KERANGKA ACUAN KERJA
PENGADAAN Managed Service VMware, Veritas, Veeam

PT. KLIRING BERJANGKA INDONESIA
Menara Danareksa Lantai 6
Jl. Medan Merdeka Selatan No 14, Jakarta Pusat 10110 2026

Daftar Isi

1. PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Maksud dan Tujuan 1
1.3 Sasaran 2
2. LINGKUP PEKERJAAN 2
2.1. Managed Service VMware Virtualization 2
2.2. Managed Service Veritas 4
2.3. Managed Service Veeam Replikasi Data 5
2.4. Pemeliharaan Preventif (*Preventive Maintenance*) 6
2.5. Transfer Knowledge & Workshop Teknis 6
2.6. Dokumentasi Vmware, Veritas, Veeam 7
3. SPESIFIKASI TEKNIS 7
3.1 Spesifikasi Umum & Ketersediaan Layanan 7
3.2 Metode Kerja 7
3.3 Spesifikasi Teknis VMware 8
3.4 Spesifikasi Teknis Tape Veritas 9
3.5 Spesifikasi Teknis Backup Replikasi Veeam 10
4. DELIVERABLES 11
5. JANGKA WAKTU PELAKSANAAN 12
6. KRITERIA DAN Nilai Tambah VENDOR 13
6.1. Kualifikasi Kemitraan Resmi dengan Prinsipal Teknologi 13
6.2. Pengalaman Perusahaan 13
6.3. Dokumen Persyaratan yang Harus Dilampirkan 13
7. *SERVICE LEVEL AGREEMENT (SLA)* 13
7.1. Tingkat Keparahan Insiden (*Severity Level*) 13
7.2. Jam Layanan dan Saluran Dukungan 14
7.3. Target Waktu Respons dan Penyelesaian Insiden 15
7.4. Target RPO dan RTO 15
8. TIMELINE PROSES PENGADAAN ..... **Error! Bookmark not defined.**
9. KOMPOSISI PENILAIAN 16
10. PENUTUP 18

DOCUMENT VERSION

Versi	Tanggal	Bagian	Jenis Perubahan	Penulis Perubahan
1.0	20 – 7 – 2026	All	Pembuatan Document	Krisna
1.1	01-10-2026	Timeline dan Termin Pembayaran	Pembuatan Timeline Proses Pengadaan dan Termin Pembayaran	Rangga

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan sistem informasi dan digitalisasi layanan di lingkungan PT. Kliring Berjangka Indonesia menuntut ketersediaan (*High Availability*), integritas, dan keamanan infrastruktur TI yang beroperasi secara non-stop (24/7/365). Infrastruktur komputasi inti saat ini bertumpu pada arsitektur virtualisasi berbasis VMware vSphere Enterprise, proteksi data dan backup enterprise menggunakan Veritas NetBackup/Backup Exec yang mengintegrasikan backup Virtual Machine serta archive jangka panjang pada media *Tape Library/Drive*, serta mekanisme *Disaster Recovery* (DR) berbasis replikasi virtual machine (*VM Replication*) menggunakan Veeam Backup & Replication yang menghubungkan *Data Center* (DC) Utama ke *Disaster Recovery Center* (DRC).

Mengingat tingginya beban kerja operasional, ketergantungan bisnis pada kontinuitas sistem, serta ancaman siber dan potensi gangguan bencana, pengelolaan infrastruktur tersebut menghadapi sejumlah tantangan strategis:

1. **Virtualisasi VMware**

   Kebutuhan pemeliharaan berkala terhadap *host* ESXi, kluster vCenter, *distributed switch*, *datastores*, serta kepatuhan *patching firmware* untuk memitigasi kerentanan keamanan.

2. **Data Protection Veritas (VM & Tape Backup)**

   Kebutuhan siklus backup VM harian, mingguan, dan bulanan, serta kepatuhan standar archive menggunakan media fisik *Tape Cartridge* guna memastikan ketersediaan data historis dan keamanan data backup.

3. **Veeam Backup Replication**

   Kebutuhan monitoring sinkronisasi *continuous/scheduled replication* dari DC ke DRC, serta mitigasi gangguan bandwidth jaringan, pengelolaan *snapshot/restore points*, serta validasi skenario DRC DRILL.

Keterbatasan kapasitas sumber daya manusia (SDM) internal baik dari sisi kuantitas menjadi alasan dibutuhkannya bantuan support layanan vmware, veritas, dan veeam.

1.2 Maksud dan Tujuan

1.2.1. Maksud

Maksud dari pengadaan ini adalah menunjuk Penyedia Jasa (*Managed Service Provider*) yang kompeten, kredibel, dan berpengalaman untuk melaksanakan pengelolaan, pemeliharaan preventif, pemantauan proaktif, penanganan insiden, serta pendampingan operasional secara menyeluruh terhadap seluruh komponen VMware, Veritas, dan Veeam pada lingkungan DC dan DRC.

1.2.2. Tujuan

- **High Availability**, memastikan seluruh kluster VMware vSphere, vCenter, ESXi Host, storage datastore, dan jaringan virtual beroperasi dengan stabilitas maksimal dan uptime tinggi.
- **Integrity Data**, memastikan seluruh aturan backup job harian, mingguan, bulanan, dan tahunan berjalan 100% sukses tanpa data loss, serta validasi fisik Tape Cartridge dapat dibaca dan dipulihkan (recoverable) setiap saat.
- **Replicate recovery**, memastikan proses replikasi VM dari DC Utama ke DRC berjalan secara kontinu dengan sync delay minimum, serta menjamin seluruh SOP Failover dan Failback siap dieksekusi secara nyata saat terjadi kondisi darurat.
- **Peningkatan Keamanan dan Hardening**, menerapkan best practices konfigurasi, patch management, vulnerability management, dan proteksi data.
- **Pengembangan Kompetensi Internal**, memberikan transfer of knowledge, pelatihan teknis resmi, dan pendampingan operasional secara berkala kepada staf Divisi Teknologi Informasi PT KBI.

1.3 Sasaran

Sasaran terukur yang hendak dicapai melalui pengadaan jasa ini adalah:

- Tingkat Ketersediaan Sistem (Uptime): Tercapainya ketersediaan layanan virtualisasi VMware minimal 99.9% per bulan.
- Keberhasilan Backup Veritas: *Success rate* pekerjaan backup VM harian/mingguan/bulanan minimal 99.5%.
- Ketercapaian Metrik Replikasi Veeam (DC-DRC):
  - RPO (Recovery Point Objective): ≤ 15 - 30 Menit untuk VM kategori *Mission-Critical*.
  - RTO (Recovery Time Objective): ≤ 1 Jam pada saat skenario *Failover* ke DRC diaktifkan.
- Kesiapan Audit dan Dokumentasi: Tersedianya dokumen topologi HLD/LLD, inventaris aset, dan log pemeliharaan yang terbarui (*up-to-date*) dan siap audit setiap saat.

2. LINGKUP PEKERJAAN

Penyedia Jasa wajib menyediakan layanan pengelolaan sistem secara menyeluruh, yang meliputi pemantauan sistem, pengelolaan dan pemeliharaan, penanganan gangguan, simulasi kebencanaan, serta pemberian pengetahuan kepada tim terkait, dengan rincian sebagai berikut:

2.1. Managed Service VMware Virtualization

Penyedia Jasa wajib melakukan pengelolaan dan pemeliharaan lingkungan VMware Virtualization secara menyeluruh untuk memastikan sistem berjalan stabil, aman, dan optimal, dengan cakupan sebagai berikut:

1. **Pemantauan Sistem 24/7/365**

a. Melakukan pemantauan secara *real-time* terhadap penggunaan CPU, Memory, Storage, dan Network pada seluruh Host ESXi dan vCenter Server.
b. Melakukan deteksi dan pemberitahuan dini apabila terjadi gangguan, seperti Host ESXi terputus, gangguan koneksi ke Storage, atau penggunaan sumber daya yang terlalu tinggi.
c. Melakukan pemantauan kondisi sistem untuk mencegah terjadinya gangguan yang dapat memengaruhi layanan.

2. **Pengelolaan dan Optimalisasi Sistem**
   a. Mengelola dan mengoptimalkan fitur VMware seperti *High Availability* (HA), *Distributed Resource Scheduler* (DRS), *Enhanced vMotion Compatibility* (EVC), dan *Storage DRS*.
   b. Mengelola jaringan virtual, termasuk *Virtual Switch*, VLAN, konfigurasi jaringan, dan mekanisme *failover*.
   c. Mengelola Storage VMware, termasuk penyediaan *Datastore*, pengaturan jalur koneksi (*multipathing*), serta pemantauan kapasitas Storage yang tersedia.
3. **Pemeliharaan, Pembaruan, dan Keamanan**
   a. Melakukan pemeriksaan, perencanaan, dan penerapan *patch* atau pembaruan pada vCenter Server dan ESXi Host secara berkala.
   b. Pelaksanaan pembaruan dilakukan dengan memperhatikan keberlangsungan layanan produksi sehingga gangguan terhadap layanan dapat diminimalkan.
   c. Menerapkan konfigurasi keamanan sesuai dengan standar *VMware Security Configuration Guide* pada seluruh Host ESXi dan perangkat terkait.
4. **Perencanaan Kapasitas dan Peningkatan Kinerja**
   a. Melakukan evaluasi penggunaan CPU, Memory, Storage, dan sumber daya virtual secara berkala.
   b. Menyesuaikan alokasi sumber daya seperti vCPU, vRAM, dan kapasitas Virtual Disk sesuai dengan kebutuhan sistem.
   c. Melakukan tindakan perbaikan apabila ditemukan penggunaan sumber daya yang terlalu tinggi atau kondisi yang dapat menyebabkan penurunan kinerja sistem.

2.2. Managed Service Veritas

Penyedia Jasa wajib melakukan pengelolaan dan pemeliharaan sistem backup Veritas dan media tape secara menyeluruh untuk memastikan data perusahaan terlindungi dan dapat dipulihkan apabila terjadi gangguan atau kehilangan data, dengan cakupan sebagai berikut:

1. **Pengelolaan Kebijakan Backup**
   - Mengatur dan mengoptimalkan jadwal backup harian, mingguan, dan bulanan untuk seluruh VM dan database sesuai dengan kebutuhan perusahaan.
   - Melakukan proses backup pada lingkungan VMware menggunakan *VMware vStorage APIs for Data Protection* (VADP) dengan memperhatikan kinerja server produksi.
   - Melakukan pemantauan kapasitas dan penggunaan media penyimpanan backup agar kapasitas tersedia dan dapat digunakan secara optimal.
2. **Pemeliharaan Server dan Data Backup**
   - Melakukan pemeliharaan rutin pada *Master Server*, *Media Server*, dan *Backup Agent*.
   - Memastikan data dan katalog backup tetap dalam kondisi baik sehingga informasi mengenai backup dapat digunakan saat proses pemulihan data.
   - Melakukan pemeriksaan dan pemeliharaan katalog backup secara berkala untuk mengurangi risiko kegagalan saat proses *restore*.
3. **Pengelolaan Media Tape**
   - Melakukan pemantauan kondisi *Tape Library*, termasuk status robot, *tape drive*, slot penyimpanan, dan kebutuhan pembersihan *tape drive*.
   - Mengatur penggunaan dan pergantian kaset tape berdasarkan jadwal penyimpanan harian, mingguan, bulanan, dan tahunan sesuai dengan skema GFS (*Grandfather-Father-Son*).
   - Memantau proses pemindahan atau penyalinan data backup dari media disk ke kaset tape (*Disk-to-Disk-to-Tape/D2D2T*).
   - Mengelola kaset tape, termasuk pelabelan, pencatatan, penyimpanan di lokasi berbeda (*offsite*) atau lokasi yang terisolasi (*air-gapped*), serta penerapan perlindungan terhadap perubahan atau penghapusan data (*Write-Protect/WORM*).
4. **Uji Pemulihan Data dari Tape**
   - Melakukan uji pemulihan data (*Restore Test*) dari kaset tape secara berkala, minimal 1 (satu) kali setiap bulan.
   - Memastikan kaset tape dapat dibaca dan data yang tersimpan dapat dipulihkan dengan baik.
   - Mendokumentasikan hasil uji *restore* sebagai bukti bahwa data backup pada kaset tape dapat digunakan ketika diperlukan.

2.3. Managed Service Veeam Replikasi Data

Penyedia Jasa wajib mengelola proses replikasi data dan VM dari Data Center (DC) Utama ke Disaster Recovery Center (DRC) untuk memastikan layanan dan data tetap tersedia apabila terjadi gangguan pada DC Utama, dengan cakupan sebagai berikut:

1. **Pengelolaan dan Penjadwalan Replikasi VM**
   a. Melakukan konfigurasi, pemeliharaan, dan pengaturan jadwal replikasi VM dari DC Utama **Cimanggis** ke DRC **BSD**.
   b. Mengoptimalkan penggunaan sumber daya Veeam seperti *Backup Proxy*, *WAN Accelerator*, dan penyimpanan data pendukung proses replikasi.
   c. Mengatur jumlah dan masa penyimpanan *Restore Point* pada VM yang direplikasi di DRC sesuai dengan kebutuhan perusahaan.
   d. Memastikan proses replikasi berjalan sesuai jadwal dan data pada VM di DRC tetap dalam kondisi siap digunakan.
2. **Pemantauan Jaringan, Bandwidth, dan Proses Sinkronisasi**
   a. Memantau kestabilan koneksi antara DC dan DRC yang digunakan untuk proses replikasi.
   b. Memantau penggunaan bandwidth pada jaringan komunikasi DC–DRC dengan kapasitas MPLS 100 Mbps.
   c. Mendeteksi dan menangani gangguan yang dapat menyebabkan proses replikasi terlambat, gagal, atau tidak selesai dengan baik.
   d. Memastikan data antara DC dan DRC tetap tersinkronisasi sesuai dengan kebutuhan dan jadwal yang telah ditetapkan.
3. **Pengelolaan dan Pengujian Failover & Failback**
   a. Menyusun dan memperbarui *Standard Operating Procedure* (SOP) untuk proses *Failover* dan *Failback*.
   b. Melaksanakan simulasi *Disaster Recovery* (DR Test) minimal 2 (dua) kali dalam 1 (satu) tahun selama masa kontrak, yang meliputi:
      1. **Planned Failover** melakukan pengalihan layanan secara terencana dari DC ke DRC dengan memastikan data tetap tersedia dan konsisten.
      2. **Emergency/Unplanned Failover** melakukan simulasi pengalihan layanan ke DRC ketika DC Utama mengalami gangguan atau tidak dapat digunakan.
      3. **Failback to Production** mengembalikan layanan dari DRC ke DC Utama setelah kondisi normal, termasuk melakukan sinkronisasi perubahan data.

4. **Validasi Aplikasi dan Jaringan** memastikan aplikasi dapat berjalan dengan baik di DRC serta melakukan pemeriksaan konfigurasi jaringan, seperti *Re-IP Rules*, DNS, dan *Gateway*.

c. Mendokumentasikan hasil setiap pelaksanaan *Failover*, *Failback*, dan DR Test sebagai bahan evaluasi dan perbaikan proses pemulihan layanan.

2.4. Pemeliharaan Preventif (*Preventive Maintenance*)

Penyedia Jasa wajib melakukan pemeliharaan secara berkala untuk menjaga kondisi perangkat dan sistem tetap baik, aman, dan dapat beroperasi secara optimal, dengan cakupan sebagai berikut:

1. Melakukan pemeliharaan secara terjadwal setiap bulan (*Monthly*) dan setiap tiga bulan (*Quarterly*) terhadap perangkat keras dan perangkat lunak yang termasuk dalam layanan.
2. Melakukan pemeriksaan kondisi sistem, meliputi pembersihan *log*, pemeriksaan kondisi vCenter dan ESXi, pemeriksaan *Tape Library*, pengecekan kapasitas disk dan tape, pemeriksaan kondisi perangkat di DRC, serta pemeriksaan potensi risiko keamanan.
3. Menyampaikan hasil pemeriksaan dan memberikan rekomendasi perbaikan atau tindakan pencegahan apabila ditemukan masalah atau potensi risiko.
4. Mendokumentasikan hasil pemeliharaan sebagai bahan pemantauan dan evaluasi kondisi sistem.

2.5. Transfer Knowledge & Workshop Teknis

Penyedia Jasa wajib memberikan pelatihan dan berbagi pengetahuan kepada staf Divisi Teknologi Informasi PT KBI agar tim internal dapat memahami dan mengelola sistem secara mandiri, dengan cakupan sebagai berikut:

1. Menyelenggarakan pelatihan teknis dan workshop praktik (*hands-on*) bagi staf Divisi Teknologi Informasi PT KBI dengan jumlah peserta minimal 5–10 orang.
2. Materi pelatihan sekurang-kurangnya mencakup:
   - Pengelolaan dan penanganan masalah pada VMware vSphere Cluster.
   - Pengelolaan Backup Veritas NetBackup, penggunaan dan pengelolaan Tape LTO, serta proses pemulihan katalog backup saat terjadi gangguan.
   - Pengelolaan replikasi Veeam, penggunaan bandwidth jaringan, serta pelaksanaan proses *Failover* dan *Failback* antara DC dan DRC.
3. Menyediakan materi atau modul panduan yang dapat digunakan oleh tim internal setelah pelatihan.
4. Menyediakan lingkungan praktik (*lab environment*) apabila diperlukan untuk mendukung proses pelatihan.
5. Menyediakan rekaman pelatihan dan sertifikat bagi peserta.

2.6. Dokumentasi Vmware, Veritas, Veeam

Penyedia Jasa wajib melakukan pencatatan dan pemutakhiran informasi aset serta dokumentasi teknis agar kondisi dan konfigurasi sistem dapat diketahui dengan jelas dan mudah dikelola, dengan cakupan sebagai berikut:

1. Membuat dan memperbarui dokumentasi teknis yang diperlukan, meliputi:
   - *High-Level Design* (HLD) dan *Low-Level Design* (LLD).
   - Diagram topologi Virtualisasi, Backup Tape, dan jaringan Replikasi DC–DRC.
   - *Disaster Recovery Runbook/Playbook* yang berisi langkah-langkah pelaksanaan pemulihan sistem secara jelas dan mudah diikuti.
2. Memastikan seluruh dokumentasi diperbarui apabila terdapat perubahan konfigurasi, perangkat, atau sistem.

3. SPESIFIKASI TEKNIS

3.1 Spesifikasi Umum & Ketersediaan Layanan

Penyedia Jasa wajib menyediakan layanan dukungan teknis dan pengelolaan sistem secara berkelanjutan untuk memastikan sistem VMware, Veritas, dan Veeam PT KBI dapat berjalan dengan baik, aman, dan tersedia sesuai kebutuhan operasional.

Komponen	Spesifikasi Layanan Minimal
Waktu Operasional Dukungan	Dukungan teknis tersedia selama 24 Jam x 7 Hari x 365 Hari (24/7/365), baik untuk pemantauan maupun penanganan gangguan.
Dukungan Personel	Menyediakan dukungan Onsite untuk kegiatan pemeliharaan terjadwal dan penanganan gangguan kritis (*Severity 1*).
Saluran Dukungan (*Helpdesk*)	Menyediakan grup komunikasi khusus antara Tim Teknis PT KBI dan Penyedia Jasa.
	Menyediakan *hotline* telepon darurat dan email resmi *helpdesk* yang dapat dihubungi 24/7.
Cakupan Sistem PT KBI	VMware: vSphere Enterprise Plus dengan jumlah 288 core.
	Veritas: NetBackup/Backup Exec dengan kapasitas backup () dan jumlah *Tape Library* LTO sebanyak ().
	Veeam: Backup & Replication Enterprise Plus dengan jumlah 50 instance.

3.2 Metode Kerja

Pelaksanaan layanan dilakukan secara terencana dan berkelanjutan melalui pemantauan sistem, pemeliharaan, penanganan gangguan, serta evaluasi berkala. Setiap kegiatan harus dicatat dan didokumentasikan sebagai bahan pemantauan dan evaluasi layanan. Metode kerja

sekurang-kurangnya meliputi:

1. **Pemantauan Sistem**
   - Melakukan pemantauan kondisi VMware, Veritas, dan Veeam secara berkala.
   - Mengidentifikasi potensi gangguan sebelum berdampak pada layanan.
   - Menyampaikan pemberitahuan apabila ditemukan kondisi yang membutuhkan tindakan.
2. **Penanganan Gangguan**
   - Menerima dan mencatat setiap laporan gangguan melalui sistem *ticketing* atau saluran bantuan yang tersedia.
   - Menentukan tingkat prioritas gangguan berdasarkan dampaknya terhadap layanan.
   - Melakukan penanganan dan pemulihan sesuai tingkat prioritas dan target waktu layanan yang disepakati.
3. **Pemeliharaan Berkala**
   - Melaksanakan *preventive maintenance* sesuai jadwal yang telah disepakati.
   - Melakukan pemeriksaan kondisi sistem, kapasitas, performa, keamanan, dan konfigurasi.
   - Memberikan rekomendasi apabila ditemukan potensi masalah atau kebutuhan peningkatan sistem.
4. **Pelaporan dan Evaluasi**
   - Menyediakan laporan hasil pemantauan, pemeliharaan, penanganan gangguan, dan kegiatan lainnya secara berkala.
   - Melakukan evaluasi layanan bersama Tim PT KBI untuk memastikan target layanan terpenuhi.

Memperbarui dokumentasi apabila terdapat perubahan konfigurasi atau lingkungan sistem.

3.3 Spesifikasi Teknis VMware

Penyedia Jasa wajib melakukan pengelolaan dan optimalisasi lingkungan VMware untuk menjaga ketersediaan, keamanan, dan kinerja sistem, dengan cakupan sebagai berikut:

1. **Pengelolaan Cluster**
   a. Melakukan pengaturan dan optimalisasi *vSphere High Availability* (HA) untuk memastikan VM tetap dapat berjalan apabila terjadi gangguan pada Host ESXi.
   b. Melakukan pengaturan *Admission Control* dan *Datastore Heartbeating* untuk membantu menjaga ketersediaan VM.
   c. Melakukan pengaturan *vSphere Distributed Resource Scheduler* (DRS) agar beban kerja VM dapat dibagi secara optimal pada seluruh Host ESXi.
   d. Mengatur aturan *Anti-Affinity* untuk VM yang memiliki fungsi penting, seperti database dan aplikasi yang berjalan dalam satu cluster.

2. **Pengelolaan Jaringan Virtual**
    a. Mengatur *vSphere Distributed Switch* (VDS) untuk memisahkan lalu lintas jaringan sesuai dengan fungsinya.
    b. Segmentasi jaringan sekurang-kurangnya mencakup *Management Network*, *vMotion Network*, *IP Storage Network*, *Veeam Replication Network*, dan *Virtual Machine Traffic*.
    c. Menggunakan VLAN (*802.1Q VLAN Tagging*) untuk membantu menjaga pemisahan lalu lintas jaringan.
    d. Mengatur penggunaan bandwidth melalui *Network I/O Control* sesuai dengan kebutuhan masing-masing layanan.
3. **Pengelolaan Storage dan Datastore**
    a. Melakukan pemantauan kapasitas *Datastore* dan memberikan peringatan apabila penggunaan mencapai batas yang telah ditentukan, yaitu **80% untuk kondisi peringatan** dan **90% untuk kondisi kritis**.
    b. Melakukan optimalisasi jalur koneksi Storage (*Multipathing*), termasuk penggunaan metode *Round Robin* apabila sesuai dengan konfigurasi Storage.
    c. Melakukan pemeriksaan dan penanganan *snapshot* VM yang sudah tidak diperlukan atau tidak terhapus dengan sempurna.
4. **Pengelolaan Lifecycle dan Patch**
    a. Menggunakan VMware Lifecycle Manager (vLCM) untuk membantu pengelolaan dan pembaruan Host ESXi.
    b. Melakukan pemeriksaan kesesuaian konfigurasi dengan *baseline* yang telah ditentukan.
    c. Memastikan perangkat keras dan VMware yang digunakan sesuai dengan *Hardware Compatibility List* (HCL).
    d. Melakukan pembaruan sistem secara terencana dengan meminimalkan gangguan terhadap layanan produksi.

3.4 Spesifikasi Teknis Tape Veritas

Penyedia Jasa wajib mengelola sistem backup Veritas untuk memastikan data dapat dicadangkan, disimpan, dan dipulihkan dengan baik, dengan cakupan sebagai berikut:

1. **Konfigurasi Backup VM**
    a. Menggunakan integrasi VADP (*VMware vStorage APIs for Data Protection*) untuk melakukan backup VM.
    b. Menggunakan metode *Changed Block Tracking* (CBT) untuk mengurangi jumlah data yang perlu diproses saat backup.

c. Mengoptimalkan proses backup agar waktu yang dibutuhkan tidak mengganggu operasional sistem.

2. **Pengelolaan Storage dan Deduplication**
   a. Melakukan pemeliharaan *Media Server Deduplication Pool* (MSDP) agar tetap berfungsi dengan baik.
   b. Memantau tingkat efisiensi *deduplication* dan kapasitas penyimpanan backup.
   c. Melakukan pemeriksaan dan pemeliharaan secara berkala terhadap sistem deduplikasi untuk mencegah gangguan pada proses backup dan restore.
3. **Pengelolaan Tape Library**
   a. Mendukung pengelolaan *Tape Library* LTO-7, LTO-8, dan LTO-9 sesuai dengan perangkat yang digunakan PT KBI.
   b. Melakukan pengelolaan kaset tape, termasuk pembacaan barcode, pemeriksaan slot, pencatatan inventaris, dan penanganan kaset yang mengalami kerusakan (*bad tape*).
   c. Melakukan pembersihan *Tape Drive* secara berkala menggunakan *cleaning cartridge* sesuai kebutuhan.
   d. Menerapkan kebijakan penyimpanan GFS (*Grandfather-Father-Son*), dengan backup harian disimpan pada disk dan backup mingguan, bulanan, serta tahunan disalin ke kaset tape untuk kebutuhan arsip.
4. **Uji Pemulihan Data dari Tape**
   a. Melakukan uji pemulihan (*restore test*) dari kaset tape yang telah disimpan di lokasi *offsite/vaulting* minimal **1 (satu) kali setiap bulan**.
   b. Memastikan data pada kaset dapat dibaca dan dipulihkan dengan baik serta tidak mengalami kerusakan atau korupsi.
   c. Mendokumentasikan hasil pengujian sebagai bukti bahwa data backup dapat digunakan saat diperlukan.

3.5 Spesifikasi Teknis Backup Replikasi Veeam

Penyedia Jasa wajib mengelola replikasi VM dari DC Utama ke DRC serta melakukan pengujian pemulihan untuk memastikan sistem dapat digunakan apabila terjadi gangguan pada DC Utama.

1. **Pengelolaan Replikasi**
   a. Menggunakan fitur Veeam yang sesuai untuk memindahkan dan menyinkronkan data VM dari DC ke DRC.
   b. Mengaktifkan *Changed Block Tracking* (CBT) untuk membantu mengurangi jumlah data yang perlu dikirim selama proses replikasi.

c. Mengoptimalkan kompresi dan penggunaan bandwidth agar proses replikasi berjalan efisien dan tidak mengganggu layanan lainnya.

2. **Penyimpanan Restore Point**
   a. Menyediakan dan menjaga minimal **7–14 Restore Points** pada DRC sesuai dengan kebutuhan dan kebijakan perusahaan.
   b. Melakukan pemantauan terhadap kondisi *Restore Point* untuk memastikan data yang tersedia dapat digunakan saat proses pemulihan.
   c. Menjaga ketersediaan *Restore Point* sebagai salah satu langkah perlindungan terhadap kegagalan sistem dan insiden keamanan, termasuk ransomware.
3. **Simulasi Disaster Recovery (DR Testing)**
   a. Melaksanakan simulasi *Disaster Recovery* sebanyak **2 (dua) kali dalam 1 (satu) tahun** dengan skenario pengalihan layanan dari DC ke DRC.
   b. Melakukan pengujian *Network Re-IP Mapping* untuk memastikan VM yang dijalankan di DRC menggunakan alamat IP dan konfigurasi jaringan yang sesuai.
   c. Melakukan pengujian aplikasi setelah *Failover* untuk memastikan aplikasi dapat berjalan dengan baik di DRC.
   d. Melakukan proses *Failback* untuk mengembalikan layanan dari DRC ke DC Utama secara aman dan memastikan data tetap konsisten.
   e. Mendokumentasikan hasil setiap pelaksanaan DR Test, termasuk hasil *Failover*, pengujian aplikasi, dan *Failback*.

4. DELIVERABLES

Penyedia jasa wajib menghasilkan dan menyerahkan seluruh deliverable berikut kepada pihak perusahaan:

Kategori Deliverable	Rincian Dokumen & Konten	Batas Waktu Penyerahan
Dokumen Asesmen Awal (Baseline Report)	Audit kondisi eksisting seluruh cluster VMware, Veritas Backup & Tape, serta Veeam Replication; analisis celah kerentanan (*gap analysis & security baseline*); rencana aksi perbaikan awal (*Remediation Plan*).	Maksimal 30 hari kalender sejak *Kick-Off Meeting*.
Dokumen Teknis Arsitektur (HLD, LLD, & DRP Playbook)	HLD & LLD sistem virtualisasi, backup, dan replikasi; diagram topologi fisik dan logikal jaringan DC-DRC; *Disaster Recovery Plan (DRP) Playbook* berisi SOP Failover & Failback langkah demi langkah.	Diserahkan pada bulan ke-2 kontrak dan dimutakhirkan setiap ada perubahan arsitektur.
Laporan Operasional	*Weekly Report*: rekap tiket, job backup, utilisasi bandwidth replikasi, status	Mingguan: setiap Senin minggu berikutnya.

Kategori Deliverable	Rincian Dokumen & Konten	Batas Waktu Penyerahan
Berkala	sistem. *Monthly Report*: analisis performa kluster VMware, rekap kepatuhan SLA, inventaris tape, status replikasi Veeam. *Quarterly Report*: evaluasi tren kapasitas, analisis insiden, rekomendasi strategis.	Bulanan: maksimal tanggal 5 bulan berjalan. Triwulanan: maksimal 10 hari kerja setelah triwulan berakhir.
Laporan Preventive Maintenance & Uji DR	Berita Acara Pelaksanaan PM (Bulanan/Triwulanan); Laporan Uji Coba Pemulihan Data dari Kaset Tape (log restore & checksum data); Laporan Hasil Simulasi DR Veeam (RPO & RTO aktual, evaluasi failover/failback).	Maksimal 7 hari kerja setelah setiap kegiatan selesai dilaksanakan.
Dokumentasi Transfer Knowledge	Silabus pelatihan, modul panduan teknis, *presentation deck*; rekaman video pelaksanaan pelatihan; daftar hadir & sertifikat pelatihan resmi.	Maksimal 14 hari kerja setelah pelatihan diselenggarakan.
Laporan Akhir Kontrak & BAST	Laporan evaluasi komprehensif layanan selama 12 bulan; rekapitulasi pencapaian SLA tahunan; pemutakhiran dokumen CMDB final; rekomendasi arah pengembangan TI tahun berikutnya; dokumen Berita Acara Serah Terima (BAST).	

5. JANGKA WAKTU PELAKSANAAN

1. **Durasi Kontrak**

   Layanan dilaksanakan selama **12 (dua belas) bulan kalender**, terhitung sejak penandatanganan Kontrak atau Surat Perintah Mulai Kerja (SPMK).

2. **Tahapan Pekerjaan**

   Pelaksanaan pekerjaan dilakukan secara bertahap dengan rencana sebagai berikut:

   a. **Minggu 1**: Pelaksanaan *kick-off meeting*, pendataan aset awal, pemeriksaan kondisi sistem (*Baseline Assessment*), serta penyusunan rencana perbaikan (*Remediation Plan*).

   b. **Minggu 2**: Penyusunan dokumen arsitektur sistem, termasuk HLD/LLD dan *Disaster Recovery Playbook*.

   c. **Bulan ke-1 sampai dengan ke-12**: Pelaksanaan layanan *Managed Service* 24/7, pemantauan sistem, penanganan gangguan, pemeliharaan berkala, uji pemulihan data dari tape setiap bulan, serta penyampaian laporan secara berkala.

   d. **Bulan ke-4 dan ke-10**: Pelaksanaan simulasi *Disaster Recovery* (DR) antara DC dan DRC, termasuk pengujian *Failover* dan *Failback*.

6. KRITERIA DAN Nilai Tambah VENDOR

6.1. Kualifikasi Kemitraan Resmi dengan Prinsipal Teknologi

Penyedia Jasa wajib memiliki hubungan kemitraan resmi dan masih aktif dengan prinsipal teknologi yang digunakan dalam layanan. Kemitraan tersebut dibuktikan dengan sertifikat partner atau surat dukungan resmi dari prinsipal terkait. Persyaratan minimal kemitraan adalah:

a. VMware/Broadcom
b. Veritas Technologies
c. Veeam Software

6.2. Pengalaman Perusahaan

Penyedia Jasa wajib memiliki pengalaman yang sesuai dengan pekerjaan yang akan dilaksanakan, dengan ketentuan:

a. Memiliki pengalaman dalam 3–5 tahun terakhir dalam pekerjaan yang berkaitan dengan *Managed Service* infrastruktur TI, virtualisasi, sistem backup, *Tape Library*, dan *Disaster Recovery*.
b. Memiliki minimal 2 (dua) pengalaman pekerjaan yang telah atau sedang dilaksanakan
c. Pengalaman tersebut diutamakan mencakup pengelolaan VMware, backup menggunakan Tape Library, serta replikasi sistem antara DC dan DRC.

6.3. Dokumen Persyaratan yang Harus Dilampirkan

Penyedia Jasa wajib menyampaikan dokumen pendukung sebagai bukti pemenuhan persyaratan, sekurang-kurangnya meliputi:

a. Company Profile dan struktur organisasi tim yang akan menangani layanan.
b. Sertifikat atau surat dukungan kemitraan resmi dari VMware/Broadcom, Veritas, dan Veeam.
c. Dokumen yang membuktikan pengalaman pekerjaan, seperti kontrak kerja, Purchase Order (PO), atau BAST, untuk pekerjaan sejenis dalam 3–5 tahun terakhir.
d. CV tenaga ahli yang diajukan, dilengkapi dengan salinan ijazah dan sertifikat keahlian yang dipersyaratkan.
e. Proposal Teknis yang menjelaskan sekurang-kurangnya:
   - Metode pelaksanaan layanan *Managed Service*.
   - Rencana *Preventive Maintenance*.
   - Metode pengujian dan pemulihan data dari tape.
   - Metode pelaksanaan simulasi *Disaster Recovery*, termasuk *Failover* dan *Failback*.
   - Rencana pemantauan, penanganan gangguan, dan pelaporan layanan.

7. *SERVICE LEVEL AGREEMENT (SLA)*

7.1. Tingkat Keparahan Insiden (*Severity Level*)

Setiap gangguan akan dikelompokkan berdasarkan tingkat dampaknya terhadap operasional PT KBI. Pengelompokan ini digunakan untuk menentukan prioritas dan waktu penanganan.

1. **Severity 1 (Critical/P1)**

   Gangguan yang menyebabkan layanan utama berhenti atau berdampak besar terhadap operasional bisnis, antara lain:

   a. Sebagian besar atau seluruh Host ESXi/Cluster VMware mengalami gangguan sehingga VM atau layanan utama tidak dapat berjalan.
   b. vCenter Server tidak dapat digunakan dan fitur HA tidak dapat berfungsi.
   c. Replikasi Veeam untuk seluruh VM yang bersifat kritis mengalami kegagalan.
   d. Master Server Veritas mengalami gangguan total sehingga proses backup dan perlindungan data berhenti.

2. **Severity 2 (High/P2)**

   Gangguan yang berdampak cukup besar, tetapi layanan masih dapat berjalan menggunakan sistem cadangan atau redundansi, antara lain:

   a. Salah satu Host ESXi mengalami gangguan sehingga VM harus dipindahkan ke Host lainnya.
   b. Penggunaan kapasitas Datastore melebihi batas kritis, yaitu lebih dari **90%**.
   c. Sebagian proses replikasi Veeam mengalami kegagalan.
   d. Terjadi kerusakan pada *Tape Drive* atau mekanisme *Tape Library*.

3. **Severity 3 (Medium/P3)**

   Gangguan dengan dampak terbatas dan tidak menghentikan layanan utama, antara lain:

   a. Backup gagal pada 1–2 VM yang tidak bersifat kritis.
   b. Penurunan kinerja *vMotion* atau gangguan monitoring yang tidak berdampak pada transaksi.
   c. Permintaan perubahan kecil pada jadwal atau konfigurasi backup dan replikasi.

4. **Severity 4 (Low/Request/P4)**

   Permintaan layanan yang tidak menyebabkan gangguan operasional, seperti:

   a. Konsultasi atau bantuan teknis.
   b. Permintaan perubahan konfigurasi standar.
   c. Permintaan laporan atau data operasional.
   d. Permintaan informasi atau asistensi teknis lainnya.

7.2. Jam Layanan dan Saluran Dukungan

1. **Jam Layanan**

   a. Severity 1 dan Severity 2: dukungan tersedia 24 Jam x 7 Hari x 365 Hari (24/7/365), termasuk hari libur nasional.

b. Severity 3 dan Severity 4: dukungan diberikan pada hari kerja, yaitu Senin–Jumat pukul 08.00–17.00 WIB, kecuali terdapat kesepakatan lain.
c. Untuk kondisi tertentu yang membutuhkan penanganan di luar jam kerja, Penyedia Jasa wajib menyediakan dukungan sesuai kebutuhan.

2. Support Team

a. Menyediakan sistem *ticketing* resmi untuk mencatat dan memantau setiap gangguan atau permintaan layanan.
b. Menyediakan grup komunikasi khusus antara Tim Teknis PT KBI dan tim teknis Penyedia Jasa.
c. Menyediakan *hotline* telepon darurat yang dapat dihubungi 24/7 untuk insiden kritis.
d. Menyediakan email resmi *helpdesk*.
e. Menyediakan akses jarak jauh yang aman (*Secure Remote Access*) melalui VPN/PAM resmi PT KBI apabila diperlukan.
f. Menyediakan teknisi *onsite* apabila gangguan tidak dapat diselesaikan melalui dukungan jarak jauh.

7.3. Target Waktu Respons dan Penyelesaian Insiden

Penyedia Jasa wajib memenuhi target waktu respons dan penyelesaian gangguan sebagai berikut:

Tingkat Insiden	Respons	Onsite Jika Diperlukan	Target Penyelesaian
Severity 1 (Critical/P1)	≤ 15 menit	≤ 1 jam	≤ 2 jam untuk *workaround/recovery*
Severity 2 (High/P2)	≤ 30 menit	≤ 2 jam	≤ 4 jam
Severity 3 (Medium/P3)	≤ 1 jam	Sesuai kebutuhan	≤ 8 jam / 1 hari kerja
Severity 4 (Low/P4)	≤ 2 jam	Tidak wajib / *Remote Support*	≤ 24 jam / 1–2 hari kerja

7.4. Target RPO dan RTO

Penyedia Jasa wajib menjaga target pemulihan data dan layanan sesuai dengan ketentuan berikut:

Parameter	Target	Keterangan
RPO (Recovery Point Objective)	≤ 15 menit, maksimal 30 menit	Batas waktu kehilangan data yang dapat diterima apabila terjadi gangguan pada DC Utama dan layanan harus dipulihkan melalui DRC.

RTO (Recovery Time Objective)	≤ 1 jam, maksimal 2 jam	Batas waktu yang dibutuhkan untuk mengaktifkan kembali VM dan layanan utama di DRC setelah terjadi gangguan pada DC Utama.

Pencapaian RPO dan RTO harus diuji dan dibuktikan melalui pelaksanaan simulasi *Disaster Recovery* secara berkala.

8. Timeline Proses Pengadaan

ESTIMASI TIMELINE PENGADAAN JASA MANAGED SERVICE VMWARE, VERITAS BACKUP DAN VEEAM PADA PT KLIRING BERJANGKA INDONESIA

Tanggal Mulai (Sejak Perencanaan) 9/30/2026

Tanggal Mulai Pengadaan 10/2/2026

Tahap	Durasi (Hari)	Kegiatan Operasional	Unsur Bertanggung Jawab	Jadwal	Waktu	Keterangan
Pelaksanaan & Evaluasi	2	Pendaftaran	Tim Pengadaan Pengadaan	10/6/2026	13.00 WIB	Pendaftaran dilakukan melalui link website PTKBI.COM
	1	Penjelasan Dokumen (Aanwijzing)	User & Tim Pengadaan	10/7/2026	10.00 WIB	Invitation dikirimkan ke email PIC masing-masing penyedia.
	4	Submit Proposal Teknis dan Surat Penawaran Harga	Penyedia	10/13/2026	15.00 WIB	Dikirimkan ke email pengadaan@ptkbi.com dan cc: dti@ptkbi.com
	1	Evaluasi Proposal Teknis dan Penawaran Harga	Tim Pengadaan dan User	10/14/2026	-	proses internal KBI
	3	Klarifikasi & Negosiasi	Fungsi Pengadaan & User	10/19/2026	10.00 WIB - 17.00 WIB	akan dikirimkan jadwal ke email masing-masing penyedia
	1	Batas Waktu Submit Penawaran Revisi Teknis dan Harga	Penyedia	10/20/2026	11.59 WIB	Dikirimkan ke email pengadaan@ptkbi.com dan cc: dti@ptkbi.com
	1	Evaluasi Administratif & Penawaran (Penilaian)	Tim Pengadaan dan User	10/21/2026	-	proses internal KBI
Penetapan & Perikatan	2	Penetapan Pemenang & Pengumuman Pemenang	Tim Pengadaan	10/23/2026	-	proses internal KBI
	4	Masa Sanggah	Penyedia	10/29/2026	-	4 hari kerja
	1	SIK (Surat Instruksi Kerja)	Tim Pengadaan/Unit Pengadaan	10/30/2026	-	SIK diterbitkan
	10	Otorisasi & Kontrak	Pejabat Berwenang & Unsur Legal	11/13/2026	-	-

Note:
- Jadwal diatas tidak termasuk hari libur (hanya hari kerja)
- Jadwal diatas dapat berubah (lebih cepat atau mundur) apabila terdapat penyesuaian jadwal yang disebabkan oleh Internal KBI/ Eksternal (Penyedia)

9. Termin Pembayaran

1. **Pembayaran Termin I sebesar 25% (dua puluh lima persen)**

   Pembayaran kepada Penyedia Jasa setelah menyelesaikan layanan operasional *Managed Service* bulan ke-1 sampai dengan bulan ke-3. Pembayaran ini dibuktikan dengan :

   a. penyerahan Laporan Asesmen Awal (*Baseline Report*)
   b. Dokumen Arsitektur Teknis mencakup *High-Level Design* (HLD)
   c. *Low-Level Design* (LLD)
   d. *Guide Disaster Recovery Plan (DRP)*
   e. Laporan Uji Pemulihan Data Tape Bulanan periode bulan ke-1 hingga ke-3
   f. Laporan Operasional Berkala (*Weekly* dan *Monthly Report*)

g. Berita Acara Serah Terima Pekerjaan (BAST) Tahap I.

2. Pembayaran Termin II sebesar 25% (dua puluh lima persen)

Pembayaran setelah penyelesaian layanan operasional bulan ke-4 sampai dengan bulan ke-6. Pembayaran dapat dilakukan setelah melengkapi :

a. Laporan Hasil Simulasi *Disaster Recovery (DR Test)* Ke-1
b. Berita Acara PM Triwulan II
c. Laporan Uji Pemulihan Data Tape Bulanan periode bulan ke-4 hingga ke-6
d. Laporan Operasional Berkala
e. BAST Tahap II.

3. Pembayaran Termin III sebesar 25% (dua puluh lima persen)

Pembayaran setelah Penyedia Jasa menyelesaikan layanan operasional bulan ke-7 sampai dengan bulan ke-9. Pembayaran diproses berdasarkan :

a. Berita Acara (BAST) PM Triwulan III
b. Laporan Uji Pemulihan Data Tape Bulanan periode bulan ke-7 hingga ke-9
c. Laporan Operasional Berkala.

4. Pembayaran Termin IV sebesar 25% (dua puluh lima persen)

Pembayaran setelah Penyedia Jasa menyelesaikan seluruh cakupan layanan operasional hingga bulan ke-12. Syarat penagihan pelunasan ini melingkupi :

a. Laporan Hasil Simulasi *Disaster Recovery (DR Test)* Ke-2
b. Berita Acara PM Triwulan IV
c. Laporan Uji Pemulihan Data Tape Bulanan periode bulan ke-10 hingga ke-12
d. Laporan Akhir Evaluasi Layanan Kontrak 12 Bulan
e. Berita Acara Serah Terima (BAST) Pekerjaan 100%.

10. KOMPOSISI PENILAIAN

Komposisi Penilaian untuk Pengadaan Managed service vmware, veritas, veeam ini adalah ditetapkan sebesar 70% untuk Teknis, dan 30% untuk Harga, menggunakan sistem scoring berikut detailnya :

No.	Penilaian	Bobot	Kriteria	Nilai
1	Teknis	70 %	Pengalaman	15 %
			Metodologi Implementasi	20 %
			Sertifikasi Partnership dan Kompetensi	10 %
			Kompetensi Tenaga Ahli	15 %
			Jangka Waktu Implementasi	10 %
2	Harga	30 %	Selisih Harga	30 %
TOTAL				100 %

11. PENUTUP

Dokumen ini menjadi acuan pelaksanaan pengadaan software office365, visio dan managed service active directory untuk mendukung kestabilan operasional perangkat jaringan dan memastikan keberlangsungan layanan TI.

Menyetujui,	Reviewer,	Pembuat,
Oki Marsetiawan	**M Ilham Utama**	**Krisna Aji Putra**
Kepala Divisi Teknologi Informasi	Staf Divisi Teknologi Informasi	Staf Divisi Teknologi Informasi