EVALUASI IMPLEMENTASI

Sistem Pemerintahan Berbasis Elektronik (SPBE)

pada Unit Kerja — Kantor Wilayah Kementerian Hukum Kalimantan Barat

Oleh :
Rendi Apriandi
Pranata Komputer Ahli Pertama

27 Agustus 2026

Mengapa Evaluasi SPBE Perlu Dilakukan?

Akselerasi transformasi digital merupakan mandat nasional untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel. Evaluasi ini disusun untuk memotret capaian, kendala, dan kondisi eksisting SPBE pada Kantor Wilayah Kementerian Hukum Kalimantan Barat Tahun 2026, sebagai kewajiban pelaporan evaluasi berkala demi perbaikan berkelanjutan.

B KONDISI SAAT INI

Identifikasi Kondisi Eksisting SPBE

Kebijakan

6 SOP teknis telah diterbitkan, mencakup layanan publik & manajerial internal

SDM TI

Ditopang JFT Pranata Komputer(1 Ahli Muda, 4 Ahli Pertama) & 1 Pengolah Data.

Infrastruktur

Topologi backbone terpusat, 3 switch hub & klaster server (Rackmount + Tower)

Aplikasi

9 aplikasi pusat berjalan + 5 aplikasi mandiri (SILANOK, dll.)

Keamanan

70 perangkat di-screening; 2 infected; 44 Office & 34 Nitro PDF bajakan

Manajemen Risiko

Formulir manajemen risiko disusun berkala berdasar laporan ke Pusdatin

Kondisi SPBE yang Ditargetkan (Ideal)

Kebijakan Terintegrasi

SOP tersinkron dengan Peta Rencana SPBE Kementerian secara menyeluruh

SDM Kompeten & Memadai

Jumlah dan kapasitas JFT Pranata Komputer mencukupi kebutuhan keamanan siber

Infrastruktur Andal

Jaringan stabil dengan skema redundansi/disaster recovery, tanpa single point of failure

Aplikasi Terintegrasi

Seluruh aplikasi mandiri tergabung dalam satu dashboard eksekutif real-time

Keamanan Terjamin

Perangkat lunak berlisensi penuh, diuji penetrasi (pentest) secara berkala

Audit Terjadwal

Audit SPBE internal & eksternal berjalan rutin dan terdokumentasi

B GAP ANALYSIS

Kesenjangan Kondisi Saat Ini vs. Diharapkan

Aspek	Kondisi Saat Ini	Kondisi Diharapkan	Gap / Prioritas
Keamanan Software	44 Office & 34 Nitro PDF bajakan	100% perangkat lunak berlisensi resmi	Masih tingginya penggunaan perangkat lunak bajakan (risiko keamanan & kepatuhan lisensi). **TINGGI**
Integrasi Data	5 aplikasi mandiri berjalan terpisah (silo)	1 dashboard eksekutif terintegrasi	Aplikasi mandiri belum terintegrasi dalam dashboard eksekutif. **TINGGI**
Audit SPBE	Belum ada agenda audit formal terjadwal	Audit internal/eksternal berkala	Ketiadaan jadwal audit formal membuat pengawasan keamanan sistem bersifat reaktif, bukan preventif, tanpa mekanisme evaluasi kepatuhan dan kontrol keamanan yang berkala dan terdokumentasi. **SEDANG**
Redundansi Server	1 Ruang Server Utama (titik tunggal)	Skema disaster recovery/backup site	Belum ada skema redundansi/disaster recovery untuk memitigasi single point of failure pada Ruang Server Utama; pemeliharaan berkala perangkat jaringan perlu diperkuat. **SEDANG**
Kapasitas SDM	JFT Pranata Komputer terbatas	SDM memadai & tersertifikasi keamanan	Kekurangan personel JFT Pranata Komputer dibanding beban kerja; kompetensi keamanan siber perlu ditingkatkan secara berkelanjutan. **SEDANG**

Kesimpulan Evaluasi Implementasi SPBE

1

Kematangan Kebijakan

Dasar operasional cukup kuat melalui 6 SOP teknis yang mencakup layanan publik & internal.

2

Ketangguhan Infrastruktur

Modernisasi topologi jaringan & klaster server meningkatkan stabilitas dan keamanan data lokal.

3

Celah Keamanan Informasi

Penggunaan perangkat lunak tidak berlisensi menjadi risiko utama meski malware aktif dapat dimitigasi.

4

Integrasi Layanan Belum Optimal

Aplikasi mandiri efektif menutup kebutuhan teknis, namun belum terintegrasi dalam satu sistem pelaporan.

D REKOMENDASI

Rekomendasi Perbaikan SPBE

1 Migrasi Perangkat Lunak

Pengadaan lisensi resmi atau migrasi ke Open Source untuk menutup celah keamanan.

2 Peningkatan Kapasitas SDM

Bimtek keamanan siber bagi JFT Pranata Komputer & digital awareness bagi pegawai.

3 Sertifikasi Keamanan

Penetration testing berkala pada aplikasi mandiri bersama BSSN/Pusdatin.

4 Penyatuan Database

Integrasi aplikasi lokal ke dalam satu dashboard eksekutif real-time.

5 Penguatan Audit SPBE

Penjadwalan audit internal SPBE secara berkala dan terdokumentasi.

6 Redundansi Infrastruktur

Kajian skema disaster recovery/backup site untuk Ruang Server Utama.

Rencana Tindak Lanjut & Target Waktu

1. Migrasi dan/atau pengadaan lisensi perangkat lunak resmi menjadi tanggung jawab Tim TI bersama Bagian Umum.

2. Pelaksanaan pelatihan keamanan siber dan peningkatan kesadaran digital (digital awareness) akan dikoordinasikan oleh Tim TI bekerja sama dengan Bagian Kepegawaian.

3. Pengujian penetrasi (penetration testing) terhadap aplikasi internal akan dilaksanakan oleh Tim TI.

4. Pengembangan dashboard eksekutif yang terintegrasi menjadi tanggung jawab Tim TI.’

5. Penjadwalan pelaksanaan audit internal Sistem Pemerintahan Berbasis Elektronik (SPBE) akan dikoordinasikan oleh Tim TI bersama pimpinan unit kerja.

6. Adapun kajian mengenai skema redundansi dan/atau pemulihan bencana (disaster recovery) menjadi tanggung jawab Tim TI.

TERIMA KASIH

Evaluasi Implementasi SPBE — Kantor Wilayah Kementerian Hukum Kalimantan Barat, Tahun 2026

Pontianak, 2026