



ASEAN SECRETARIAT

Terms of Reference

***Renewal and Maintenance Support of IT Disaster
Recovery Plan (DRP) System and Services***

Table of Contents

1	Background.....	2
2	Objectives.....	2
3	Expected Deliverables	3
4	Scope of Services	3
5	Indicative Work Schedule.....	4
6	Vendor Qualifications, Knowledge, and Experiences	5
7	Expected Backup and Replication Strategy	5
8	Expected Recovery Strategy	6
9	Preventive and Corrective Maintenance.....	6
10	Contract Period and Service Fee	6

Term of Reference for the Renewal and Maintenance Support of IT Disaster Recovery Plan (DRP)

1 Background

The ASEAN Secretariat (ASEC) was established in February 1976 by the Foreign Ministers of ASEAN. Currently staffed with approximately 430 people, the mission of ASEC is to initiate, facilitate and coordinate ASEAN stakeholder collaboration in realizing the purposes and principles of ASEAN as reflected in the ASEAN Charter. In order to effectively fulfil its function in providing greater efficiency in the coordination of ASEAN organs and implementation of ASEAN Programs and Projects, ASEC needs to be equipped with sufficient up-to-date technology and proper disaster recovery plan (DRP).

Having DRP in place will ensure recovery of its data/information in the event of a disaster. Therefore, ASEC has established its DRP in 2020 with 37 Client Agents/Licenses. ASEC's existing DRP system¹ is set up in two locations:

- a. On-premises Location (at ASEC)**
- b. Off-site Location (outside of Indonesia within ASEAN Region)**

2 Objectives

ASEC is seeking a qualified vendor to provide a more better DRP solution or maintain the current one to backup ASEC's corporate data/documents locally and to a secure remote replication off-site. Currently, the ASEC has an existing backup software and ASEC's secure remote replication site is outside of Indonesia, i.e., in another ASEAN country. The vendor may maintain the existing software and site or provide a better/recommended solution whichever solution² is the most efficient. The solution for the remote replication shall have a storage capacity of at least 40TB and is expandable to accommodate future need for additional storage capacity.

¹ Details of the existing system/software will be provided to interested vendors - refer *ASEC Request for Proposal (RFP)*.

² The most efficient solution is a secure solution with a reasonable cost and in-line with recommended international standards e.g., ISO, etc.

The selected vendor shall be tasked to achieve the following objectives:

1. To ensure that any proposed solution is compatible with ASEC's hardware and that all data/documents at ASEC premises are safely replicated to the remote site;
2. To implement a new remote replication solution to enhance data/document protection and disaster recovery;
3. To migrate the existing data/documents, totalling to approximately 30TB, to a new secure replication site;
4. To provide the uplink/downlink bandwidth at least 50Mbps or as per recommendation;
5. Ensure the proposed solution able to cater storage capacity of at least 40TB with expandable options for additional storage capacity in the future.

3 Expected Deliverables

The expected deliverables include:

1. Provision of necessary hardware and software which are scalable and compatible with ASEC existing hardware;
2. Maintenance and support of the backup solution with the existing on-premises hardware and software and DRP solution on 24/7 basis during the contract period with ASEC;
3. Preparing reports which include daily/weekly/yearly technical activity, incident report, etc.;
4. Provision of necessary licenses for the proposed backup and replication solution;
5. Provision 25% increase of storage capacity annually during the contract period;
6. 24-hour monitoring of DRP system (hardware and software) for both of on-premises and remote site to prevent downtime;
7. Provision of technical guidelines/manual and other training to ASEC IT, if necessary.

4 Scope of Services

The vendor shall work closely with the ITSD team and follow the overall direction and guidance provided by the Director of Corporate Affairs and/or ASEC Management. In order to achieve the above objectives and expected deliverables, the selected vendor will undertake the following:

- 1) Technical approach, outlining the proposed solution architecture and methodology;

- 2) Implementation plan including timelines, resource allocation, and milestones to be achieved;
- 3) Data migration strategy and ensuring minimal disruption to ongoing operations;
- 4) Assessment of the existing backup infrastructure and proposing a suitable remote replication solution;
- 5) Design and implementation of the remote replication solution with the ASEC existing hardware;
- 6) Migrating the existing data/documents to the new replication site, ensuring data integrity and minimal downtime;
- 7) Configuration and optimization of the new infrastructure for efficient backup and replication operations;
- 8) Conducting thorough testing and verification to ensure the reliability and effectiveness of the solution (backup and restoration completion report);
- 9) Documenting the implemented solution, including configuration details, procedures, and best practices;
- 10) Knowledge transfer and training to the ASEC IT staffs on managing and maintaining the new DRP solution;
- 11) Configuration of scheduled backup and setting to enable backup to Disk, duplication to tape and remote site through a secured link;
- 12) Reconfiguration when there is any additional new component (hardware and software) or any additional configuration required;
- 13) Performing hardware and software patches including firmware to prevent incompatibility, vulnerability, and stability in accordance with the official recommendation of the software or hardware manufacturer;
- 14) Specifying clearly any involvement or expectation of ASEC IT team to work in the vendor's team in undertaking this project, if any.

5 Indicative Work Schedule

The selected vendor is requested to provide a clear methodology and approach in carrying out this assignment. This includes demonstrating relevant knowledge and skills warranting that the team will be executed this project within a planned timeframe.

6 Vendor Qualifications, Knowledge, and Experiences

The to-be-selected Vendor shall meet the following criteria:

- 1) An established company with a business registration and a proven record in provision of DRP/replication solutions, or similar systems for multi-national companies, governmental agencies, or international organizations;
- 2) Provide at least five (5) customer references/testimonials who have acquired DRP/replication solutions and/or implementation of backup solutions in the past 5 years;
- 3) Authorised business partner and/or supporting letter (surduk) of a software and/or hardware which the vendor will be implemented for ASEC;
- 4) Able to provide assurance, trust and non-disclosure agreement to protect and secure the DRP system and its contents;
- 5) Have the ability and infrastructure to provide adequate application support including helpdesk 24/7 and on-site field support as necessary;
- 6) Have certified support engineer team in proposed backup software linux Redhat , Firewall, Network routing/switching, SAN/NAS storage and Server;
- 7) All personnel assigned for this project shall have good communications in English, both written and verbal communications;
- 8) The selected company and all personnel assigned for this project shall agree to sign a Non-Disclosure Agreement (NDA) to abide to the rules, regulation and ethical to ensure to protect the ASEC's confidentiality of all ASEC information.

7 Expected Backup and Replication Strategy

All required vital data (file level and/or image level) from both Physical and Virtual system in the ASEC Server room will be backed up to on-premises' backup server/storage and duplicate to tape backup media and replicate to remote site. The backup operation will be verified and validated to ensure the backed up vital data/records can be read and restored before replicated to remote site through a secured site to site VPN link with encryption engine of at least 256-bit AES encryption standard. The vital data shall be backed up accordingly to the required scheduling.

8 Expected Recovery Strategy

- a. Recovery Testing for Data/File must be undertaken every quarterly period (3 months) to ensure that the vital records are validated and verified for recovery in case of an emergency or disaster situation.
- b. In the event of any natural or man-made failure/disaster of data/file level occurrence, the authorised ITSD staff(s) will perform the initial Data/File Recovery from on premises DRP System at ASEC premises. If the initial Data/File Recovery from on premises is unsuccessful, then will perform a restoration process directly from Remote site.
- c. Vendor should perform restoration services from Remote site not longer than 30 minutes once the vendor received ASEC's restoration request form through email or other support services provided by the vendor.
- d. Restoration processes should be well documented/recorded and to be provided to ASEC after the restoration is done.
- e. A penalty will be carried out on the vendor if the vendor is unable to perform or restore the requested Data/File within the agreed SLA. The penalties will be agreed with the vendor before confirming the project acceptance, and it will be reflected in the Special Services Agreement (SSA).

9 Preventive and Corrective Maintenance

During the contract period, the preventive and corrective maintenance shall be performed **without any additional cost to ASEC**. It shall cover, but not limited, to the following:

- (i) Maintenance, updating, patching, replacement, remedying, or otherwise resolve any problem on the DRP system, its hardware and remote storage platform;
- (ii) Ad-hoc technical support on 24/7 basis. Response shall be within three (3) hours to ASEC's request;
- (iii) Provide corrective maintenance support at least twice (2x) per month and shall be performed by authorised software support engineer(s).

10 Contract Period and Service Fee

The contract period is for 36 months, but ASEC will pay the service fee on a yearly basis.

***TERMS OF REFERENCE – Renewal and Maintenance Support of IT Disaster Recovery Plan (DRP)
System and Services***

Vendor shall quote the service fee for 3 years. This service fee remains no change for 3 years.

Vendor shall also quote the rate for storage capacity for remote site in Terabyte basis and this rate shall remain no change during the contract period. In case additional storage is needed, ASEC will buy accordingly.