



ASEAN SECRETARIAT

TERMS OF REFERENCE

Support and Maintenance of the ASEAN Secretariat’s DRP Cloud
Infrastructure and Deployment of On-Premises to Cloud Backup Services

Version 1.0

Version	Date	Status	Author
1	09/07/2025	Final	CAD & ITSD

Table of Contents

1 Background..... 3

2 Objectives..... 3

3 Existing ASEAN Secretariat Cloud Platform..... 4

4 Scope of Services..... 5

5 Service Level Agreement and Penalty..... 7

6 Project Schedule and Delivery..... 7

7 Vendor Qualification and Experience..... 7

Annex 1. Azure Existing Components for ASEC Cloud Platform..... 9

Annex 2. ASEC Server Infrastructure in Azure.....12

Annex 3. ASEC On Premises Server to be backup to Azure Cloud Platform.....13

Annex 4. ASEC On Premises Shared Folder to be migrated and backup to Azure Cloud Platform...14

Terms of Reference

Support and Maintenance of the ASEAN Secretariat's DRP Cloud Infrastructure and Deployment of On-Premises to Cloud Backup Services

I. Background

The ASEAN Secretariat (ASEC) was established in February 1976 by the Foreign Ministers of ASEAN to coordinate and facilitate collaboration among ASEAN Member States and stakeholders. With approximately 450 personnel, ASEC plays a crucial role in driving ASEAN's initiatives as outlined in the ASEAN Charter.

As part of its technology modernization initiatives, ASEC is migrating its servers to Microsoft Azure cloud so that it enhances ASEC IT and network infrastructure, i.e. operational efficiency, security and agility. The transition offers advanced security, robust disaster recovery and failover capability, and scalable resource management. It also reduces the risk of system failures and service disruptions and ensures seamless operations and institutional continuity.

In alignment with this strategy, ASEC has already established its Azure Cloud Platform and completed the migration of several key servers to the cloud. ASEC is now planning to further expand its cloud adoption by implementing a cloud-based backup for its remaining on-premises servers and setup of recovery and failover infrastructure in its Azure Cloud Platform.

II. Objectives

To provide maintenance and support to ASEC's Azure Cloud Platform, but not limited to, configuration and troubleshooting to ensure stability of ASEC Cloud Platform and servers as well as of additional servers to be created or migrated in future into this Platform.

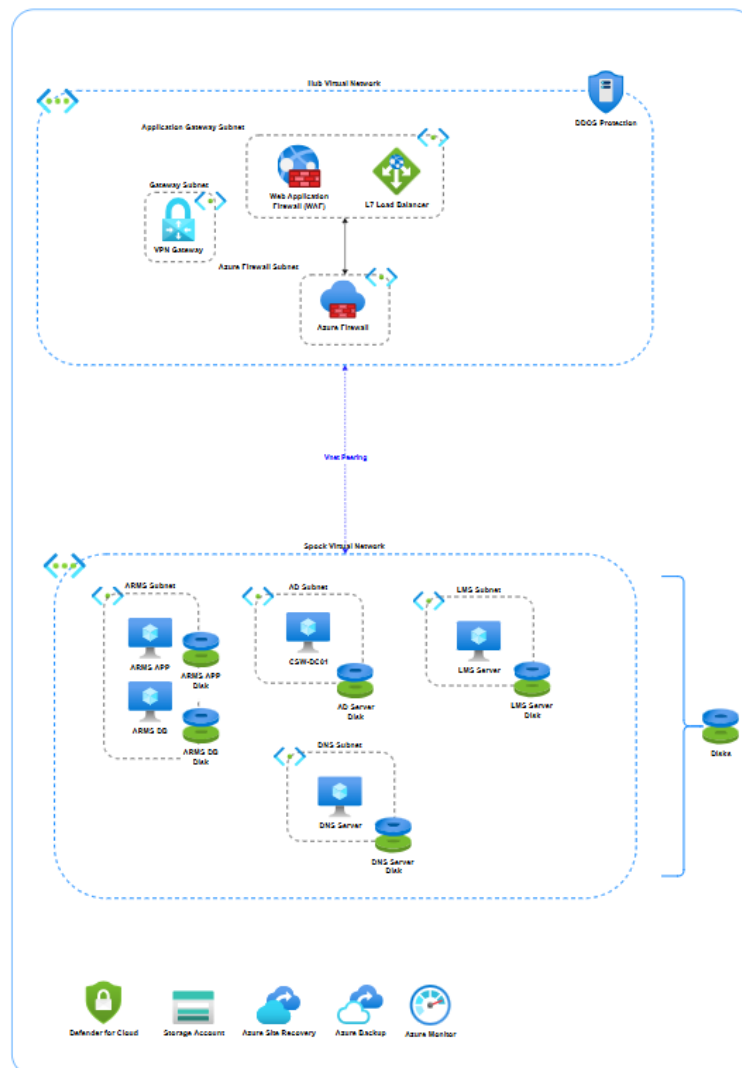
To implement a backup solution for on-premises servers to Azure Cloud Platform, with comprehensive support that includes continuous monitoring, timely troubleshooting, periodic verification of backup integrity and the adoption of best practices for a secure and cost-effective backup.

III. Existing ASEAN Secretariat Cloud Platform

Existing ASEC cloud platform is designed using Hub and Spoke architecture, where the Hub (VLAN Hub) acts as a central point for security while the Spoke (VLAN Main) for workload specific resources.

- VLAN Hub – Security Virtual Networks
 - Azure Firewall Subnet
 - Gateway Subnet (S2S VPN)
 - Application Gateway Subnet
- VLAN Main – Main Virtual Network for Core Services
 - AD-Subnet : Dedicated subnet for Active Directory
 - ARMS-Subnet : Dedicated subnet for ARMS servers
 - LMS-Subnet : Dedicated subnet for LMS servers

Detail Azure resources for VLAN Hub refers to Annexure 1 and for VLAN Main refer to Annexure 2. Below is the network topology of ASEC Azure cloud infrastructure:



IV. Scope of Services

The vendor shall work closely with ITSD Team and follow the overall direction and guidance provided by the Director of Corporate Affairs and/or ASEC Management. The vendor will undertake the following tasks:

1. Managing and maintaining ASEC Azure Platform

- Manage and maintain the Hub and Main virtual network
- Ensure seamless tunnel connection between ASEC Azure infrastructure and ASEC on-premises infrastructure
- Perform configuration needed to support existing servers, new server deployment or to migrate on premise servers to ASEC Azure platform
- Perform review of existing configuration ensuring optimal configuration
- Provide automatic email alert and timely troubleshoot for issues related to ASEC Azure platform

2. Deployment and Maintenance of Azure cloud backup solution for ASEC on-premises servers

- Implement best practice backup strategy in-line with ISO standard (RTO, RPO, backup granularity, retention policies, encryption, etc)
- Configure immutable backup and ZRS (Zone Redundant Storage) for all backup data
- Implement backup at image level, configured with daily incremental backup and feature to do granular restore on file-level or folder-level
- Backup should be implemented with recovery points as follows: daily recovery points for the past 7 days, weekly recovery points for the past 4 weeks and monthly recovery points for the past 6 months
- Perform and document periodic restore testing (2x per year) to ensure backup integrity
- Perform configuration support and on-demand restore support as and when needed
- Reviewing and troubleshoot error codes in logs
- Perform regular update of backup agents
- Daily monitoring of backup jobs, configure and provide automated email alert and perform timely troubleshooting
- Produce documentation on all configuration
- Provide monthly report on backup status and resources usage monitoring

3. Maintenance of all servers in Azure Cloud Platform

- Provide maintenance and support for all the servers
- Configure immutable backup, Standard SSD for storage, ZRS (Zone Redundant Storage) and ASR (Azure Site Recovery to East Asia Region) for server resources, backup and failover
- Implement backup at image level, configured with daily incremental backup and feature to do granular restore on file-level or folder-level

- Backup should be implemented with recovery points as follows: daily recovery points for the past 7 days, weekly recovery points for the past 4 weeks and monthly recovery points for the past 6 months
 - Perform investigation and troubleshoot all server infrastructure related issues
 - Daily monitoring of server backup jobs, configure and provide automated email alert and perform timely troubleshooting
 - Perform and document periodic restore testing and site recovery test failover (2x per year)
 - Provide monthly report on server health (CPU, Memory, Disk usage, Uptime, Backup Status, etc)
4. Migration of on-premises Shared folders to Azure Cloud Platform
- Configure user access permissions to replicate existing user access permission
 - Provide maintenance and support for the shared folder
 - Configure immutable backup, Standard SSD for storage, ZRS (Zone Redundant Storage) and ASR (Azure Site Recovery to East Asia Region) for server resources, backup and failover
 - Implement backup at image level, configured with daily incremental backup and feature to do granular restore on file-level or folder-level
 - Backup should be implemented with recovery points as follows: daily recovery points for the past 7 days, weekly recovery points for the past 4 weeks and monthly recovery points for the past 6 months
 - Perform and document periodic restore testing (2x per year) to ensure backup integrity
 - Perform configuration support and on-demand restore support as and when needed
 - Daily monitoring of backup jobs, configure and provide automated email alert and perform timely troubleshooting
 - Provide monthly report on backup status and resources usage monitoring
5. Leveraging best practices
- Prior to carrying out this assignment, the to-be-selected vendor is expected to review and analyze the requirements outlined in this TOR. Based on the expertise and industry's best practices, the vendor is encouraged to propose alternative approaches or solutions, where appropriate, that may offer enhanced performance, reliability, and cost-efficiency. Any proposed alternatives should be accompanied by technical justifications for ASEC's consideration
6. Disaster Recovery
- In the event of a major disaster impacting the Azure Southeast Asia region where the ASEC cloud platform is currently hosted, the vendor shall be fully responsible for establishing an equivalent cloud infrastructure in the Azure East Asia region within three (3) working days or an agreed duration with ASEC from the date of the incident.

7. Provide annual support and maintenance service for a contract period of 36 months. The scope of support and maintenance should cover all necessary software license required to perform the service as detailed in Scope of Service and subscription of Azure resources as detailed in Annex. 1 , Annex. 2, Annex. 3 and Annex. 4 including further expansion up to a maximum of 10 servers to be hosted in Azure and up to 25 on-premises servers to be backup to Azure. Any additional Azure resources beyond those specified in the annexes and the stated limits will be subject to separate charges, to be provided separately in the proposal.

V. Service Level Agreement & Penalty

SLA Category	Description	Response Time	Resolution Time	Measurement Window	Penalty
1. Critical (P1)	- Complete service outage due to failure in Azure infrastructure (e.g. firewall down, routing failure between Hub & Spoke, etc) - Backup services are not running for more than 3 consecutive days	1 hour	6 hours	24/7	0.015% of the annual support and maintenance fee for each hour beyond the SLA resolution time, capped at a maximum of 10% of the annual fee per year
2. High (P2)	- Major performance degradation impacting operation (e.g. one spoke virtual network is inaccessible, etc) - Backup services are not running for more than 1 days but less than 3 days	4 hour	12 hours	24/7	
3. Medium (P3)	Minor performance degradation (e.g. VM performance degradation, resource misconfiguration not impacting operation, etc)	8 hours	2 working days	9:00 AM - 5:00 PM (Business Hours)	
4. Low (P4)	Cosmetic issues (e.g. report formatting, etc) or requests for information that do not impact system functionality.	24 hours	5 working days	9:00 AM - 5:00 PM (Business Hours)	-

VI. Project Schedule and Delivery

The vendor shall ensure that all activities outlined in this Terms of Reference (TOR), including the provisioning, configuration, and implementation of the required services, are fully completed and accepted by The ASEAN Secretariat no later than 31 December 2025.

In the event that the vendor fails to complete the project by the stipulated deadline, a penalty of 0.5% of the annual support and maintenance fee shall be imposed for each calendar day of delay, up to a maximum of 10% of the annual support and maintenance fee. The ASEAN Secretariat reserves the right to deduct the penalty amount from any payments due to the vendor.

VII. Vendor Qualification and Experience

The vendor should provide a team of qualified consultants that meet the following requirements:

- a. Proven experience in designing, implementing and maintaining Hub and Spoke Architecture in Azure
- b. Proven experience with Azure-native backup tools such as Azure Backup, Recovery Services Vault, Azure Site Recovery, and immutable backup configuration.
- c. At least 3 successful projects involving implementation of Azure cloud Architecture, migration of servers to Azure and backup of on premises servers to Azure
- d. At least 5 years of experience working with international organisations, multinational corporations, or regional organisations similar to ASEAN Secretariat;
- e. Among the Support Team, its core member/s must at least be equipped with the following:
 - A minimum of 5 years of experience working with Microsoft Azure Infrastructure,
 - Certified Azure Administrator Associate,
 - Certified Azure Solutions Architect Expert,
 - Certified Azure Security Engineer Associate,
 - Certified Azure Network Engineer Associate.
- f. Authorised Letter/Partner and/or support of software solution/platform to be supplied
- g. All experts assigned for this project shall have good written and verbal English communication skills.
- h. Leadership; Strong leadership and inter-personal skills including excellent communication, facilitation and training skills are required

ANNEX 1 – Azure Existing Component for ASEC Cloud Platform

No.	Service Category	Service Type	Custom Name	Region	Description
01	Networking	Azure Firewall	Core Network - Firewall	Southeast Asia	Standard tier, 1 Logical firewall units x 730 Hours, 1 TB Data processed
02	Networking	Application Gateway	Core Network - Application Gateway	Southeast Asia	Web Application Firewall V2 tier, 730 Fixed gateway Hours, 2 compute units and 10,000 persistent connections with 20 mb/s throughput, 1 TB Data transfer
03	Networking	VPN Gateway	Core Network - VPN Gateway	Southeast Asia	VPN Gateways, VpnGw2 tier, 730 gateway hour(s), 0 additional S2S tunnels (beyond included amount), 0 additional P2S connections (beyond included amount), 0 GB, VPN VPN gateway type
04	Networking	IP Addresses	Core Network - Static IPs	Southeast Asia	Global (ARM), 50 Static IP Addresses X 730 Hours, 0 Public IP Prefixes X 730 Hours
05	Security	Microsoft Defender for Cloud	Security - Microsoft Defender for Cloud	Southeast Asia	Microsoft Defender for Cloud Workload Protection: 0 Plan 1 servers x 730 Hours, 60 Plan 2 servers x 730 Hours, 0 Container vCores x 730 Hours, 0 additional container image scans, 0 App Service nodes x 730 Hours, 0 SQL Database servers on Azure, 0 SQL Database servers outside Azure x 730 Hours, 0 MySQL Instances, 0 PostgreSQL Instances, 0 MariaDB Instances x 730 Hours, Cosmos DB 0 x100 RU/s x 730 Hours, 2 Storage

					accounts x 730 Hours with 0 million total coverage of transactions across each storage account and 0 GB storage scanned for malware, Defender for APIs – Plan 1 with 0 estimated API monthly transactions, 1 Key Vault(s), 0 Subscription(s)
06	Networking	Azure DDoS Protection	Security DDoS Protection	Southeast Asia	IP Protection, Protection for 2 resources x 730 Hours
07	Networking	Bandwidth	Bandwidth	Southeast Asia	Internet egress, 2072 GB outbound data transfer from Southeast Asia routed via Public Internet
08	Networking	Azure DNS	DNS	Southeast Asia	Zone 1, DNS, Public; 5 hosted DNS zones, 50 DNS queries
09	Networking	Traffic Manager	Traffic Manager	Southeast Asia	50 million DNS queries/mo, 10 Azure endpoint(s), 10 Fast Azure endpoint(s), 0 External endpoint(s), 0 Fast External endpoint(s), 50 million(s) of user measurements, 0 million(s) of data points processed.
10	Networking	Load Balancer	Load Balancer	Southeast Asia	Standard Tier: 20 Rules, 2,000 GB Data Processed

ANNEX 2 – ASEC Server Infrastructure in Azure

No	System Description	Specification		Operating System
		VM (Region: South East Asia)	Azure Backup and Site Recovery (Region: East Asia)	
1	Public DNS	1 B4als v2 (4 vCPUs, 8 GB RAM) x 730 Hours (Pay as you go), Linux, (Pay as you go); 1 managed disk – E6; Internet egress, 5 GB outbound data transfer from Southeast Asia routed via Public Internet	Azure VMs, Standard Backup policy, 1 Instance(s) x 64 GB, LRS Redundancy, Low Average Daily Churn, 93 GB Average monthly backup data in Standard Tier, 0 GB Average monthly backup data in Archive Tier	RedHat
2	Active Directory	1 B4als v2 (4 vCPUs, 8 GB RAM) x 730 Hours (Pay as you go), Windows (License included), OS Only; 1 managed disk – E10; Internet egress, 5 GB outbound data transfer from Southeast Asia routed via Public Internet	Azure VMs, Standard Backup policy, 1 Instance(s) x 128 GB, LRS Redundancy, Low Average Daily Churn, 187 GB Average monthly backup data in Standard Tier, 0 GB Average monthly backup data in Archive Tier	Windows Server 2022
3	ARMS Application Server	1 B2als v2 (2 vCPUs, 4 GB RAM) x 730 Hours (Pay as you go), Linux, (Pay as you go); 1 managed disk – E10; Internet egress, 5 GB outbound data transfer from Southeast Asia routed via Public Internet	Azure VMs, Standard Backup policy, 1 Instance(s) x 128 GB, LRS Redundancy, Low Average Daily Churn, 187 GB Average monthly backup data in Standard Tier, 0 GB Average monthly backup data in Archive Tier	Linux (ubuntu 22.04)
4	ARMS Database Server	1 B2als v2 (2 vCPUs, 4 GB RAM) x 730 Hours (Pay as you go), Linux, (Pay as you go); 1 managed disk – E10; Internet egress, 5 GB outbound data transfer from Southeast Asia routed via Public Internet	Azure VMs, Standard Backup policy, 1 Instance(s) x 128 GB, LRS Redundancy, Low Average Daily Churn, 187 GB Average monthly backup data in Standard Tier, 0 GB Average monthly backup data in Archive Tier	Linux (ubuntu 22.04)
5	LMS Application Server	1 B4as v2 (4 vCPUs, 16 GB RAM) x 730 Hours (Pay as you go), Windows (License included), OS Only; 1 managed disk – E10; Internet egress, 5 GB outbound data transfer from Southeast Asia routed via Public Internet.	Azure VMs, Standard Backup policy, 1 Instance(s) x 128 GB, LRS Redundancy, Moderate Average Daily Churn, 243 GB Average monthly backup data in Standard Tier, 0 GB Average monthly backup data in Archive Tier	Windows Server 2022

ANNEX 3 – ASEC On Premises Server to be backup to Azure Cloud Platform

No	On Premise Server				Project Scope **
	System Name	Specification *	Operating System *	Disk Size (GB)	
1	ASEAN-MASSDB-01	vCPU 8, RAM 18	Windows Server 2016 Std	50	Backup to cloud
2	ASEAN-FINAPP-02	vCPU 6, RAM 16	Windows Server 2016 Std	150	Backup to cloud
3	ASEAN-FINDB-02	vCPU 6, RAM 32	Windows Server 2016 Std	100	Backup to cloud
4	SW-ERPDCS01	vCPU 5, RAM 10	Windows Server 2019 Std	50	Backup to cloud
5	SW-ELACCESS-01	vCPU 8, RAM 8	Windows Server 2019 Std	100	Backup to cloud
6	SW_PABX01	vCPU 3, RAM 6	Windows Server 2019 Std	150	Backup to cloud
7	LS-HRAC01	vCPU 7, RAM 8	Redhat Enterprise 9	50	Backup to cloud
8	SW-EPASS-01	vCPU 4, RAM 16	Windows Server 2019 Std	50	Backup to cloud
9	SW-EPMC01	vCPU 5, RAM 12	Windows Server 2019 Std	100	Backup to cloud
10	SW-FINGER01	vCPU 4, RAM 6	Windows 11	100	Backup to cloud
11	SW-DC08	CPU Dual Proc @8Cores RAM 16 (Physical)	Windows Server 2016 Std	350	Backup to cloud
12	KDMS - Cluster MSSQL DB				
	- ASEAN-DMSDB-01	vCPU 2, RAM 32	Windows Server 2019 Std	900	Backup to cloud
	- ASEAN-DMSDB-02	vCPU 2, RAM 32	Windows Server 2019 Std		Backup to cloud
13	KDMS Enadoc Data	vCPU 2, RAM 192	Windows Server 2019 Std	250	Backup to cloud
14	ERP MSSQL DB				
	-SW-SQLP01	vCPU 8, RAM 32	Windows Server 2019 Std	800	Backup to cloud
	-SW-SQLP02	vCPU 8, RAM 32	Windows Server 2019 Std		Backup to cloud
Total Storage needed in Azure for backup				3200	

* On-premises server specifications are provided here for reference purposes only and are not intended for provisioning under the Azure subscription

** Backup to be performed at image-level to allow full system restoration, including Operating System, Applications, and Databases

ANNEX 4 – ASEC On Premises Shared Folder to be migrated and backup to Azure Cloud Platform

No	On Premise Server				Project Scope
	System Name	Specification *	Operating System *	Disk Size (GB)	
1	SW-DOC01	vCPU 3, RAM 6	Windows Server 2019 Std	900	Shared folder for migration to Azure and cloud backup
2	ASEAN-SUNDB-03	CPU Dual Proc @8Cores RAM 32 (Physical)	Windows Server 2016 Data Center	3550	Shared folder for migration to Azure and cloud backup
Total Storage needed in Azure for Shared folder				4450	

* On-premises server specifications are provided here for reference purposes only and are not intended for provisioning under the Azure subscription

Summary of Azure resources required to be subscribed by vendor to host the Shared Folders:

System Name	CPU	Memory	Operating System	Disk Storage (GB)
SW-DOC01	6 core	12 GB	Windows Server 2022 Standard	900
ASEAN-SUNDB-03	10 core	16 GB	Windows Server 2022 Standard	3550