AZURE LANDING ZONE AUTOMATION

The Vendor is to propose to automate the Azure Landing Zone setup and configuration using Terraform wherever possible.

Cloud Adoption Framework foundations landing zone for Terraform provides features to enforce logging, accounting, and security. This landing zone uses standard components known as Terraform modules to enforce consistency across resources deployed in the environment. CAF Terraform modules will be leveraged and customized to automate Azure LZ components.

3.11. AZURE LZ DOCUMENT DELIVERABLES

The Vendor shall hand over all the documents of the deployment to Singtel with information like Azure landing zone setup, security and account strategy which will be part of the Document Deliverables.

- Azure Landing Zone High Level Design
- Azure Landing Zone Low Level Design
- Azure Landing Zone Terraform scripts

4. Proposed Project timelines

The vendor is to propose the Project timelines for this SOW.

5. Pricing

The Vendor is to propose the Pricing for this SOW in Appendix O.

Appendix C – Landing Zone Design - GCP

1. Overview

Singtel's end-customers are looking for migrating their infrastructure to GCP cloud. The Vendor shall be able to perform the following activities listed in this appendix. The Vendor is to propose an GCP Cloud Landing Zone solution to smoothen the workloads onboarding on GCP cloud, with following key attributes:

- GCP Account Structure
  - Management Groups
  - Subscriptions

- Network Architecture
  - Site to Cloud Connectivity

- Security Risk and Governance
  - Identity and Access management
  - Logging and Monitoring
  - Security

- Cost & Billing Management
  - Cost Analysis
  - Budgets
  - Naming & Tagging
  - Azure Enterprise Reports

2. Scope of Work

Vendor will help Singtel identify workloads prioritized by risk and migrate the related operating environments to GCP. Faster migration will lead to faster innovation will lower the cost of later transformation, and once workloads are running on GCP, Singtel's end customer will have the ability to optimize application and service usage.

The key scope objectives are:

- To identify workloads using an accurate, tool-assisted inventory of the server landscape (physical and/or virtualized), including applications running on each server and an assessment to assist with migration planning and risk mitigation
- To build a lightweight foundational GCP landing zone that will provide the core basis for this migration
- To build Migrate for Compute Engine runbook(s) that will serve as a self-documenting, auditable migration plan by describing source application components, dependencies, run order, and desired end state in GCP
- To migrate candidate VMs from on-premises (VMWare/Physical), AWS, or Azure to Compute Engine on GCP
- To provide an end-of-program review that documents successes and improvements for future migration efforts

- When the engagement concludes, all workloads will be migrated and running in GCP.

The Vendor is to perform the following phased approach for setting up of a Landing Zone on GCP Cloud :

Phases	Activities	Deliverables / Outcomes
Project Set up	• Kick-off with stakeholders • Stakeholder identification • Detailed planning of activities • Finalization of project deliverables	• Stakeholder List with roles
Assessment and Requirement Gathering	• Understand the security guidelines and organization structure. • Understand account structure requirement • Understand regulatory requirements. • Understand target state strategy for cloud adoption • Gather information on IT strategy and billing strategy. • Define user access requirements via AD federation or AD connector. • Number of business units and the accounts required. • Decision on Terraform scripts for implementation	• Overall understanding of the landing zone requirement
Design	• Design the different workload accounts, Identity subscription account, Connectivity subscription account, Management subscription account and Sandbox subscription account. • Network Architecture Design • Security design • Design Identity & Directory Architecture • Design DNS Architecture • Define Logging and monitoring policy • Define Cost & Billing Management • Design Sign off from customer • Design Terraform script for automating resource provisioning	• Custom Landing Zone design • User roles, policies and groups
Implementation	• Implement all the required accounts. • Implement Network components as per agreed design. • Setup security resources and guidelines as per customer requirements • Setup identity and directory architecture • Implement DNS as per agreed design • Setup logging and monitoring policy as per organization standard • Setup cost & billing management for defined accounts	• Custom Landing Zone ready for use • Centralized logging • Centralized identity management

Transition/Handover	- Handover GCP Landing Zone to customer for resource deployment - Provide training and supporting documentation to customer team - Project Sign Off	- Landing Zone Design document - Landing Zone architecture - Sign off report

3. Solution Approach

I. Kick-off planning and preparation

Professional Services supports Singtel in preparing for the project kick-off by providing reference templates for a successful Landing Zone kick-off.

II. Architecture review

Professional Services reviews architectures for foundational Landing Zone designs and discusses the right approach for the given customer. Professional Services will also review design decisions around networking, IAM, resource management, and security for best practices and to identify common pitfalls.

III. Advisory consultation and regular office hours

Throughout the engagement, Professional Services and the vendor agree on regular office hours and advisory consultation sessions or meetings to help answer questions, review designs, and provide insights into Singtel's best practices. Professional Services will provide technical expertise on foundational topics and include appropriate subject matter experts.

IV. Automation

Vendor to provides reference templates for automating Terraform or Deployment Manager through the Cloud Foundation Toolkit.

V. Final review

At the end of the engagement, vendor reviews the overall findings of, and recommendations for, the project and provides inputs on the final deliverable to Singtel's end-customer.

4. Proposed Project timelines

The vendor is to propose the Project timelines for this SOW.

5. Pricing

The Vendor is to propose the Pricing for this SOW in Appendix O.

Appendix D - Migrations (AWS)

1. Overview

Singtel's end-customers are looking for migrating their infrastructure to AWS cloud. The Vendor shall leverage the scalability, elasticity and robustness of AWS to setup and migrate Singtel's end-customer infrastructure to the AWS Cloud. Cloud native network and security configurations may be implemented to make the setup secure and robust.

Migration to AWS cloud will involve following phases:

- Assessment phase
- AWS account Setup Phase
- Migration Phase
- Transition Phase

2. Scope of Work

Phases	Activities	Deliverables
Phase 1 - Planning and Assessment Phase	Detailed requirement gathering • Project Scope & Definition • Stakeholder Identification • Share Current Server Sizing Details Analyze the AS-IS state • Existing Infrastructure assessment and analysis • Due diligence of current application and database infrastructure • Determine current application and database workload based on CPU/memory utilization, I/O operations • Assess existing security and compliance requirements • Mapping of current state workloads to AWS Cloud. Create target architecture diagram	• Assessment Report • Final architecture diagram • Project timeline and schedule

	Approve target architecture diagram	
Phase 2 – AWS Account Setup	Creating Production environment to provision below components as depicted in AWS Architecture • EC2 instance • EBS storage Setup Cloud Native Network and Security Configuration • Virtual Private Cloud (VPC) • Configuring Public and Private Subnets • Network Security Group (NSG) Setup AWS Site-to-Site VPN between on premise DC and AWS Cloud Setup Logging and Monitoring • AWS CloudWatch – To monitor health of instances • AWS CloudTrail – To log, monitor and retain events on AWS infrastructure Configure Access control using IAM • Setup user access and configure separate account for users • Protect access for IAM users • Configure permissions for IAM groups	• AWS Infrastructure
Phase 3 - Migration	Vendor will employ a lift & shift strategy to move the applications to AWS	• Workloads on AWS • Sign-off

	Start migration using CloudEndure which helps in following ways • AWS readiness • AWS sizing • Dependency visualization Migrate Prod environment Fix issues on infrastructure and help in fixing issues on applications Cutover to AWS production environments	
Phase 4 – Transition to Managed Services	Provide Aftercare for 1-week post sign-off Handover to managed service team for on-going operation support Provide training and supporting documentation to customer team	• After Care support and sign off from transition team

3. The Vendor is to propose a high-level overview of networking, compute & storage units that will be utilized to host the workloads

4. The Vendor is to also provide the project timelines to execute this SOW, along with the Project RACI

5. The Vendor is to propose pricing for this SOW in Appendix O

Appendix E – Migrations (Azure)

1. Overview

Singtel's End-Customer is looking for migrating their infrastructure to Azure cloud. Vendor is to leverage the scalability, elasticity and robustness of Microsoft Azure to setup and migrate Singtel's end-customer infrastructure. Cloud native network and security configurations shall be implemented to make the setup secure and robust. Vendor will make use of services such as Azure VM, Azure Storage, Azure AD, VNET, etc. to provide a comprehensive solution. Moving to Azure cloud will involve following phases:

- Assessment phase
- Azure account Setup Phase
- Azure Migrate Applicate Setup
- Migration Phase
- Transition Phase

2. Scope of Work

Phase	Activities	Deliverables
Phase 1 - Planning and Assessment Phase	Detailed requirement gathering • Project Scope & Definition • Stakeholder Identification • Share Current Server Sizing Details Analyze the AS-IS state • Existing Infrastructure assessment and analysis • Due diligence of current application and database infrastructure • Determine current application and database workload based on customer inputs • Assess existing security and compliance requirements • Mapping of current state workloads to Azure Cloud. Create target architecture diagram Approve target architecture diagram	Assessment Report Final architecture diagram Project timeline and schedule
Phase 2 – Azure Account Setup	Creating Azure account to provision below components as depicted in Azure Architecture • Virtual Machine • Azure Managed Disk • Azure Storage Account	Azure Infrastructure

	• Azure Recovery Vault Setup Cloud Native Network and Security Configuration • Virtual Private Network (VNET) • Network Security Group (NSG) Setup Azure VPN between on premise DC and Azure cloud VNET Setup Logging and Monitoring • Azure Monitor – To monitor health of instances • Setup Azure Log Analytics for Alert Management • Azure Security Center – To log, monitor and retain events on Azure infrastructure Configure Access Control • Setup user access and configure separate account for users • Configure permissions for IAM groups	
Phase 3 – Setup Azure Migrate Appliance	Azure Migrate Appliance • Setup Azure Migrate project in Client Subscription • Deploy Azure Migrate Appliance on VMware/Hyper-V Vendor will employ a rehost strategy to move the Virtual Machines to Azure using Azure Migrate service • Discovering the VMs for Migration through Azure Migrate • Creation of Assessment and migration groups • Selecting the VMs for Migration • Replicating the selected VMs	Azure Migrate Appliance Server wise Migration Schedule and approach
Phase 4 - Migration	• Running a test migration to check the migration is working as expected • Running a full VM migration after test successful • Migrate the workloads • Fix issues on infrastructure and help in fixing issues on applications • Cutover to Azure production environments •	Workloads on Azure Sign-off
Phase 5 – Transition to Managed Services	• Provide Aftercare for 1-week post sign-off • Handover to managed service team for on-going operation support	After Care support and sign off from transition team

	• Provide training and supporting documentation to customer team	

3. The Vendor is to propose a high-level overview of networking, compute & storage units that will be utilized to host the workloads

4. The Vendor is to also provide the project timelines to execute this SOW, along with the Project RACI

5. The Vendor is to provide pricing for this SOW in Appendix O.

Appendix F – Migrations (GCP)

1. Overview

Singtel's end customer current infrastructure and operating environments are hosted under their or a vendor's management. They would like to migrate these applications to the cloud. Vendor will lead a migration engagement to migrate the infrastructure into Google Cloud Platform (GCP).

The source environments to be migrated consist of over VMs in VMWare, physical machines, and/or AWS/Azure VMs across data center environments.

Migration Objectives

Vendor will help identify workloads prioritized by risk and migrate the related operating environments to GCP. Faster migration will lead to faster innovation will lower the cost of later transformation, and once workloads are running on GCP the customer will have the ability to optimize application and service usage.

I. To identify workloads using an accurate, tool-assisted inventory of the server landscape (physical and/or virtualized), including applications running on each server and an assessment to assist with migration planning and risk mitigation

II. To build a lightweight foundational GCP landing zone that will provide the core basis for this migration

III. To build Migrate for Compute Engine runbook(s) that will serve as a self-documenting, auditable migration plan by describing source application components, dependencies, run order, and desired end state in GCP

IV. To migrate candidate VMs from on-premises (VMWare/Physical), AWS, or Azure to Compute Engine on GCP

2. Scope of Work

Vendor will provide high-level migration plans for each targeted application stack, identifying key decisions, and highlighting trade-offs. These plans will include the foundational technical configuration of a Singtel's end-customer's GCP estate, with dependencies such as identity and access management, networking, programmable infrastructure, and cost control, identified. Vendor then assists the customer with the installation of tooling, preparation, migration, and post-migration verification of the workload.

Stage and Activities

Migration engagement is delivered in a series of phases that vary based on the size and length of the agreement. Vendor will coordinate the schedule with Singtel aligned with the following delivery model;

I. Stage Zero: Pre-kickoff activities

a. Customer Readiness Checklist

Professional Services provides detailed lists of resources, staff, software, and security requirements needed to support the migration.

b. Pre-kickoff update / check-in meetings

Before scheduling the kickoff, Professional Services works with customer representatives to ensure that all checklist items are addressed, so that the effort is efficient and focused, helping to minimize delays.

II. Stage One: Assessment / Discovery activities

a. Kickoff workshop: project stakeholders

Vendor facilitates a workshop to present key decision points on the setup of the foundational technical configuration and operating model to best support all solutions across the development and production environments.

b. Discovery tooling deployment

Vendor advises on how to install and run discovery automation tools in data center to collect inventory data and server dependencies.

c. Discovery application documentation creation

Vendor defines and provides the application stack documentation template that forms the landing zone for information gathered during the course of the project.

d. Discovery questionnaire deployment

Vendor to gather information in a structured and repeatable fashion and circulates a form among applicable application stack owners. The information gathered as a result of this exercise then forms the basis of the discovery documentation and further workshop discussions.

e. Application assessment workshops

Vendor schedules a workshop with the application stack stakeholders to discuss the findings and confirm the migration approach.

I. Surveys and interviews application teams and stakeholders to collect more detailed information regarding up to complex applications in Singtel's end-customer landscape

II. Assesses the appropriate migration strategy for up to applications and VMs, taking into consideration technical and business requirements

III. Assesses the complexity associated with the migration of those applications at a high-level

IV. Develops migration wave plans (groupings) for the different applications, taking into consideration the various dependencies

V. Recommends the first application migration

VI. Models and plots the application journey (pre-migration, migration, post migration testing / validation procedures)

VII. Describes in detail the application validation testing and the roles that will be required:
   - Boot verification
   - Performance testing
   - Connectivity
   - Application functionality

f. Migration Foundation Workshop

Vendor facilitates a Migration Workshop to:

I. Review and validate GCP cloud foundations and migration readiness, including design recommendations for network, security, IAM, monitoring, and billing

II. Engage key stakeholders in defining project framework, time frames, overall objectives of the engagement, and a RACI model for the migration

III. Detail key foundation resources required for the Migration landing zone:
   a. IP connectivity / routing

b. VPN interconnectivity
c. DNS / AD integration
d. Database connectivity
e. Load balancer connectivity validation
f. API connectivity
g. SAN / NAS storage connectivity
h. Logging / monitoring integration testing
i. Backup / recovery verification
j. DR plan
k. Network and process latency
l. Customer-specific validation requests

III. Stage Two: Migration Planning / POC

Professional Services works to define and assist in the installation of the GCP foundation for migration.

a. Migration planning activities
   I. Schedule migration waves
   II. Recommend best practices and provide troubleshooting guidance on deploying Professional Services' "Migrate for Compute Engine"
   III. Review and further assess the detailed migration plan (migration runbook) for in-scope applications
   IV. Review migration grouping (waves) and [Customer]'s scheduling of the different migration waves

b. Pilot migration (POC)
   I. Migrate pilot wave
   II. Review/update the runbooks based on the pilot outcomes

IV. Stage Three: Migration Runs

Over the course of the engagement, Vendor works to migrate workloads through a series of two-week migration run. During which, vendor conducts the activities listed below.

a. Discovery — Assess existing infrastructure and organization
b. Planning — Plan migration priorities and build migration foundation
c. Runbook creation — Build prioritized migration plans
d. Pre-migration preparation — Optimize, clean up, and install migration prerequisite
e. Migration testing — Perform test clones and validate post-migration runbooks
f. Migration execution — Define and execute migrations using runbooks
g. Post-migration — Validate functionality and resources, and (if required) access rolling back
h. Clean-up — Archive historical VMs, final backups, retirement process

V. Stage Four: End-of-engagement review

Vendor to run an end-of-engagement review to document the progress made and identify potential future improvements. When the engagement concludes, all workloads will be migrated and running in GCP.

3. The Vendor is to propose a high-level overview of networking, compute & storage units that will be utilized to host the workloads

4. The Vendor is to also provide the project timelines to execute this SOW, along with the Project RACI

5. The Vendor is to provide pricing for this SOW in Appendix O.

Appendix G - VMware on AWS

1. Background

Customer has its on-premise data centres built on VMWare and is looking at options to establish a scalable, flexible and cost-effective hybrid cloud platform that protects its VMWare investments while driving cost savings and innovation through accelerated AWS Cloud adoption.

In this context, Customer has requested to develop a proposal for designing and implementing a hybrid cloud platform and:

I. Demonstrate migration of on-premise workloads to the established cloud platform with no refactoring and minimal configuration changes.

II. Establish framework to extend migrated workloads by leveraging AWS Cloud native services such as S3, Relational Database Services (RDS) etc.

III. Establish framework to integrate migrated applications to existing and future AWS Cloud native applications (e.g. Mobile apps etc.)

2. Solution Overview

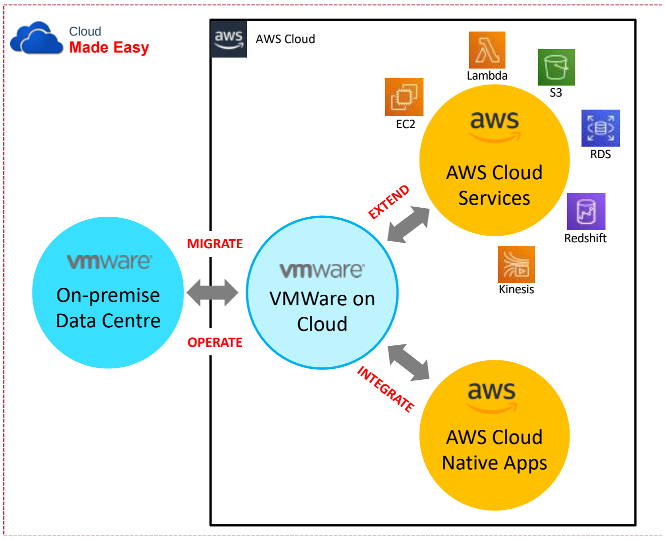
This SOW allows for rapid deployment of a scalable, flexible and secure hybrid cloud platform using VMWare Cloud (VMC) on AWS.

It includes:

I. A VMWare Cloud on AWS designed for rapid migration of Virtual Machines (VMs) from on-premise.

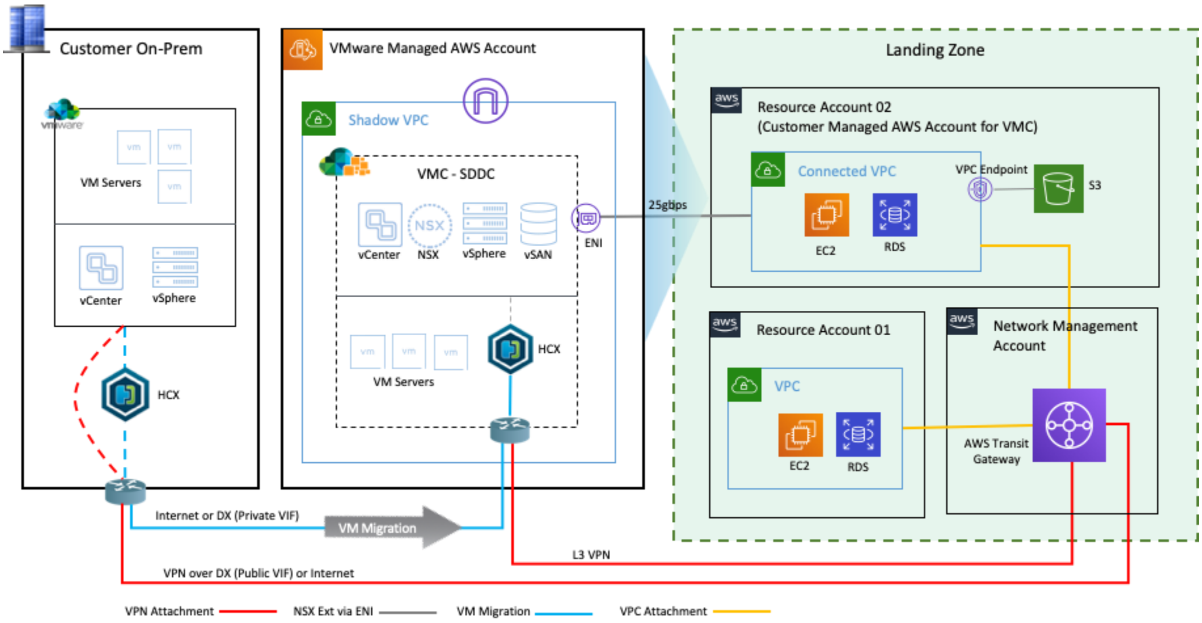
II. A secure, flexible and scalable AWS Landing Zone (LZ) that is tightly integrated with VMWare Cloud to allow not only cost-effective extension of Customer's traditional VM-based applications with AWS Cloud native services, but also seamless integration between Customer's traditional and cloud-native applications (built on AWS Cloud).

III. Flexible, fault-tolerant and high-speed network connectivity between Customer's on-premise datacentres and AWS Cloud designed, integrated and supported end-to-end by Singtel.



This SOW is designed to facilitate bulk migrations of VMs from on-premise to VMC making it relevant for both on-premise Data Centre extension and exit requirements. The integration between VMC SDDC (Software Defined Data Centre) and AWS Landing Zone is at networking level with focus on reliability, scalability and cost-effectiveness. Finally, the product is designed for fast deployment and allow Customer to establish an enterprise-grade hybrid cloud platform in as short as 2-3 weeks.

A high-level network architecture of Singtel's product is depicted below:



3. Features and Benefits:

I. **Offers a consistent VMWare experience**: Same tools (vCenter, vSphere, vSAN and NSx) across on-premises and VMWare Cloud allowing Customer to leverage its existing on-premises talent to drive cloud transformation.

II. **Built on VMWare HCx**: Enables fast, secure infrastructure lift-and-shift from on-premises to AWS Cloud while providing unified management and support.

III. **Singtel AWS Landing Zone**: Establishes a stable, secure, flexible and scalable base for Customer on AWS Cloud through a Landing Zone design aligned to AWS best practices

IV. **Optimal data egress charges**: Connectivity from VMC SDDC to AWS Cloud native services such as EC2, S3 and RDS on connected VPC through ENI preventing Customer from incurring any data egress charges.

V. **Scalable and secure cloud-native app integration**: Connectivity from VMC SDDC to cloud-native applications on AWS Cloud via VPN and Transit Gateway (TGW)

VI. **Flexible hybrid connectivity options powered by Singtel**:

   a. Internet or DX (Private VIF) for VM migration. Singtel offers Customer a choice of a permanent or temporary DX connectivity based on Customer context and use case.

   b. VPN over Internet or DX (Public VIF or Transit VIF) to access and operate resources on both VMC and AWS Landing Zone. This design ensures redundancy (Customer can use both Internet and DX) and hence increases overall reliability.

VII. **Designed for future growth**: Allows additional VMC SDDC and Landing Zone subnets and span across multiple availability zones in Singapore to support Customer's current and future growth needs

VIII. **Prod and non-Prod separation**: Across both VMC SDDC and AWS Landing Zone to ensure security and operational control and compliance. Isolated Prod and non-Prod integration across VMC SDDC and AWS Cloud.

IX. **Built for scale**: Designed to host a minimum of 200 VMs (4-node SDDC cluster) supporting production workloads

X. **Ease of maintenance**: Bastion access through AppStream enabling secure and easy way to access

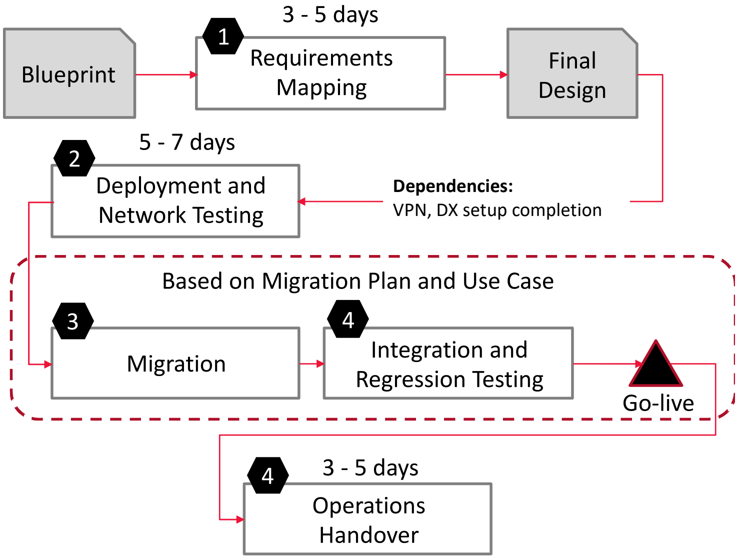
4. Points to note:

I. This SOW does not use VMC HCx L2 extender and hence on-premise IP addresses for VMs between will not be migrated to VMC SDDC. This in turn ensures a tighter integration at network level (CIDR range compatibility between VMC SDDC and AWS LZ) and ensures that Customer does not pay for data egress charges to access AWS Cloud native services from within VMC SDDC.

II. The product does not use Hybrid Linked Mode (HLM) to simplify design and reduce number of integration points (points of failure) in the hybrid cloud platform. Hence it will be swivel chair administration of vCenter across on-premises and cloud.

5. Engagement Approach

Singtel will use a blueprint based approach to enable a fast deployment of the hybrid cloud platform.



This methodology starts with a detailed blueprint that will be converted into a final design by Vendor through a detailed, but quick requirements mapping exercise with the Customer. Once the dependencies (hybrid connectivity etc.) are resolved, Vendor will deploy the final design and complete network testing. Vendor team will then work with Customer to design and execute a migration plan for identified workloads. Once tested and certified, Vendor will hand over the operations of hybrid cloud platform to the Customer nominated Operations team. Below section details the activities, expected outcomes, deliverables and assumptions for the end-to-end engagement approach.

Step 1: Requirements Mapping

Activities:

- Workshop with Customer team using Vendor’s blueprint to identify business, technical and security requirements for hybrid cloud platform

Expected Outcome:

- A common understanding of business requirements and hybrid cloud platform design between Customer and Singtel teams

Deliverables:

- Updated blueprint or in other words, Final Design Document

Assumptions:

- Customer will identify and makes available relevant personnel for attending the requirements mapping workshop. Customer provides necessary logistics to conduct the workshop

- Customer's business requirements can be met within Singtel's blueprint. Any changes beyond blueprint scope will be handled as a bespoke engagement.
- There is sufficient Internet bandwidth at Customer premises
- Availability of Direct Connect (DX) between AWS and Customer on-premises environment

Step 2: Deployment and Network Testing

Activities:

- Configure VMC as per final design
- Complete AWS Cloud deployment including VMC integrations as per final design
- Establish hybrid connectivity between on-premises and AWS Cloud
- Perform end-to-end connectivity testing

Expected Outcomes:

- A hybrid cloud platform ready for workload (VMs) migration from on-premises to VMC on AWS Cloud

Deliverables:

- Deployment instructions
- End-to-end connectivity test summary and test results

Assumptions:

- Customer owns and performs updates / testing at application level
- Customer owns and supports any network configuration changes / firewall changes at its end to support setting up end-to-end connectivity

Step 3: Workload Migration

Activities:

- Identify sample workloads (VMs) to test migration from on-premise to cloud (VMC)
- Test migration of identified workloads in non-Prod. Update integrations and required configurations to handle IP address change.
- Develop detailed migration plan based on inputs from target workload migration

Expected Outcomes

- A fully tested hybrid cloud platform with a detailed migration plan to move on-premises workloads

Deliverables:

- High-level Workload Migration Plan
- Auditable test results from sample workload migration

Assumptions:

- There is sufficient Internet bandwidth at Customer premises
- Customer provides IP addresses for allocation
- Singtel will be provided access to Customer on-premise vCenter
- Customer has pre-defined data classification policy

Step 4: Operations handover

Activities:

- Prepare and handover Operations handover checklist to Customer
- Perform in-classroom Operations handover to Singtel nominated operations team

Expected Outcomes:

- An Operations team that is fluent and well-versed with the new hybrid cloud platform

Deliverables:

- Operations handover checklist

Assumptions:

- Customer nominated Operations team has sufficient skills and experience to take over the hybrid cloud platform

6. Organization Structure

Vendor Project Team Organization - Vendor to provide how the delivery team will be setup for this SOW

7. Proposed High Level Timeline

#	Step	Duration	Start Date	End Date
1	Step 1: Requirements Mapping			
2	Step 2: Deployment and Network Testing			
3	Step 3: Workload migration			
4	Step 4: Operations handover			

8. Vendor to provide pricing for this SOW in Appendix O.

Appendix H - VMware on GCP

1. Background

Google Cloud VMware Solution delivers a simple and seamless way to migrate to the cloud without having to re-architect or refactor applications and allows benefit from flexible, on-demand capacity to rapidly meet business needs and realize cost savings compared to running workloads on-premises.

Customers running VMware-based workloads in Google Cloud allows them to maintain operational continuity and leverage existing investments and tools, while benefiting from the agility, speed, and automation of the cloud.

Workloads continue to run on a native VMware SDDC stack on bare metal, including VMware vSphere, vCenter, vSAN and NSX to ensure consistency and compatibility. This allows you to migrate, manage, and scale workloads from your data center to the cloud, without refactoring or causing disruption to your network, security, or operational policies. Google Cloud's API lifecycle management capabilities also deliver consistent operations, so your teams don't have to worry about patches, upgrades, or maintenance, freeing up time for customers to focus on value add projects.

By migrating applications to Google Cloud, customers can access new business insights from existing data by connecting to native Google Cloud services via APIs. Plug into native Google Cloud services such as BiqQuery, AutoML, and AI services to make real time, data-driven business decisions and derive additional value from data available. Combined with the benefits of speed and agility, this solution not only allows you to seamlessly lift and shift, but lift and improve your workloads by deriving additional value and freeing up resources inside an organization.

2. Solution Overview

VMware permissions - In order for Migrate for Compute Engine to work properly in an on-premises data center, a VMware administrator must perform the following:

1. Deploy the Migrate for Compute Engine On-Premises Backend virtual appliance OVA.
2. Create and assign vCenter roles for Migrate for Compute Engine to manage migrations.

Scope

I. Permissions needed to be defined at the source environment:
For Migrate for Compute Engine to work properly on an on-premises data center a VMware administrator needs to:
- Vendor needs to deploy the Migrate for Compute Engine On-Premises Backend virtual appliance.
- Vendor needs to create and assign vCenter roles for Migrate for Compute Engine to manage migrations for the Migrate for Compute Engine Service user in vCenter by assigning the Migrate for Compute Engine service role

II. Secure Migrate for Compute Engine deployment prerequisites
- Vendor to confirm the bandwidth in place between the source and target (GCP) environments is larger than 20 Mbit/sec symmetric.
- Vendor to confirm that the VMs targeted for migration are running supported a supported operating system.
- If the source environment includes VMware, Vendor to verify the version is supported by reviewing on-premises requirements. VMware versions Migrate for Compute Engine supports migrations from VMware vCenter and ESXi.
- The latest Migrate for Compute Engine release is compatible with the following VMware versions:
    - vCenter: 5.5U1, 6.0U1, 6.5, 6.5U1, 6.7

- ESXi: 5.5U1, 6.0 U1, 6.5, 6.7

Customer environment details	
Operating systems	Customer environment has the following operating systems • <Placeholder for actual list>
VMware versions	vCenter Version: ESXi Version:
Storage devices	<Placeholder for any special storage solutions used on prem> *Virtual Machine disks in Dependent mode (default) and Virtual RDM mode are supported with full functionality.
Network bandwidth	1.5 Gbps connectivity between the data center and GCP via VPN

III. Network connectivity

Vendor to perform a migration, connect the components, which means setting up the following resources:

- Firewall rules across all environments: on-premises and Google Cloud Platform Virtual Private Cloud.
- VPNs or other network connections are set up with routing and forwarding rules to the correct network subnets and VMs between GCP, or inside the corporate LAN.
- GCP Network Tags or Instance Service Accounts that allow traffic to pass between instances.

IV. IAM

Before migrating applications using Migrate for Compute Engine, vendor to configure GCP organization and setting up a GCP organization. Once GCP organization is ready, vendor need to create GCP roles and service accounts that Migrate for Compute Engine to create GCP resources and manage the Cloud Storage API. Migrate for Compute Engine also should include a Cloud Shell script for making these changes - The script creates roles and service accounts in the infrastructure project. Vendor to prepare the script to create the Migrate for Compute Engine Manager role at the organization level, creating the other role and service accounts in the infrastructure project.

3. Assumptions:

Customer nominated Operations team has sufficient skills and experience to take over the hybrid cloud platform

4. Organization Structure

Vendor Project Team Organization - Vendor to provide how the delivery team will be setup for this SOW

5. Proposed High Level Timeline

#	Step	Duration	Start Date	End Date
1	Step 1: Requirements Mapping			
2	Step 2: Deployment and Network Testing			
3	Step 3: Workload migration			
4	Step 4: Operations handover			

6. Vendor to provide pricing for this SOW in Appendix O.

Appendix I - Managed Services

1. Scope of Service Matrix details with the relevant Service Tiers are as follows:

Managed Services

	Scope of Service	**Day 2 Bronze**	**Day 2 Silver**	**Day 2 Gold**	**Scope**
a	Transition from Day 1 (Design/Implementation) to Day 2 (Managed Services) teams.	X	X	X	Vendor to provide a detail template for consistency detailing the following: i. Pre-requisties comprehensive checklist of tranisition from Day 1 to Day 2; ii. Design Document as a template for consistency (also to facilitate acceptance and subsequent records for work done and for proper hand over) for defined acceptance criteria; iii. The project coordination activities; iv. Transition deliverables and timing; v. Transition period cannot be more than 1 month. Vendor will pay to Singtel a service credit of Two Hundred and Fifty US Dollars for each day beyond for which the Transition period SLA was not met ("Transistion Service Credit"). vi. Governance procedures.
b	Logging, Monitoring and Event Management	X	X	X	a. Vendor Managed Services shall monitor End Singtel Managed Environment for logging activity, availablity, performance and Alerts based on different health checks. b. Vendor Managed Services will monitor and investigate Alerts that are created whenever one or more alarms from applicable Vendor services are triggered. Alerts will be investigated by Vendor Managed Services to determine if they qualify as an Incident. c. Vendor Managed Services will aggregate and store all logs generated as a result of all operations in CloudWatch Logs and CloudTrail.

					d. Vendor to provide Singtel access to Vendor System(s) for visibility for Logging, Monitoring and Event Management. Vendor will also allow Singtel make enquiries or conduct inspections, at its discretion, without demand to confirm the Services are provided with respect In-Scope Services set out. e. Vendor will provide monthly reports to Singtel according to a format to be determined to facilitate acceptance and payment for work done in this section.
c	Continuity Management		X	X	a. Vendor Managed Services provides backups of Stacks using standard, existing Amazon Elastic Block Store (EBS) and RDS snapshot functionality (or equivalent) on a scheduled interval determined by the End Singtel. b. Restore actions from specific snapshots must be performed by Vendor Managed Services per End Singtel. Data changes that occur between snapshot intervals are the responsibility of the End Singtel to backup. c. The End Singtel may submit a backup/snapshot requests outside of scheduled intervals. In the case of Availability Zone (AZ) unavailability in a Region, with the End Singtel's permission, Vendor Managed Services will restore the Managed Environment by recreating new Stack(s) based on templates and available EBS snapshots (or equivalent) of impacted Stacks.
d	Security and Access Management		X	X	a. Vendor Managed Services provides Security Management services such as configuring anti-malware protection, intrusion detection and intrusion prevention systems. b. Vendor Managed Services also configures default Vendor security capabilities that will be approved by the End Singtel during onboarding, such as Identity Access Management (IAM) roles and EC2 security groups(or equivalent). End Singtels will manage their users via an approved directory service provided by the End Singtel.

					c. Vendor Managed Services also configures VM Endpoint Protection: Cloud Antivirus/Malware to: • Protect the End Singtel's in scope VMs against malware including, but not limited to, viruses, trojans, and spyware. • Help automatically checks for new vendor malware signature updates every 15 minutes. • Help deliver remediation actions which clean, delete, deny access, or quarantine malicious software identified. d. Vendor will provide standard monthly reports detailing events encountered, investigation and remediation taken are provided as part of the Services. e. Vendor will assess AWS Master Account Management and including initial Build of root accounts. f. Vendor will assess AWS Identity, Federation and Role based groups design to be deployed to meet End Singtel's policies. g. Vendor will assess Key Management Services to meet End Singtel's Policies. h. Vendor will assess Endpoint Security Services that includes End Singtel's Vulnerability and Compliance Checks and Reporting. i. Vendor will assess Encryption Services for End Singtels that includes storage and databases. j. Vendor will provide monthly reports to Singtel according to a format to be determined to facilitate acceptance and payment for work done in this section.
e	Patch Management		X	X	a. Vendor will assess Managed Services that applies and installs updates to EC2 instances for supported operating systems and software pre-installed with supported operating systems. b. End Singtels chose a monthly one-hour maintenance window for Vendor Managed Services to perform

					maintenance activities including patching activities. Vendor Managed Services will apply Critical Security Updates outside of the selected maintenance window. Vendor Managed Services will apply Important Updates during the selected maintenance window. c. Patch Management is limited to Stacks in the Managed Environment, including all Vendor Managed Services Managed Applications and supported Vendor services with patching capabilities (e.g. RDS or equivalent). d. In order to assess all types of infrastructure configurations when an update is released, Vendor Managed Services will i. Update the EC2 instance (or equivalent) and ii. Provide an updated Vendor Managed Services AMI for the End Singtel to use. Vendor Managed Services will notify the Singtel in advance with the details of the upcoming updates. e. The End Singtel can exclude Stacks from Patch Management or reject updates as they deem fit. If the End Singtel rejects an update provided under Patch Management, but later changes their mind, the End Singtel will be responsible for initiating the update. f. It is the End Singtel's responsibility to install, configure, patch, and monitor any additional applications not specifically covered above. g. Vendor to provide a monthly Patch Management Report, showing the patch level of each managed VM Or showing the status of Critical/High/Medium/Low Security patches not applied to the managed VMs. Vendor to provide real-time dashboard beyond static report shared in the former.
f	Change Management			X	a. Vendor will offer Managed Services to facilitate Change Management, which is the mechanism for End Singtels to get access to or affect any changes in their Managed Environment.

					b. Vendor will assess the End Singtel Change Management Service Request(s) when required. c. Vendor will assess the End Singtel Change Management Service Request(s) to make changes and to follow a defined Change Management process. Access to Singtel resources within a managed environment is only possible unless authorized and requested by the Singtel and must be approved by Vendor Managed Services before it is actioned. Alternatively, if the change is initiated by day-2 Vendor, then the approval will be at End-Singtel end. d. Vendor will assess the End Singtel to a designated start time for the requested change to be performed through the Change Management process. e. Vendor will ensure the Change Management service consists of the following activities in relation to the In-Scope Services: i. log and track all Change Requests from receipt to completion; ii. manage Change Requests using the appropriate Pre-Approved Change, Simple Change or Complex Change type category; iii. provide, update and manage the processes by which Changes are made to your In-Scope Services; iv. validate authorisation of Changes; Vendor will pay to Singtel a service credit of Two Hundred and Fifty US Dollars for each unauthorised change. (“Unathorised Change Service Credit”). v. plan, test, coordinate, implement, configure, certify, manage and monitor approved Changes;

					vi. co-ordinate all internal and external parties to execute approved Changes; i. review and schedule all proposed Changes, including details of any proposed scheduled outages and communicate those details to you in accordance with the agreed change management procedures, if any; ii. where appropriate, develop a contingency plan for Changes prior to implementation; iii. update the relevant technical, management, operational and procedures documentation for all implemented Changes and distribute the updated documentation. iv. implement the Change subject to suspension of the Service Levels applicable to the relevant service, until the parties have agreed to appropriate amendments to the relevant Service Level. f. Vendor to assess the Change Management process against the Service Levels as defined in section 4.2. g. Vendor will provide monthly reports to Singtel according to a format to be determined to facilitate acceptance and payment for work done in this section.
g	Incident		X	X	a. Vendor will provide Managed Services and proactively notify Singtels of Incidents detected by Vendor Managed Services. b. Vendor will provide Managed Services and respond to Incidents and resolve Incidents in a time bound manner based on the Incident priority and against Acceptable Quality Level (AQL) to meet for Incident closure. Acceptable Quality Level (AQL) would be aligned to Singtel expectation as desired towards a Service Improvement Plan (SIP).

					c. Vendor to provide Singtel access to Vendor System(s) for visibility for Incident Management. Vendor will also allow Singtel make enquiries or conduct inspections, at its discretion, without demand to confirm the Services are provided with respect In-Scope Services set out. d. Vendor to provide Incident Response and Incident Resolution report as a Service Level Reporting on a Monthly frequency including a Four month rolling summary of: i. Incidents closed; ii. Unresolved incidents; iii. Incident response times; and iv. Performance against incident response Service Levels. e. Vendor to provide "War room" in the event of Critical Castrophic Service Incident (as determinded by Singtel) and provide: i. Vendor's conference bridge within 60 mins of incident being raised; and ii. Provide an hourly update until incident is resolved. f. The Incident Management process is responsible for managing the lifecycle of all incidents. Incident Management ensures that normal service operation is restored as quickly as possible and the business impact is minimized. Vendor to note that any unplanned event which is not part of normal service operation and causes interruption or degradation to a service will be recorded as an incident. g. Vendor to ensure that the Incident Management service features consists of the following incident management activities in respect of the In-Scope Services: i. log, action and monitor incidents; ii. establish incident classification and priority;

					iii. assign incidents to appropriate assess resolver groups; iv. update existing incidents with new information or status; v. monitor and track incidents; vi. maintain a record of all enquiries, incidents and request for change; vii. provide a notification and an escalation point for issues relating to incidents; viii. activate the End Singtel escalation process (where required); and ix. liaise with authorised operational contacts and assist in End Singtel planning options to minimise the impact of scheduled outages. h. Suppiler to ensure that Incident reports will remain open until incident is resolved. i. Vendor will provide monthly reports to Singtel according to a format to be determined to facilitate acceptance and payment for work done in this section.
h	Problem Management		X	X	a. Vendor Managed Services will investigate Problems and identify the root cause, and remediate them either with a workaround, or a permanent solution that prevents recurrence of similar future Incidents. b. Vendor to provide Singtel access to Vendor System(s) for visibility for Problem Management. Vendor will also allow Singtel make enquiries or conduct inspections, at its discretion, without demand to confirm the Services are provided with respect In-Scope Services set out. c. Vendor to define what type of Incident ticket will become a problem ticket. All problem ticket must have Acceptable Quality Level (AQL) to meet for Incident closure. Acceptable Quality Level (AQL)

					would be aligned to Singtel expectation as desired. towards a Service Improvement Plan (SIP). d. Vendor to propose what kind of incident gets promoted into a Problem Ticket e. Vendor to ensure that there exisit a Problem Management process for managing the lifecycle of all problems. The objective of Problem Management is to prevent incidents from happening, and to minimize the impact of incidents that cannot be prevented. A problem is the unknown cause of one or more incidents. Problem Management seeks to investigate and diagnose the underlying cause of incidents. f. Vendor to ensure that there is a Problem Management service feature is designed to minimise: i. the adverse impact of an incident or technology solution-related problems impacting End Singtel business; and ii. future re-occurrence caused by errors within the relevant infrastructure. g. Vendor to ensure that the Problem Management process consists of the following activities: i. relate incidents to open problem records; ii. manage individual incidents and problems for trend analysis and to help prevent re-occurrence; iii. diagnose problems and attempt resolution; iv. provide a comprehensive problem management process that is consistent with an common problem management practices agreed between Vendor and Singtel;

					v. develop, maintain and update the approved problem management process for the management of service-related problems from point of receipt of the incident or problem by Singtel; and vi. complete problem reviews for priority level 1 critical incidents. h. Vendor will provide monthly reports to Singtel according to a format to be determined to facilitate acceptance and payment for work done in this section. i.
i	Reporting			X	a. Vendor Managed Services to provide End Singtels with a monthly service report which summarizes key performance metrics of Vendor Managed Services. Reports are delivered by a Vendor Cloud Service Delivery Manager (CSDM) assigned to the End Singtel. b. Vendor to provide Singtel an Incident Response and Incident Resolution report as a Service Level Reporting on a Monthly frequency including a Four month rolling summary of: i. Incidents closed; ii. Unresolved incidents; iii. Incident response times; and iv. Performance against incident response Service Levels.
j	Service Request Management			X	a. Vendor to assess End Singtels who can request information on their Managed Environment, Vendor Managed Services, or Vendor Service Offerings by submitting Service Requests. b. Vendor to assess a Service Request provides a channel for End Singtels to make standard requests in relation to In-Scope Services. The Vendor is to follow the request fulfilment process to log, track, action, manage and resolve all enquiries. c. All enquiries which are not deemed an incident or a Change will be treated as a Service Request.

					d. Vendor will provide monthly reports to Singtel according to a format to be determined to facilitate acceptance and payment for work done in this section. e. Vendor service request turnaround time based on types of Service Request. Service Request handling be limited to normal office hour (5 days week). Eg. Urgent SR – within 1 day (Chargable-to be agreed with Singtel). Normal SR – within 2 days and during office hours.
k	Service Desk		X	X	a. Vendor will provide Managed Services staffs engineering operations with full-time employees to fulfill non-automated requests including Incident Management, Service Request Management, and Change Management. The Service Desk operates 24 x 7 X 365 days a year. b. The Vendor Service Desk is available via a local contact number during the hours of operation as specified above. c. Vendor will provide a single point of contact for registration and management of the following actions: i. Service Request – any enquiry made with the Service Desk that does not result in a Change or an incident work request being raised; ii. Incident – any issue related to In-Scope Service performance which requires rectification by Vendor and/or Singtel, or a third party under Vendor and/or Singtel' control involved in the provision of the relevant In-Scope Service. iii. Change – all changes with the managed environment including Pre-Approved Change, Simple Change and Complex Change type categories to an In-Scope Service. d. Vendor will provide monthly reports to Singtel according to a format to be determined to facilitate acceptance and payment for work done in this section.

Managed Services Roles & Responsibilities

Vendor will support the Services in accordance with the Responsibilities and Singtel Responsibilities set out in the following table 4 below (where R= Responsible, A=Accountable, C=Consulted, I= Informed).

Table 2.2 : Roles & Responsibilities

	Task	Vendor	End Singtel
a	CSP Console, identity, and permission management	R	A
b	Consolidated invoice creation for all linked CSP Hosting accounts	A	I
c	Production and distribution of monthly cost optimization reports	A	I
d	Creation of new CSP Hosting accounts for management through the Services	A	R
e	Configuration of CSP Hosting accounts (e.g. firewall configuration, vpc creation)	A	R
f	Respond to and acknowledge alerts	A	I
g	Opening all tickets with Vendor support for problems, issues, and questions regarding the Services service	R	A
h	Opening all tickets with Vendor support for problems, issues, and questions regarding the AWS provided services	R	A
i	Analysis, Tirage, and Response to support issues raised by End Singtel	A	I
j	Any changes made to the CSP environment based on the cost optimization report	A	I
k	Implement the agreed tagging strategy	A	I

Response, Resolution and Escalation Service Levels.

Below is the Incident - Response, Resolution and Escalation Service Levels. Reference is taken to table in this section for Vendor to support and comply as part of this SOW.

a) Priority means the level classification of the incident which is automatically calculated by the Vendor Service Desk based an assessment of the impact and urgency of the logged incident.

b) Incident Response Time means the time between End Singtel sending an incident message or making a call to Vendor and End Singtel receiving an email or call from Vendor acknowledging receipt and advising End Singtel of the actions being taken to rectify the incident. During this time the incident will allocated to appropriate personnel. Vendor will respond to incident notifications within the Incident Response Times shown in this section.

c) The Business Hours timeframes above are dependent on the call being logged with the Vendor Service Desk after 9:00 am and before 6:00 pm local time in Singapore. Calls logged after this time will be reflected as being recorded the next Business Day.

d) Incident Resolution Time means implementing a permanent solution or implementing an acceptable workaround to restore service until a permanent solution is identified. Additional work maybe required after service restoration in order to provide a final corrective resolution. This would be driven through Vendor Problem Management and /or Change Management process. Incident Resolution Time is measured from the creation date/time stamp of the incident to the time when Vendor has achieved service restoration minus the time spent by non-Vendor teams.

Table 2.3 : Response, Resolution and Escalation Service Levels

Definition		**Vendor Service Desk Response**			**Escalation**	
Priority Level	**Hours**	**Incident Response Time**	**Incident Resolution Time**	**Service Level Target**	**Escalation Response Time**	**Contact*** (* to be provided by Vendor)
1-Critical	24x7	< 30 Minutes	<4 hours	> 90% AQL (i.e. >90% tickets closed within SLA)	Immediate	Shift/Team Leader and Service Delivery Manager
					Triggered when SLA failed.	Service Assurance Manager
					Triggered when SLA failed.	Operations Director and General Manager
2-High	24x7	< 60 Minutes	<8 Hours	> 90%	> 4 Bus. Hours	Shift/Team Leader and Service Delivery Manager
					> 1 Bus. Days	Service Assurance Manager
					> 2 Bus. Days	Operations Manager and General Manager
3-Medium	24x7	< 1 Bus. Day	<5 Bus. Days	> 80%	> 2 Bus. Days	Shift/Team Leader
					> 5 Bus. Days	Service Assurance Manager And Service Delivery Manager

Definition		Vendor Service Desk Response			Escalation	
					> 10 Bus. Days	Operations Manager
4-Low	24x7	< 1 Bus. Day	<10 Bus. Days	> 80%	> 7 Bus. Days	Shift/Team Leader
					> 10 Bus. Days	Service Assurance Manager And Service Delivery Manager
					> 14 Bus. Days	Operations Manager

Table 2.4 : Incident Priority Level Determination

Priority Level	Description
1 – Critical	Any incident which causes severe impact to End Singtel business operations where no workaround is available or exists. End Singtel are affected by: • Service stoppage or malfunction; • Substantial reduction in service performance due to an outage, fault, issue or degradation of a business critical application; • Time-sensitive application to all or majority of business units within End Singtel organisation.
2 – High	Any incident which causes major impact to End Singtel business operations where no workaround is available but an alternative and temporary fix is possible. End Singtel are affected by: • Service degradation • Varying level of reduction in service performance due to a fault, issue or degradation of essential business applications • Time-sensitive application to at least one user or business units within End Singtel organisation.
3 – Medium	Any incident which causes partial impact to End Singtel business operations where a workaround is available. End Singtel are affected by: • Non-critical fault and issues that can still allow End Singtel business operations to function

Priority Level	Description
4 – Low	Any incident which has non-critical, minor or no impact to End Singtel business operations. A workaround may be available or exists but not necessary. End Singtel may or may not be affected by: • Minor issues that cause a tolerable or slight inconvenience to at least one user or business units within End Singtel organisation; or • Any incident that may not be associated with End Singtel business operations but rather informational in nature than technical.

Change Management Service Levels

The actions to be taken during this time and the Service Levels for Changes are summarised below. Vendor is to comply to the timeframe against the associated Change type stipulated in table 7.

a) Change Response Time means the time between End Singtel logging a Change Request at the Vendor's Change Management channel and the Vendor Service Desk acknowledging receipt along with a Change ticket reference number for tracking purposes.

a. Change Resolution Time means the time between End Singtel upon approval of a Change Request at the Vendor's Change Management channel and:

i. Vendor advising End Singtel of completion of a Pre-Approved Change or Simple Change; or

ii. Vendor advising End Singtel for a Complex Change* (e.g, Upgrading of OS to higher major version) that will be properly scoped with a statement of work, timeframe for completion and pricing, and allocated to appropriate personnel for action; (*Chargable - Vendor to be consulted) or

b) Timeframe applies to standard business operating hours: 9am to 6pm Monday to Friday, excluding public holidays. Vendor reserves the right to amend the timeframe depending on the complexity of the Change Request.

Table: Change Requests - change types, response times and actions

Change Type	Timeframe*	Actions	Service Level Target
Pre-Approved Change	1 Business Day Change Response Time	• Contact End Singtel to acknowledge Change Request; • Provide change ticket number for tracking purposes;	• 90% completed in each month for Timeframe.
Simple Change	1 Business Day Change Response Time	• Contact End Singtel to acknowledge Change Request; • Provide change ticket number for tracking purposes;	• 90% completed in each month for Timeframe.

Change Type	Timeframe*	Actions	Service Level Target
	2 Business Days Change Resolution Time in addition to the 1 Business Day Change Response Time	• Implement the Change; • Notify Vendor or dispatch work request to the appropriate service provider(s) to perform the change • Vendor will contact the Singtel directly to implement the change • Provide confirmation of completed change.	• 90% completed in each month for Timeframe.
Complex Change	1 Business Day Change Response Time	• Contact End Singtel to acknowledge Change Request; • Provide change ticket number for tracking purposes.	• 90% in each month for Timeframe.
	7 Business Days for quote to be provided plus Change Response Time	• Provide a quote for the change.	• 95% in each month for Timeframe.
	Where carriage provisioning is required; 21 Business Days Change Resolution Time once carriage is provisioning is complete. Where carriage provisioning is not required; Change Resolution Time is as per timeframe presented in quote.	• Vendor shall advise of ready for service (RFS) date including installation of device on End Singtel site • Dispatch work request to the appropriate Vendor team; and • Provide confirmation of completed change.	• Completion within quoted Timeframe plus 5%.

2. Service Level Availability

At minimum Vendor must achieve minimal Service Availability of >=99.95% uptime per calendar month. Vendor's Service Level for the Services is 99.95% availability during the Total Minutes in each measurement period of one calendar month starting on the first day of the month following the completion of onboarding. Availability is defined as Vendor Managed Service being available for Singtel to without impact to End Singtel business operations set out in this SOW (e.g. Priority 1 or Priority 2 resolution time). Availability is calculated as a percentage (rounded to 1 decimal place) where for the measurement period:

[(Actual Services Available Minutes) + (Permitted Outage Minutes)] / (Total Minutes)) x 100 and where:

i. “Actual Services Available Minutes” is calculated as 24 x 60 x number of days in the measurement period minus total Outage Time in that measurement period.

ii. “Permitted Outage Minutes” means the period in minutes for all Permitted Outages during a measurement period.

iii. “Total Minutes” is calculated as 24 x 60 x number of days in the measurement period.

3. Response Service Credits

Vendor will pay the associated Response Service Credits in any given month for the following situations.

a. If Vendor fails to respond to a Priority 1 or Priority 2 incident within the Response Time SLAs, a service credit of Two Hundred and Fifty Singapore Dollars for each incident for which the Response Time SLA was not met (“Response Service Credit”) will apply.
b. If Vendor fails to meet the minimum availability >=99.95% uptime per calendar month, a service credit of Five Hundred Singapore Dollars for which the Service Availability SLA was not met (“Response Service Credit”) will apply.

4. Reporting

Vendor must provide the following report(s) by the corresponding Due Date(s) below and each report is defined by a specific unique Singtel Project.

Description of Report	Due Date
Logging, Monitoring and Event Management - Vendor will provide monthly reports to Vendor according to a format to be determined to facilitate acceptance and payment for work done in this section.	1st Wednesday of every month
Security and Access Management - Vendor will provide standard monthly reports detailing events encountered, investigation and remediation taken are provided as part of the Services. Vendor will provide monthly reports to Vendor according to a format to be determined to facilitate acceptance and payment for work done in this section.	1st Wednesday of every month
Patch Management - Vendor to provide a monthly Patch Management Report, showing the patch level of each managed VM Or showing the status of Critical/High/Medium/Low Security patches not applied to the managed VMs. Vendor to provide real-time dashboard beyond static report shared in the former.	1st Wednesday of every month
Change Management - Vendor will provide monthly reports to Vendor according to a format to be determined to facilitate acceptance and payment for work done in this section.	1st Wednesday of every month

Incident - Vendor to provide Incident Response and Incident Resolution report as a Service Level Reporting on a Monthly frequency including a Four month rolling summary of:
I. Incidents closed;
II. Unresolved incidents;
	1st Wednesday of every month

III. Incident response times; and IV. Performance against incident response Service Levels. Vendor will provide monthly reports to Vendor according to a format to be determined to facilitate acceptance and payment for work done in this section.	
Service Request Management - Vendor will provide monthly reports to Vendor according to a format to be determined to facilitate acceptance and payment for work done in this section.	1st Wednesday of every month
Service Desk - Vendor will provide monthly reports to Vendor according to a format to be determined to facilitate acceptance and payment for work done in this section.	1st Wednesday of every month
Operational Integrations and CMDB - Vendor will provide monthly reports to Vendor according to a format to be determined to facilitate acceptance and payment for work done in this section.	1st Wednesday of every month

5. The Vendor is to propose pricing for this SOW in Appendix O. The pricing shall be in both :
    a. % of Public Cloud consumption
    b. Per VM pricing

Appendix J – Manpower Services

To outline your Cloud Professional Services Capabilities, including the Certifications and Competencies in Public, Private and Hybrid Clouds, including number of delivery personnel in Singapore and overseas, as well as frameworks and methodologies.

Cloud Specialist	Years of AWS Experience	Number of Directly Employed Staff Certified (In Singapore)	Number of Directly Employed Staff Certified (Outside Singapore)
AWS Solutions Architect (Associate)	>2		
AWS Developer (Associate)	>2		
AWS SysOps Administrator (Associate)	>2		
AWS Solutions Architect (Professional)	>3		
AWS DevOps Engineer (Professional)	>3		
AWS Advanced Networking (Speciality)	3-5		
AWS Security (Specialty)	3-5		

Cloud Specialist	Years of Azure Experience	Number of Directly Employed Staff Certified (In Singapore)	Number of Directly Employed Staff Certified (Outside Singapore)
Microsoft Certified: Azure Administrator Associate	>2		
Microsoft Certified: Azure Security Engineer Associate	>2		
Microsoft Certified: Data Analyst Associate	>2		
Microsoft Certified: Azure Developer Associate	>2		
Microsoft Certified: Azure Data Engineer Associate	>2		
Microsoft Certified: Azure Solutions Architect Expert	3-5		
Microsoft Certified: DevOps Engineer Expert	3-5		

Cloud Specialist	Years of GCP Experience	Number of Directly Employed Staff Certified (In Singapore)	Number of Directly Employed Staff Certified (Outside Singapore)
Google Cloud Certified - Associate Cloud Engineer	>2		
Google Cloud Certified - Professional Cloud Architect	>3		
Google Cloud Certified - Professional Cloud Network Engineer	>3		
Google Cloud Certified - Professional Cloud Security Engineer	>3		

Google Cloud Certified - Professional Cloud Developer	>3		
Google Cloud Certified - Professional Data Engineer	3-5		
Google Cloud Certified - Professional Data Analyst	3-5		

Appendix K – Customer References

The vendor is to outline a list of Customer Projects in Singapore and overseas, and highlight the Customer’s challenge, objectives, complexities of the project, why you were selected, and how did you differentiate your company from the competition.

No	Customer Projects in Singapore and overseas Project Scope	Date of Rollout/Handover of project (Month/Year)	Why you were selected, and how did you differentiate your company from the competition	Contact Person for validation

Appendix L - Key Differentiators

Key differentiators	Highlight your key differentiators
Unique value proposition which your company can brings to Singtel and its customers.	

Appendix M- Vendor Terms and Conditions

By participating in the RFP, the vendor accepts all terms in the GMSA and Services Module provided in RFP package, and will in good faith work with Singtel to finalise the Statement of works within 2 weeks from the award of the RFP.

(i) The Singtel Group Mater Supply Agreement (GMSA)

_DSC_Group MSA
BaseTCs High 01101

(ii) Services Module

SERVICES
MODULE.pdf

Appendix N – Governance

The Collaboration Governance model shall include regular deal cadences, project reviews, escalation and support paths to ensure Customer Projects are delivered successfully. The Supplier must comply with the governance set out or referred by Singtel from time to time.

Please submit a governance structure for

(i) Deal Cadences
(ii) Project Reviews
(iii) Escalation and Support Paths

Example

Levels	**Name**	**Contact details**	**Position**	**Role or function under this SOW (including time dedicated)**
Level 0			Sales Manager	Sales Manager
			Sales Director	Sales Director
Level 1			Associate Solution Architect	Shift/Team Leader
			Group - Operation Manager	Service Assurance Manager
			Operations Director	Operations Director
Level 2			Associate Solution Architect	Shift/Team Leader
			Project Coordinator	Project Coordinator
			Group - Operation Manager	Service Assurance Manager
			Operations Director	Operations Director
Level 3			Solution Architect	Shift/Team Leader
			Group - Operation Manager	Service Assurance Manager And Service Delivery Manager
			Operations Director	Operations Director
			CTO	CTO

Appendix O – Pricing

Special Notes:

- Pricing is by Customer Project.
- Suppliers will be requested to supply and provide more competitive pricing for Strategic / larger deals.

1. Landing Zone Design - AWS

Type	Customer Size	Estimated Man Days	Price (SGD)
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

2. Landing Zone Design - Azure

Type	Customer Size	Estimated Man Days	Price (SGD)
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

3. Landing Zone Design - GCP

Type	Customer Size	Estimated Man Days	Price (SGD)
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

4. Migrations (AWS)

Type	Customer Size	Estimated Man Days	Price (SGD)
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

5. **Migrations (Azure)**

Type	**Customer Size**	**Estimated Man Days**	**Price (SGD)**
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

6. **Migrations (GCP)**

Type	**Customer Size**	**Estimated Man Days**	**Price (SGD)**
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

7. **VMware on AWS**

Type	**Customer Size**	**Estimated Man Days**	**Price (SGD)**
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

8. **VMware on GCP**

Type	**Customer Size**	**Estimated Man Days**	**Price (SGD)**
Tiny	< Up to 20 VMs		
Small	> Up to 50 VMs		
Medium	51VMs - 120 VMs		
Large	121 VMs and Greater		

9. Managed Services (AWS, Azure, GCP)

a. Managed Service - Per VM Model

Dedicated Resources

Type	Customer Size	Estimated Man Days	Price (SGD)
Brownfield Environment - Tiny	< Up to 20 VMs		
Brownfield Environment - Small	> Up to 50 VMs		
Brownfield Environment - Medium	51VMs - 120 VMs		
Brownfield Environment - Large	121 VMs and Greater		
Green Field Environment -Tiny	< Up to 20 VMs		
Green Field Environment - Small	> Up to 50 VMs		
Green Field Environment Medium	51VMs - 120 VMs		
Green Field Environment - Large	121s and Greater		

Shared Resources

Type	Customer Size	Estimated Man Days	Price (SGD)
Brownfield Environment - Tiny	< Up to 20 VMs		
Brownfield Environment - Small	> Up to 50 VMs		
Brownfield Environment - Medium	51VMs - 120 VMs		
Brownfield Environment - Large	121 VMs and Greater		
Green Field Environment -Tiny	< Up to 20 VMs		
Green Field Environment - Small	> Up to 50 VMs		
Green Field Environment Medium	51VMs - 120 VMs		
Green Field Environment - Large	121 VMs and Greater		

b. Managed Service - Monthly (For Each Project)

Dedicated Resources

Service Type	% of Monthly CSP consumption charges of End Customer
Bronze Support	
Silver Support	
Gold Support	

Shared Resources

Service Type	% of Monthly CSP consumption charges of End Customer
Bronze Support	
Silver Support	
Gold Support	

10. FTE Pricing

a. AWS

FTE (Labour) – Onsite

Cloud Specialist	Years of AWS Experience	Daily Rates (SGD$)
AWS Solutions Architect (Associate)	>2	
AWS Developer (Associate)	>2	
AWS SysOps Administrator (Associate)	>2	
AWS Solutions Architect (Professional)	>3	
AWS DevOps Engineer (Professional)	>3	
AWS Advanced Networking (Speciality)	3-5	
AWS Security (Specialty)	3-5	

FTE (Labour) – Offshore

Cloud Specialist	Years of AWS Experience	Daily Rates (SGD$)
AWS Solutions Architect (Associate)	>2	
AWS Developer (Associate)	>2	
AWS SysOps Administrator (Associate)	>2	
AWS Solutions Architect (Professional)	>3	
AWS DevOps Engineer (Professional)	>3	
AWS Advanced Networking (Speciality)	3-5	
AWS Security (Specialty)	3-5	

b. Azure

FTE (Labour) – Onsite

Cloud Specialist	Years of Azure Experience	Daily Rates (SGD$)
Microsoft Certified: Azure Administrator Associate	>2	
Microsoft Certified: Azure Security Engineer Associate	>2	
Microsoft Certified: Data Analyst Associate	>2	
Microsoft Certified: Azure Developer Associate	>2	
Microsoft Certified: Azure Data Engineer Associate	>2	
Microsoft Certified: Azure Solutions Architect Expert	3-5	
Microsoft Certified: DevOps Engineer Expert	3-5	

FTE (Labour) – Offsite

Cloud Specialist	Years of Azure Experience	Daily Rates (SGD$)
Microsoft Certified: Azure Administrator Associate	>2	
Microsoft Certified: Azure Security Engineer Associate	>2	
Microsoft Certified: Data Analyst Associate	>2	
Microsoft Certified: Azure Developer Associate	>2	
Microsoft Certified: Azure Data Engineer Associate	>2	
Microsoft Certified: Azure Solutions Architect Expert	3-5	
Microsoft Certified: DevOps Engineer Expert	3-5	

c. Google Cloud (GCP)

FTE (Labour) – Onsite

Cloud Specialist	Years of GCP Experience	Daily Rates (SGD$)
Google Cloud Certified - Associate Cloud Engineer	>2	
Google Cloud Certified - Professional Cloud Architect	>3	
Google Cloud Certified - Professional Cloud Network Engineer	>3	
Google Cloud Certified - Professional Cloud Security Engineer	>3	
Google Cloud Certified - Professional Cloud Developer	>3	
Google Cloud Certified - Professional Data Engineer	3-5	
Google Cloud Certified - Professional Data Analyst	3-5	

FTE (Labour) – Offsite

Cloud Specialist	Years of GCP Experience	Daily Rates (SGD$)
Google Cloud Certified - Associate Cloud Engineer	>2	
Google Cloud Certified - Professional Cloud Architect	>3	
Google Cloud Certified - Professional Cloud Network Engineer	>3	
Google Cloud Certified - Professional Cloud Security Engineer	>3	
Google Cloud Certified - Professional Cloud Developer	>3	
Google Cloud Certified - Professional Data Engineer	3-5	
Google Cloud Certified - Professional Data Analyst	3-5	

About Singtel

Singtel is Asia's leading communications technology group, providing a portfolio of services from next-generation communication, technology services to infotainment to both consumers and businesses. For consumers, Singtel delivers a complete and integrated suite of services, including mobile, broadband and TV. For businesses, Singtel offers a complementary array of workforce mobility solutions, data hosting, cloud, network infrastructure, analytics and cyber-security capabilities. The Group has presence in Asia, Australia and Africa and reaches over 710 million mobile customers in 21 countries. Its infrastructure and technology services for businesses span 21 countries, with more than 428 direct points of presence in 362 cities.

Awards

Frost & Sullivan 2019 Singapore Cloud Infrastructure
Competitive Strategy, Innovation & Leadership Award

2019 VMware Cloud Partner of the Year, SEA & Korea

Telecom Asia Awards 2018
Best Cloud-based Service Award

Frost & Sullivan Best Practices Award 2018
Asia-Pacific Managed Cloud Services Competitive
Strategy, Innovation & Leadership Award